

Architectuurstatement Digitaal Archiveren Rechtspraak

Goedgekeurde versie:

Document	Status DA	Versie	Link naar het goedgekeurd document
Architectuurstatement Digitaal Archiveren Rechtspraak	Definitief	1.0	

Versiebeheer

Datum	Versie	Auteur	Wijziging	Ter review aangeboden
08 Oct 2021	0.1		Eerste versie omschrijven van GPSA naar Architectuur Statement	
21 Feb 2022	0.2		Eerste versie ter collegiale reviews	
21 Mar 2022	0.3		Aanpassingen op basis van de collegiale	
12 Apr 2022	0.4		Opmerkingen DA verwerkt	
21 Apr 2022	0.5		Bussines architectuur aangepast	
12 May 2022	1.0		Vastgesteld door de DA	DA
10 Oct 2022	1.1		Aanpassingen voor een SaaS dienst	
27 Oct 2022	1.2		Laatste Wijzigingen aangebracht op basis van de collegiale review	

Inhoudsopgave

- [1. Inleiding](#)
- [2. Context en scope](#)
 - [Context](#)
 - [Archiveren by design](#)
 - [Document lifecycle](#)
 - [Scope](#)
 - [Scope binnen de rechtspraak](#)
 - [Businessdoelen](#)
 - [Huidige situatie](#)
 - [Archiveren vanuit Primaire Proces Systemen \(PPS\)](#)
 - [Toekomstige situatie: Conceptueel model](#)
 - [Archiveren Primaire Proces Systemen \(PPS\)](#)
 - [Archiveren ondersteunende diensten](#)
 - [Uitgangspunten](#)
- [3. Grondslagen](#)
 - [Beleidskaders](#)
 - [Wet en regelgeving](#)
 - [Normen en standaarden](#)
 - [IVO beleid en strategie](#)
- [4. Businessarchitectuur](#)
 - [Betrokkenen](#)
 - [Interne betrokkenen](#)
 - [Gedelegeerd betrokkenen](#)
 - [Externe betrokkenen](#)
- [5. Informatie-architectuur](#)
 - [Relatie tussen de modellen](#)
- [6. Applicatie-architectuur](#)
 - [Uitgangspunten](#)
 - [Communicatie](#)
- [7. Technische architectuur](#)
 - [SaaS](#)
- [8. Security en Privacy](#)
 - [8.2 BIV-P classificatie](#)
 - [8.4 Privacy eisen](#)
- [9. Kwaliteitseisen](#)
- [Bijlage 1: Woordenlijst](#)

1. Inleiding

Dit document beschrijft de referentie architectuur voor het project Digitaal Archiveren Rechtspraak (DAR). Het document is gebaseerd op een eerder geschreven [GPSA](#), vergeleken

met deze GPSA is de scope beperkter, o.a. het aansluiten van de bronsystemen, of het digitaliseren van documenten is geen onderdeel van het project. Het is de vertaling van de algemene principes en beleidslijnen naar dit specifieke onderwerp, en bestaat uit concrete standaarden, normen en richtlijnen, en de modellen die hierbij gehanteerd worden. Het legt de belangrijkste ontwerpkeuzes vast met betrekking tot digitaal archiveren binnen de Rechtspraak.

2. Context en scope

Context

De Rechtspraak is door de Archiefwet zorgdrager voor een goede informatiehuishouding en daarmee verplicht 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. Hierin streeft de Rechtspraak het principe van ‘duurzame toegankelijkheid’ na.

‘Duurzaam toegankelijk’ betekent dat informatie vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zolang als noodzakelijk. Hierbij wordt rekening gehouden met aspecten van openbaarheid en privacy. Duurzaam betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard. Dit is niet alleen nodig voor de informatie die binnen de werkprocessen verwerkt wordt, maar ook van de contextinformatie (zoals wie, wat, waarom, waar, etc.)

Archiveren by design

Archiveren vereist dat de werkprocessen en de daarbij gebruikte informatiesystemen (de werksystemen) daarop ingericht worden. Zodanig dat de informatie die voortkomt uit de werkprocessen duurzaam toegankelijk is. De maatregelen die daarvoor nodig zijn bepaal je het beste op het moment dat de werksystemen gekocht, gebouwd, aangepast of afgeschaft worden. We noemen dit ‘archiveren by design’.

Wanneer een organisatie archivering by design consequent toepast wordt alle informatie geleidelijk duurzaam toegankelijk. Maar dat kan voor bestaande werksystemen bij de Rechtspraak lang duren als er geen plannen zijn voor vervanging of aanpassingen. Of als de organisatie het systeem niet kan aanpassen. Voor deze systemen is het verstandig om te bepalen of de duurzame toegankelijkheid een onacceptabel risico vormt. Zo ja, overweeg dan welke maatregelen genomen kunnen worden. Bijvoorbeeld om cruciale informatie te verplaatsen naar een archiefsysteem, of mogelijk toch aanpassingen aan het werksysteem voor te stellen.

Document lifecycle

Document lifecycle verwijst naar de verschillende fases die een document tijdens zijn gehele ‘leven’ doorloopt: van creatie tot verwijdering of archivering. Het is een manier van documentbeheer, waarbij chronologisch gewerkt wordt.



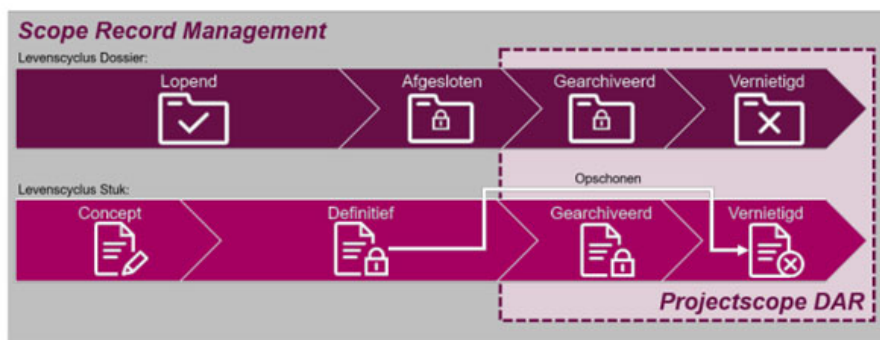
Binnen de Rechtspraak worden elke dag documenten aangemaakt. Deze documenten kunnen bedoeld zijn voor verder intern gebruik, of om naar ketenpartijen gestuurd te worden. De meeste documenten doorlopen in grote lijnen dezelfde fases:

1. Creatie: in deze fase wordt het document opgemaakt. Het document wordt altijd gecreëerd door één gebruiker. Deze persoon zorgt voor de aanmaak (de 'geboorte') van het document, ook al is het nog maar een eerste opzet.
2. Organisatie en classificatie: zodra een document gecreëerd is, moeten er metadata aan worden toegevoegd. Deze extra data geven context aan het document. Metadata zorgen er ook voor dat het document op elk moment eenvoudig kan worden teruggevonden in het documentbeheersysteem.
3. Samenwerking en revisie: bij veel documenten zijn verschillende personen betrokken. Zij leveren hun eigen bijdrage aan het document, of reviseren het werk van anderen. Soms moet er in real-time samengewerkt worden of is er een strikte volgorde waarin een document van de ene gebruiker naar de andere gestuurd wordt.
4. Verificatie en gebruik: zodra een document een eindversie bereikt heeft, wordt er nog een laatste check op uitgevoerd. Wanneer het document goedgekeurd wordt, kan het gebruikt of opgestuurd worden. Dit betekent niet dat het document nooit meer bewerkt kan worden. Veel (interne) documenten krijgen 'instructies' mee in het Document Management System DMS, zoals bijvoorbeeld een revisie. Het DMS geeft hiervoor een notificatie, en het document gaat weer terug naar fase 3. Veel regels met betrekking tot de revisie van documenten komen rechtstreeks voort uit bepaalde ISO-normen.
5. Archivering of verwijdering: het levenseinde van een document valt samen met de beslissing om het te archiveren (retentie) of permanent te verwijderen. Deze keuze wordt beïnvloed door veel verschillende factoren, waaronder de Archiefwet en ook de Algemene Verordening Gegevensbescherming (AVG). Wanneer een document aan zijn levenseinde is, wordt dit meestal aangegeven door het DMS zelf. De vervaldatum werd namelijk ingesteld bij de publicatie van het document. Dit kan manueel of kan geautomatiseerd worden.

Scope

Waar nu papieren dossiers na behandeling worden gearchiveerd in dozen, moet er bij digitale dossiers al bij de start (archiveren-by-design) van de behandeling rekening worden gehouden met het archiveren. Het is daarom van belang dat de duurzame toegankelijkheid van informatie vanaf ontvangst of creatie ook technisch wordt geborgd. Hierom is bepaald dat de scope van het project zich voorlopig beperkt tot het digitale zaakdossiers (digital born) . Het project richt zich daarbij op de randvoorwaarden en vereisten om digitale dossiers te kunnen archiveren. De realisatie van beide is geen onderdeel van de scope. Het werkdoosier (DWD) is buiten scope, omdat het werkdoosier geen archiefmateriaal bevat.

De document lifecycle en record management richten zich op de volledige lifecycle van een document dit is een bredere scope dan waar het project DAR zich mee bezig houdt. In onderstaande figuur is aangegeven welk deel van record management binnen het DAR project valt.



Scope binnen de rechtspraak

Aangezien de archiefwet 1995 van toepassing is op alle overheidsdossiers en -archieven wordt de scope van het project DAR van toepassing op alle domeinen:

- Civiel;
- Bestuur;
- Straf;
- Toezicht;
- Bedrijfsvoering.

Naast de domeinen is de archiefwet ook van toepassing op de ondersteunende diensten en applicaties.

Businessdoelen

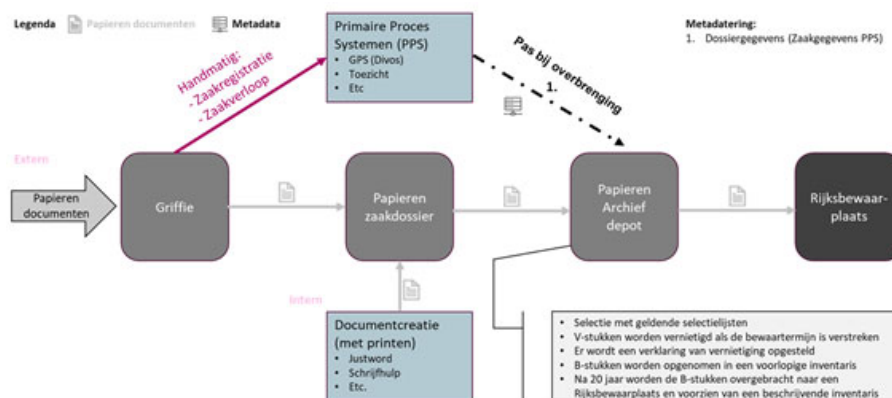
Het verder digitaliseren van de Rechtspraak betekent dat archivering zich fasegewijs verplaatst van papier naar digitaal. Bij archiveren wordt informatie voor korte of langere tijd veilig gesteld,

hetgeen bij wet verplicht is. Overheidsorganen zijn verplicht de onder hen berustende archiefbescheiden (informatieobject) in goede, geordende en duurzaam toegankelijke staat te brengen en te bewaren. De Archiefwet 1995 is een van de wetten voor de informatievoorziening en informatiebeheer van de Nederlandse overheid. Ze is in samenhang te lezen, te begrijpen en te implementeren met bijvoorbeeld de Wet openbaarheid van Bestuur, de Algemene Verordening Gegevensbescherming en de Wet strafvorderlijke gegevens. Wat de Rechtspraak moet archiveren en welke bewaartermijn daaraan gekoppeld is, staat beschreven in het [Basisselectiedocument](#). Een bewaartermijn is de termijn dat een informatieobject bewaard moet blijven, waarna de zorgdrager een informatieobject moet vernietigen dat voor vernietiging in aanmerking komt. Het kan ook voorkomen dat informatieobjecten blijvend bewaard moeten worden. Die informatieobjecten moeten op papier of digitaal overgedragen worden naar het Nationaal Archief.

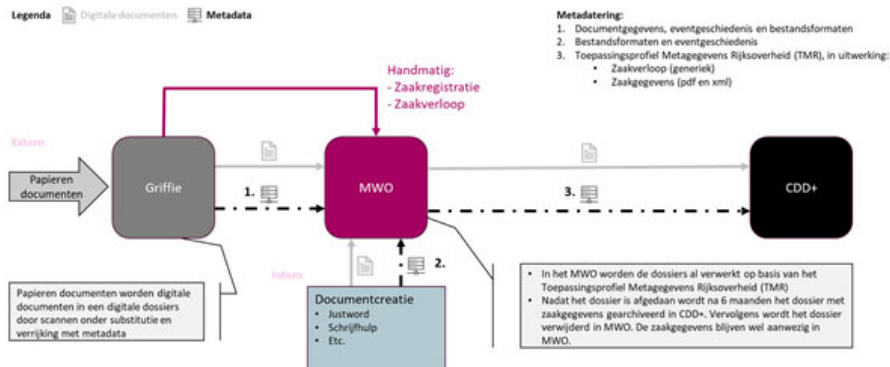
Huidige situatie

Archiveren vanuit Primaire Proces Systemen (PPS)

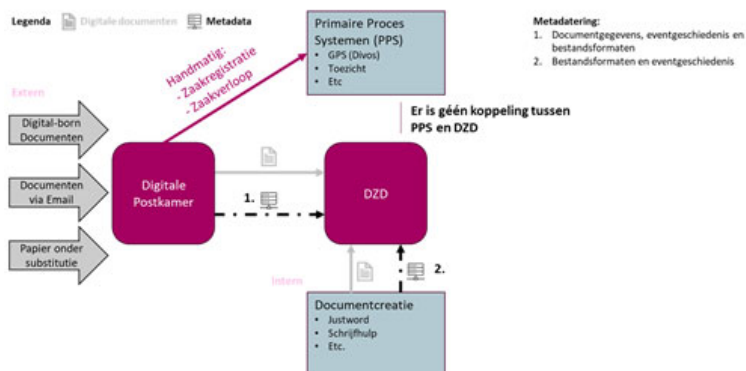
De gerechten zijn zorgdragers voor hun archieven. Tot op heden bestaat het archief hoofdzakelijk uit fysieke, lees papieren, informatieobjecten. Er zijn weliswaar systemen, de zogenaamde primaire processystemen, waarin gegevens van zaken worden vastgelegd, doch omtrent de bewaring van de informatieobjecten uit deze systemen is nu alleen vastgelegd dat slechts een set met kerngegevens behoeft te worden bewaard. In de selectielijst is vastgelegd welke informatieobjecten voor blijvende bewaring moeten worden overgeheveld naar een regionaal c.q. naar het nationaal archief.



Er zijn op dit moment twee zaaksystemen waarin ook digitale dossiers functioneren, als vervanger van de papieren dossiers. Dat betreft GPS in strafzaken en MWO in Asiel-bewaringszaken. Ten aanzien van GPS bestaat een gezamenlijke verantwoordelijkheid van OM en Rechtspraak voor de digitale archivering van de in GPS opgenomen digitale dossiers. Feitelijk is op dit onderdeel nog geen praktijk van digitale archivering ingericht. Voor MWO worden de dossiers digitaal opgeslagen in CDD+, het e-depot van Justid.



De Rechtspraak werkt aan de digitalisering van zaakstromen met als hoofddoel om een eenvoudige digitale toegang te realiseren voor procespartijen en procesvertegenwoordigers. De realisatie van het project rondom Digitale Toegang (DT) moet hier voor zorgen. In de Digitale Postkamer komen processtukken van externe partijen binnen. Alle documenten worden opgeborgen in een Digitaal Zaaksdossier (DZD). Voorafgaand aan het gebruik van de Digitale Postkamer, moet de zaak eerst geregistreerd worden in de huidige systemen zoals Berber en Civiel. Op dit moment kan er geen archivering plaatsvinden van documenten in de gedigitaliseerde zaakstromen van DT. In tegenstelling tot MWO is er geen koppeling met CDD+ en zijn de aansluitvoorwaarden van CDD+ niet meegenomen bij de inrichting.



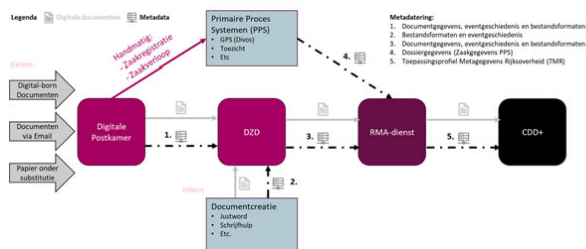
Naast het archiveren van de gegevens uit de primair proces systemen moeten er ook gegevens uit andere proces systemen gearcheeerd worden denk hierbij aan HRM, of financiële systemen, maar ook aan email en websites. Een verschil met het primaire proces is dat de informatie in deze systemen niet altijd onderdeel is van een dossier, of op een andere manier is gestructureerd. Op dit moment vindt archivering plaats in het systeem zelf, met uitzondering van de web content. De web content wordt gearcheeerd met behulp van [archiefweb](#). Archiefweb wordt overheids-breed gebruikt voor het archiveren van de web content en zal ook binnen de Rechtspraak voor dit doel ingezet blijven worden.



Toekomstige situatie: Conceptueel model

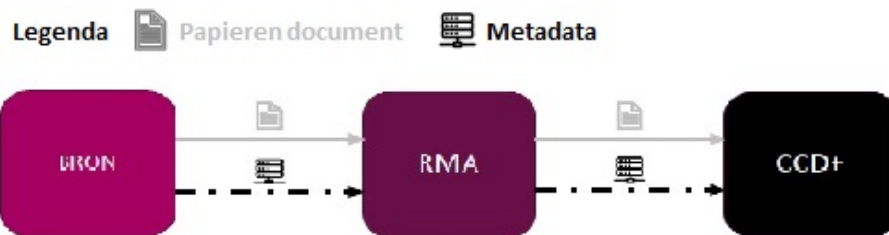
Archiveren Primaire Proces Systemen (PPS)

Om de mogelijkheid aan te bieden om alle digitale zaakdossiers (digital born) te archiveren conform wettelijke vereisten, moet er een generiek archiefsysteem binnen de Rechtspraak worden gerealiseerd. De zaakdossiers bevatten zowel de gegevens uit de zaakstroom als de bijbehorende documenten en de voor de het archiveren relevante log informatie. Dit is mogelijk door het in gebruik nemen van een dienst met een Record Management Applicatie (RMA). Met een RMA wordt automatische archieffunctie geïntegreerd in de werkprocessen. Deze automatisering maakt het ook mogelijk om ieder moment aan te tonen hoe de werkzaamheden zijn verricht. Een RMA stelt in staat om op een juiste manier, conform de wettelijke kaders, een elektronische archief op te bouwen en te beheren. De RMA wordt aangesloten op het digitale zaakdossier (DZD) van DT en in lijn met MWO worden de dossiers digitaal opgeslagen in CDD+, het e-depot van Justid.



Archiveren ondersteunende diensten

Voor de ondersteunende diensten wordt dezelfde oplossing voorgesteld om digitale content te archiveren conform de wettelijke richtlijnen. Het eerder beschreven centrale zal naast de zaakdossiers ook de mogelijkheid moeten bieden om gemetadateerde documenten uit andere stromen te kunnen archiveren. Dit stelt als extra eis dat het systeem naast gestructureerde data ook ongestructureerde data moet kunnen ontvangen. Van ieder proces wordt vastgesteld, of de betreffende gegevens centraal gearchiveerd gaan worden in het nieuwe archief systeem. Indien een stroom op een andere manier gearchiveerd wordt, zoals bijvoorbeeld web content, moet dit los worden opgenomen in een bijbehorend architectuur document met de bijbehorende rationale.



Uitgangspunten

- Vanuit het domein bedrijfsvoering is de strategie dat er voor standaard software een SaaS tenzij strategie gevoerd wordt.

3. Grondslagen

Geef aan welke grondslagen van toepassing zijn

- Beleidskaders
- Wet- en regelgeving
- Normen en standaarden

Geef aan of er nog speciale overwegingen met betrekking tot basisprincipes zijn.

Beleidskaders

- Loggingbeleid: Voor het archiveren is er sprake van verschillende logs, deze moeten op een correcte manier worden verzameld en opgeslagen;
- Cloudbeleid: Voor digitaal archiveren is het de bedoeling om een SaaS product uit te vragen. Dit product moet voldoen aan het cloud beleid.

Wet en regelgeving

- [Archiefbesluit 1995](#)
- [Archiefregeling](#)
- [Archiefwet 1995](#)
- [Wet Justitiele en strafvordelijke gegevens](#)
- [AVG](#)
- [Uitvoeringswet AVG](#)
- [Primair proces van 'de Rechtspraak', selectielijst voor de waardering van alle rechtszaak gebonden stukken, ontvangen of opgemaakt vanaf \(1985\) 2005](#)

Normen en standaarden

- [Baseline Informatiebeveiliging Overheid \(BIO\)](#)
- [Minimum norm rubricering Digitale Informatie](#)

IVO beleid en strategie

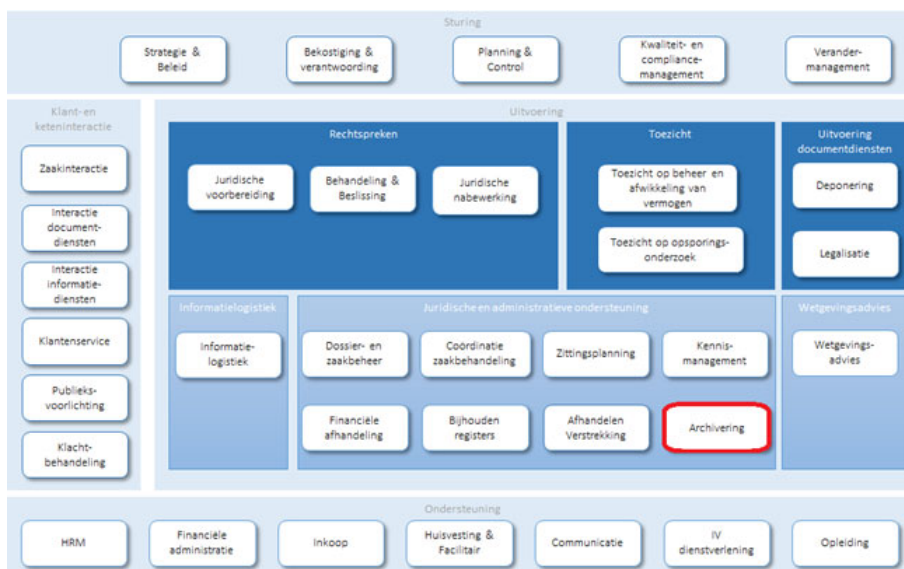
4. Businessarchitectuur

Binnen het project DAR definiëren we het Digitaal Archief als:

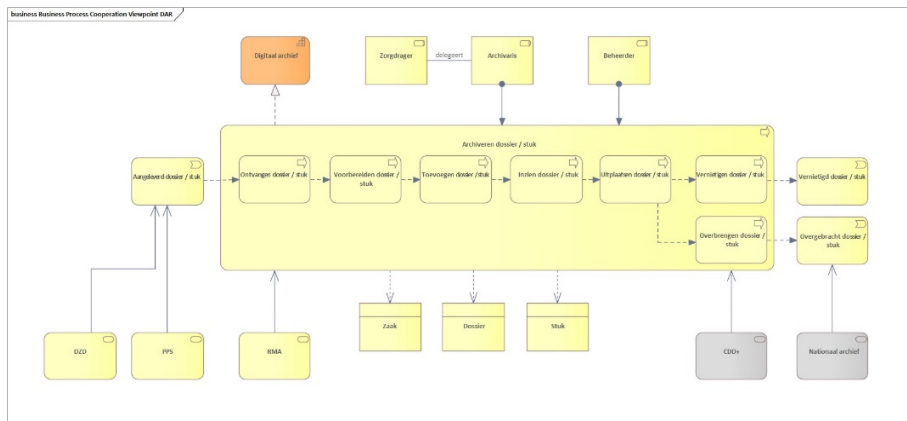
Het geheel aan diensten, processen en systemen dat tot doel heeft digitale archiefbescheiden te bewaren, ontsluiten en vernietigen conform wet- en regelgeving.

Het Digitaal Archief is volgens de definitie een capability en niet een systeem of dienst op zich.

Archiveren is onderdeel van de bedrijfsfunctie Juridische en administratieve ondersteuning



Het werkproces Archiveren dossier bestaat uit de volgende stappen, wordt ondersteund door de gerelateerde IV diensten en vallen onder verantwoordelijkheid van de gerelateerde rollen:



Processtappen	Omschrijving
Ontvangen dossier / stuk	Dit proces maakt het mogelijk om binnen de rechtspraak te archiveren stukken samen te brengen op een centrale plaats.
Voorbereiden dossier	Binnen dit proces wordt het dossier geschoond, gestructureerd en geclassificeerd indien dat niet op een andere plek al is gedaan
Toevoegen stuk	Dit proces heeft tot doel zaken op te nemen binnen het Digitaal Archief en/of stukken toe te voegen aan bestaande zaken. Stukken kunnen gestructureerd zijn.
Inzien dossier / stuk	Dit proces maakt het mogelijk voor partijen om zaken en stukken in het Digitaal Archief (na autorisatie) in te zien. In geen enkel geval is anonieme toegang mogelijk.
Uitplaatsen dossier / stuk	Verzendt zaakdossiers en stukken naar een andere archiefdienst en wist vervolgens het betreffende dossier met stukken uit het Digitaal Archief. De huidige zorgdrager blijft eindverantwoordelijk.
Overbrengen dossier / stuk	Verzendt zaakdossiers en stukken naar een andere archiefdienst en wist vervolgens het betreffende dossier met stukken uit het Digitaal Archief. De ontvanger wordt de nieuwe zorgdrager.
Vernietigen dossier / stuk	Na het verstrijken van de bewaartermijn vervalt de wettelijke grondslag om de archiefinhoud te bewaren en toegankelijk te maken. Stukken en bijbehorende zaakgegevens worden daarom vernietigd, tenzij d.m.v. macroselectie is aangegeven dat dossiers integraal bewaard moeten worden.

Betrokkenen

Op basis van deze indeling kunnen we een aantal conceptuele rollen definiëren die gebruik maken van het Digitaal Archief. Deze zijn weergegeven in het volgende viewpoint:

Rol	Omschrijving
Zorgdrager	Degene die bij of krachtens wet belast is met de zorg voor archiefbescheiden.
Archivaris	Ambtenaar die met het beheer van een archief belast is (bron van Dale)
Beheerder	Zorgt voor het technisch beheer van het Digitaal Archief. Voor zover delen van het Digitaal Archief worden uitbesteed aan derde partijen kan deze rol ook door een medewerker van deze partijen worden ingevuld.

Interne betrokkenen

In de Archiefwet 1995 is vastgelegd dat de zorgdrager de hoogst bestuurlijke verantwoordelijke is voor de informatie in haar/ zijn organisatie. De zorgdrager van een archief is en blijft hierdoor verantwoordelijk voor alle dossiers en stukken die zich daarin bevinden, tot het moment dat deze aan een andere partij worden overgedragen. Een voorbeeld van een zorgdrager is een gerechtsbestuurder.

Dat wil niet zeggen dat de zorgdrager alle processen zelf hoeft uit te voeren of dat iedere zorgdrager hiervoor unieke voorzieningen moet treffen. Integendeel, het project DAR heeft juist tot doel om centraal generieke voorzieningen te realiseren, in combinatie met een beheerorganisatie om deze te ondersteunen. Het staat de zorgdrager niet vrij om hiervan af te wijken.

Gedelegeerd betrokkenen

Daarnaast zijn reeds twee partijen buiten IVO Rechtspraak voorzien als aanbieders van archiefdiensten:

- **Justid**
Leverancier van de dienst Centraal Digitaal Depot (CDD+), een e-Depot dat zich specialiseert in het conform wet- en regelgeving duurzaam bewaren, beschikbaar maken en uiteindelijk vernietigen van dossiers en stukken. Hierbij is sprake van uitplaatsing, waarbij de oorspronkelijke zorgdrager eigenaar blijft.
- **Nationaal Archief**
Overheidsdienst die zich specialiseert in het conform wet- en regelgeving bewaren en beschikbaar maken van archiefwaardig materiaal. Hierbij is sprake van overdracht, waardoor het Nationaal Archief de nieuwe zorgdrager wordt.

Externe betrokkenen

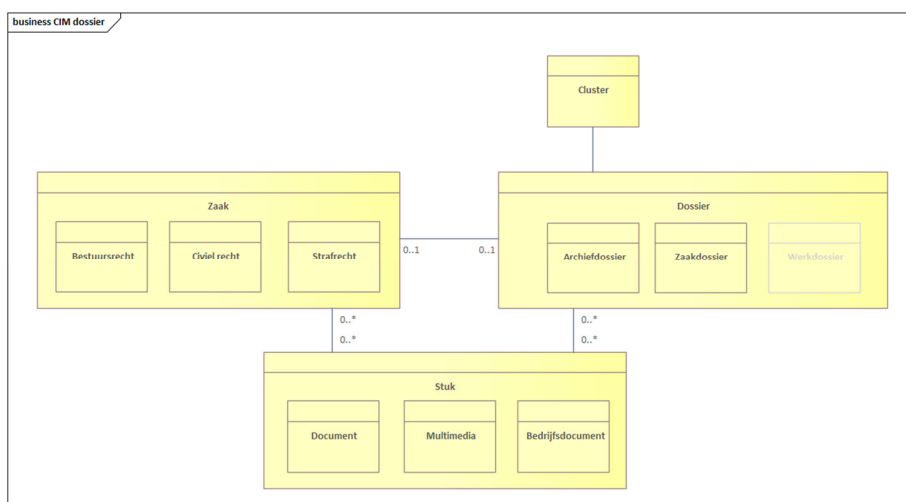
Het Digitaal Archief wordt als een dienst aangeboden. Wet- en regelgeving schrijft voor dat de afnemers van deze dienst (partijen en vertegenwoordigers) in staat moeten zijn stukken en/of dossiers uit het Digitaal Archief op te vragen. Of deze verzoeken ook gehonoreerd worden is afhankelijk van een aantal factoren, waaronder:

- Beschikbaarheid van de opgevraagde informatie op basis van bewaartermijnen
- Toegankelijkheid van de opgevraagde informatie op basis van classificatie

Het project DAR zal voorzien in een proces waarmee dergelijke verzoeken beoordeeld kunnen worden en waarmee (na goedkeuring en autorisatie) de informatie verstrekt kan worden. Het gaat hierbij om informatie die digitaal gearhiveerd is.

5. Informatie-architectuur

Op basis van het CIM zijn de volgende informatieobjecten herkend op hoofd niveau.



De benaming van deze entiteiten is afkomstig uit het Conceptueel Informatie Model (CIM). Het Conceptueel Informatie Model (CIM) beschrijft de gegevens die de Rechtspraak beheert in een logische onderlinge samenhang.

De detail uitwerking is vastgelegd in het [Logisch Gegevens Model \(LGM\)](#). In dit model worden ook de verplichte velden vastgelegd. Dit zijn de eisen die aan te archiveren stukken en dossiers zijn gesteld. In het SAD wordt de laatste versie van het LGM opgenomen.

De relatie van deze informatieobject op in wet- en regelgeving genoemde begrippen wordt in onderstaande tabel weergegeven:

Informatieobject(subtype)	Informatieobject(supertype)	Toelichting
Cluster		Geeft de samenhang tussen dossiers weer voor bijvoorbeeld de behandeling.

Informatieobject(subtype)	Informatieobject(supertype)	Toelichting
Zaak		Omschrijft de gegevens van de zaak / zaken waar een dossier betrekking op heeft. Per zaak kunnen meerdere dossiers bestaan. Ook zaakgegevens worden gearcheveerd.
Bestuursrecht	Zaak	Rechtspraak door onafhankelijke rechter in geschillen die niet uit burgerlijke rechtsbetrekkingen zijn ontstaan (art. 112 lid 2Gw)
Civiel recht	Zaak	Rechtsvordering waardoor een rechtsgeding van het burgerlijk recht, in tegenstelling tot het strafrecht, in gang wordt gezet.
Strafrecht	Zaak	Het geheel van regels betreffende de strafbaarstelling van bepaalde feiten en de daarop gestelde straffen (Buiten scope)
Dossier		Verzameling papieren, bundel stukken
Archiefdossier	Dossier	Opgeschoond zaakdossier t.b.v. archiveren
Zaakdossier	Dossier	Alle informatie (stukken + gegevens) die in principe alle partijen kunnen inzien
Werkdossier	Dossier	Alle informatie (eventueel over meerdere zaken) die nodig is om juridische zaakbehandeling te doen. Persoonlijk dossier voor ieder die met het zaakdossier werkt (Buiten scope, omdat het werkdossier geen informatie bevat die gearcheveerd moet worden)
Stuk		Een stuk is vastgelegde informatie of vastgelegd object dat als een eenheid kan worden behandeld.

Relatie tussen de modellen

Door Justid is voor het Centraal Digitaal Depot (CDD+) een relatie gelegd tussen de eigen binnen Justid geldende entiteiten en het Toepassingsprofiel Metadata Rijk (TMR).

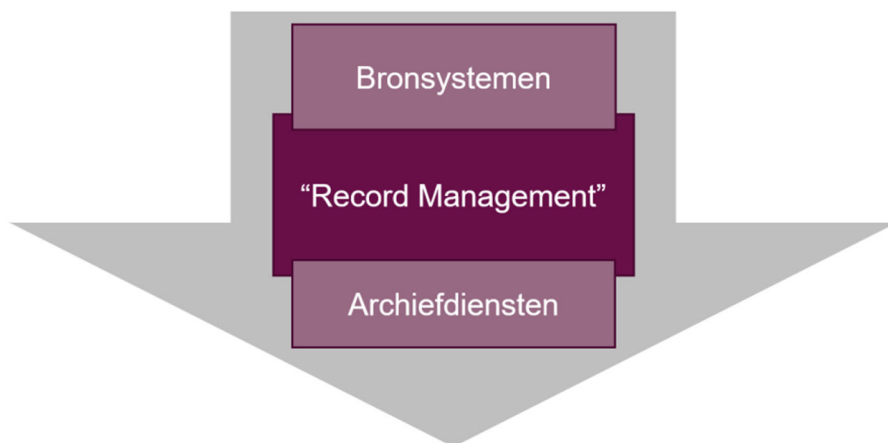
Binnen IVO Rechtspraak wordt het Logisch Gegevens Model (LGM) gehanteerd om entiteiten met bijbehorende metadata te beschrijven. Binnen IVO Rechtspraak is een set met metadata aanwezig die minimaal beschikbaar moet zijn om een dossier op een correcte wijze te kunnen archiveren.

Het project DAR zal intern het LGM hanteren. De entiteiten van het LGM en CDD+/TMR aan elkaar worden gerelateerd en op elkaar afgebeeld, in overleg met de Informatie Architecten van IVO Rechtspraak. Waar nodig zal het LGM worden uitgebreid om dit mogelijk te maken. Deze definities zullen vervolgens in beheer worden genomen door de Informatie Architecten.

Op basis van de vastgestelde relatie wordt een lijst samengesteld met daarin de minimale velden om een informatieobject goed te kunnen archiveren. Deze lijst met minimale gegevens is in de bijlage opgenomen. ([MetadataMapping SOS en DAR.xlsx](#)). In het SAD staat de laatste versie van de mapping.

6. Applicatie-architectuur

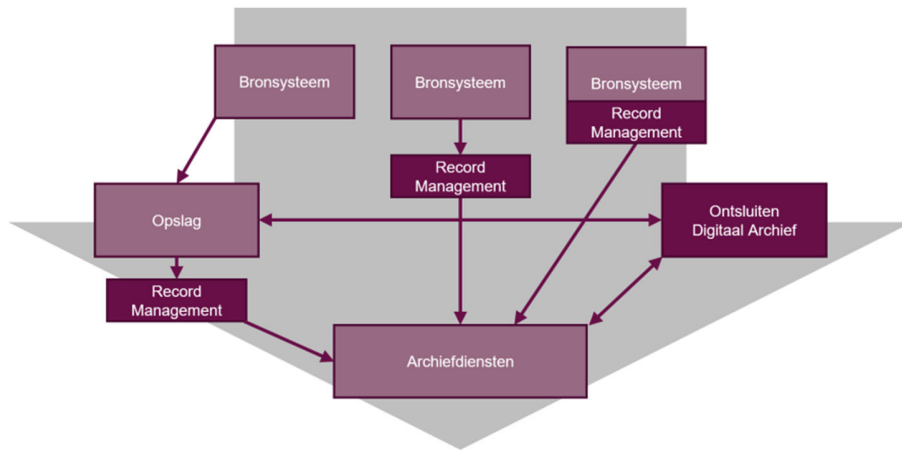
Wanneer we het Digitaal Archief in helicopterview bekijken, dan ontstaat op basis van de voorgaande hoofdstukken het onderstaande beeld:



Vanuit bronsystemen die zaakgegevens, dossiers en/of stukken bevatten worden de functionaliteiten die onder de noemer "Record Management" vallen uitgevoerd. Uiteindelijk worden de archiefbescheiden overgedragen aan één of meer archiefdiensten.

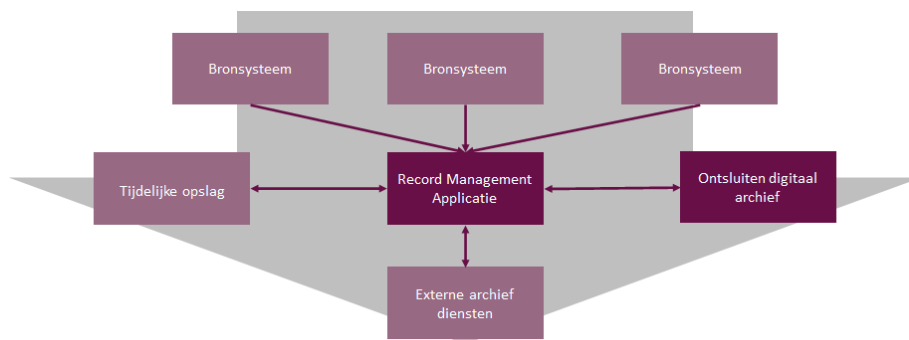
Bronsystemen zijn echter niet uniform en bieden ook niet allemaal de mogelijkheid om Record Management functionaliteiten te gebruiken of toe te voegen. In sommige gevallen is de

benodigde functionaliteit aanwezig in het bronsysteem of kan deze worden toegevoegd. In andere gevallen is een aparte component nodig om dit te realiseren. Een dergelijk scenario brengt met zich mee dat business logica en Record Management functionaliteiten op meerdere plaatsen worden geïmplementeerd, met alle risico's van inconsistenties en verhoogde onderhoudskosten van dien.



In dit scenario zouden bronsystemen bovendien verantwoordelijk zijn voor hun eigen koppelingen met (externe) archiefdiensten, met dezelfde risico's.

Het project Digitaal Archiveren Rechtspraak gaat daarom uit van onderstaande aanpak, waarbij Record Management functionaliteiten op een centrale plaats als dienst worden aangeboden.

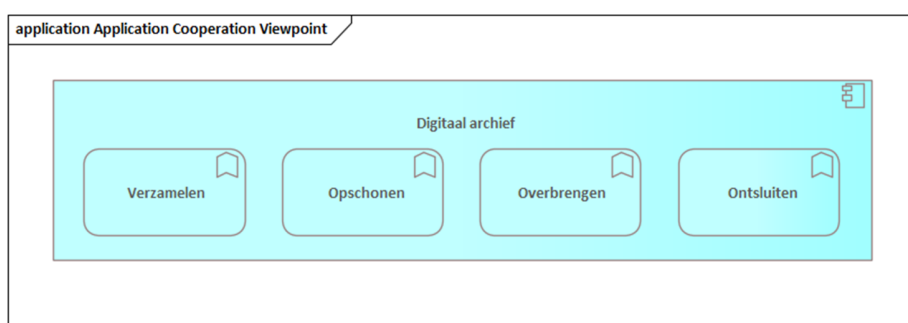


In de bovenstaande figuur wordt het Record management aangeboden door een centrale applicatie. Hierin worden zaakgegevens, dossiers en stukken op uniforme wijze verzameld uit de verschillende bronsystemen. Om in staat te zijn deze informatie te verzamelen is tijdelijke opslag nodig. Ook kan hier worden geverifieerd of dossiers volledig zijn verkregen uit de bronsystemen. Na een geslaagde overdracht worden zaakgegevens en stukken uit de bronsystemen gewist. De bronsystemen zorgen zelf voor de overdracht naar het digitaal archief. Dit moet worden opgenomen in de SAD's van de verschillende bronsystemen.

Dossiers in het digitaal archief kunnen door de archivaris worden gestructureerd. Archivarissen geven in deze fase ook aan welke dossiers integraal bewaard moeten worden (zgn. macroselectie).

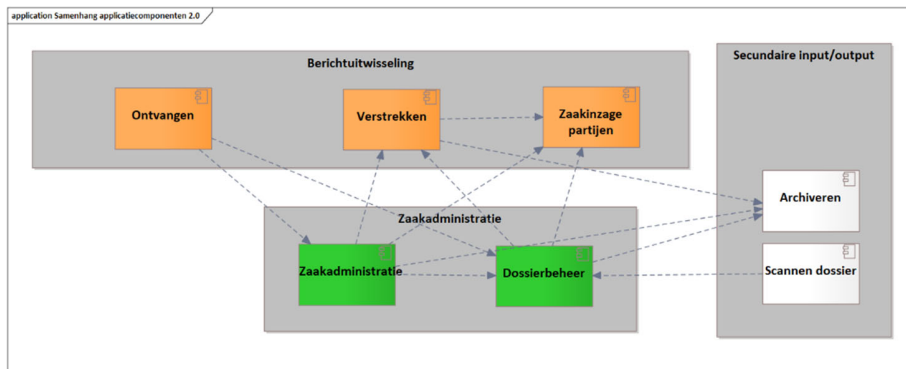
Op basis van selectielijsten wordt bepaald of, en zo ja hoe lang, stukken en zaakgegevens bewaard moeten blijven, waarna de stukken worden overgeplaatst naar de externe archief diensten.

Om aan de verplichting van het ontsluiten van archieven te kunnen voldoen maakt ook deze voorziening onderdeel uit van het Digitaal Archief. Hierbij wordt niet alleen de opslag van IVO Rechtspraak doorzocht, maar ook die van eventuele externe archiefdiensten. De hoofdfunctionaliteiten van de dienst zoals opgenomen in de REA

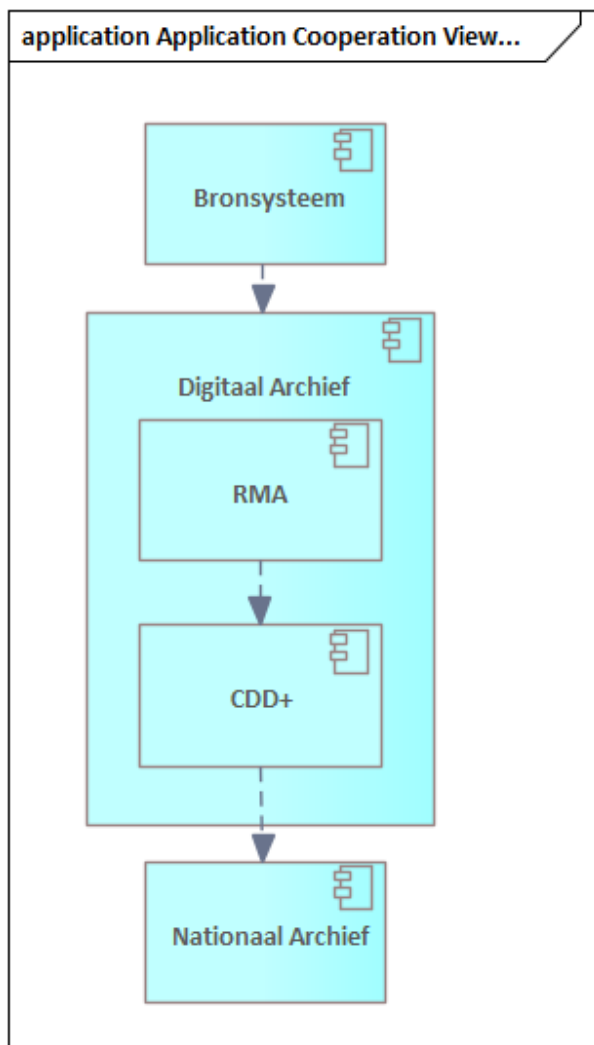


Component functie	Omschrijving
Verzamelen	Dit proces maakt het mogelijk om binnen de rechtspraak te archiveren stukken samen te brengen op een centrale plaats.
Opschonen	Dit proces zorgt dat stukken na het verlopen van de bewaartermijn conform het Basisselectiedocument uit het Digitaal Archief worden verwijderd en vernietigd of overgedragen aan het Nationaal Archief. Wanneer een zaak geen stukken meer bevat zal ook de zaak zelf verwijderd en vernietigd worden.
Overbrengen	Dit proces zorgt er voor dat er binnen de rechtspraak stukken die voor lange termijn opgeslagen moeten worden in een archief dienst onder gebracht worden. Het overbrengen van de stukken en de dossiers wordt de ontvanger de zorgdrager van de ondergebrachte stukken.
Ontsluiten	Dit proces zorgt er voor dat de archief dossiers beschikbaar zijn. Het maakt het mogelijk om in het archief te zoeken en dossiers op te vragen.

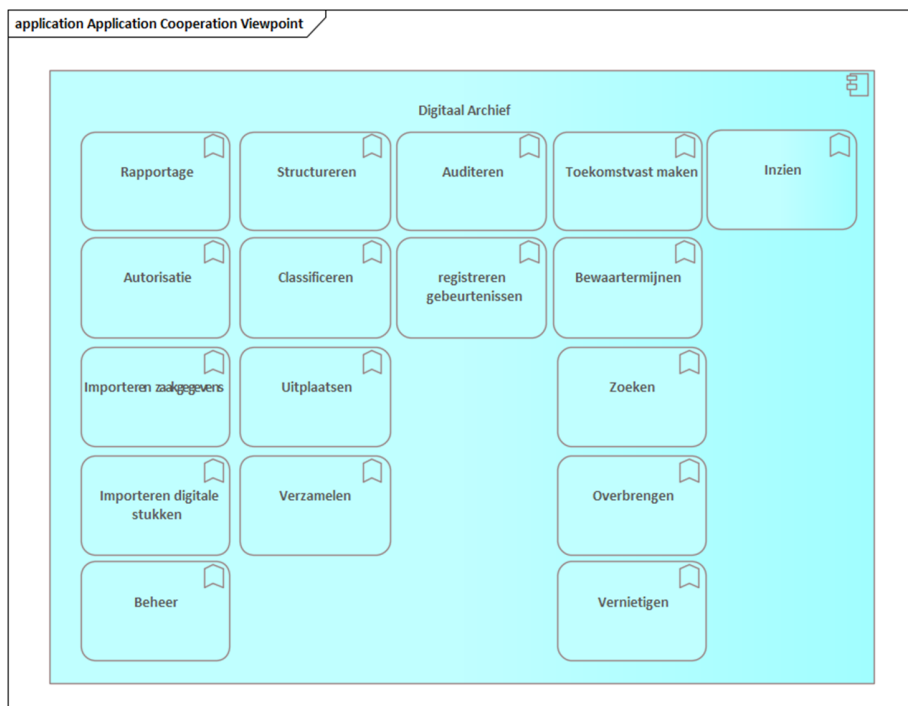
Op dit moment maakt een Record Management Applicatie (RMA) geen onderdeel uit van het applicatielandschap van IVO Architectuur. Binnen de REA wordt het digitaal als volgt geplaatst



Het Digitaal archief bestaat uit een aantal bouwblokken die samen de archief functie gaan ondersteunen



Onderstaande figuur geeft schematisch de functionele bouwblokken voor het archief weer om tot een archief oplossing te komen. Het figuur geeft dus niet weer waar de functionaliteiten zijn belegd.



Bouwblok	Omschrijving
Importeren zaakgegevens	Maakt het mogelijk om via het import koppelvlak digitale zaakgegevens op uniforme wijze te importeren uit verschillende bronsystemen.
Importeren digitale stukken	Maakt het mogelijk om via het import koppelvlak digitale stukken op uniforme wijze te importeren uit verschillende bronsystemen.
Autorisatie	Het herkennen van gebruikers (authenticatie), bepalen welke taken deze gebruikers binnen het digitaal archief mogen uitvoeren (autorisatie) en vervolgens garanderen dat dit de enige taken zijn die de gebruiker uit kan voeren. Bij voorkeur door het toekennen van rollen aan gebruikers en een koppeling aan de generieke IAM oplossing.
Rapportage	Maakt het mogelijk om rapportages te verstrekken over capaciteit, gebruik en operatie van het Digitaal Archief met als doel verantwoording af te leggen.
Beheer	Onderdeel dat het mogelijk maakt om het Digitaal Archief te configureren, beheren en monitoren. Omvat o.a. het configureren van opslag (storage) om zaakgegevens en stukken te bewaren.

Bouwblok	Omschrijving
Tijdelijke opslag	Opslag waar gegevens die het digitaal archief verzamelt en structureert kunnen worden bewaard. Omvat het bewaren van zaakgegevens en stukken op een zodanig medium dat de gegevens en stukken niet onbedoeld verloren kunnen gaan. Doordat de opslag tijdelijk is zal het bronformaat niet gewijzigd hoeven worden. Dit is niet hetzelfde als de opslag voor toekomst vaste ontsluiting die o.a. de externe archiefdiensten bieden.
Auditeren	Stelt zorgdragers in staat om aan te tonen dat het Digitaal Archief voldoet aan wet- en regelgeving m.b.t. security, privacy en bewaartermijnen.
Registreren gebeurtenissen	Maakt het mogelijk om verschillende gebeurtenissen (zoals opnemen, inzien, vernietigen, etc. van alle soorten archiefbescheiden) te definiëren en per gebeurtenis vast te leggen wanneer dit plaats heeft gevonden, wie de opdrachtgever is en op welke content van het Digitaal Archief de gebeurtenis betrekking heeft. Het doel van deze registratie is om verantwoording te kunnen afleggen over het gebruik van het Digitaal Archief.
Structureren	Maakt het mogelijk om archieven, dossiers, mappen en stukken te ordenen binnen het Digitaal Archief wanneer deze structuur nog niet digitaal aanwezig is in bronsystemen. De verantwoordelijkheid ligt bij de zorgdrager, die dit aan een centrale of decentrale functionaris kan delegeren.
Bewaartermijnen	Maakt het mogelijk om per type stuk (in combinatie met zaakstroom) een bewaartermijn te definiëren. Hierbij is het [BSD ZM] leidend. De bewaartermijn van een zaakdossier is het maximum van de bewaartermijnen van de daarin opgenomen stukken.
Classificeren	Maakt het mogelijk om stukken te herkennen als een bepaald type, bij voorkeur op basis van zaakstroom en metadata. Stelt archivarissen in staat om macroselectie toe te passen, waarmee wordt aangegeven welke dossiers integraal en/of voor onbepaalde tijd bewaarde moeten worden.
Zoeken	De mogelijkheid om het gehele Digitaal Archief (incl. archiefdiensten) te doorzoeken op verschillende kenmerken met als doel zaakdossiers en stukken te vinden. Zoeken moet in ieder geval mogelijk zijn op zaaknummer, trefwoorden en metadata.
Toekomstvast maken	Zorgt dat archiefbescheiden zodanig worden bewaard dat deze gedurende de gehele bewaartermijn ontsloten kunnen worden. Kan betekenen dat een stuk wordt geconverteerd naar een ander formaat, bij voorkeur via een generieke dienst.

Bouwblok	Omschrijving
Overbrengen	Verzendt zaakdossiers en stukken naar een andere archiefdienst en wist vervolgens het betreffende dossier met stukken uit het Digitaal Archief. De ontvanger wordt de nieuwe zorgdrager. Is niet hetzelfde als het koppelvlak, aangezien dit slechts een gestandaardiseerde interface levert.
Uitplaatsen	Verzendt zaakdossiers en stukken naar een andere archiefdienst en wist vervolgens het betreffende dossier met stukken uit het Digitaal Archief. De huidige zorgdrager blijft eindverantwoordelijk. Het verschil met overbrengen ligt functioneel in verantwoordelijkheden en rechten na verzenden.
Vernietigen	Wist een dossier en/of stukken uit het Digitaal Archief, na het verlopen van de bewaartermijn ongeacht in welk deel van het Digitaal Archief deze zijn opgeslagen. De gebeurtenis wordt gelogd.
Inzien	Maakt het mogelijk om zaakgegevens en/of stukken te raadplegen en verstrekken.

In de eerste fase wordt onderzocht welke functionaliteiten in het Record Management worden opgenomen en welke functionaliteiten van CDD+ gebruikt worden. Het gevolg hiervan is dat deze functionaliteiten niet meer in het RMA hoeven te worden opgenomen en er dus een dunne tussenlaag ontstaat tussen de bronsystemen en het CDD+.

Uitgangspunten

Binnen het digitaal archief wordt onderscheid gemaakt tussen core en fallback functionaliteiten.

Bij de fallback functionaliteiten heeft het de voorkeur dat deze op een plaats binnen het applicatie landschap worden belegd. Binnen het RMA worden deze functionaliteiten alleen aangeboden aan de stromen die hier geen voorziening voor hebben. Het structureren van archief bescheiden wordt alleen mogelijk gemaakt als de archiefbescheiden ongestructureerd worden aangeboden. Indien alle stromen de functionaliteit buiten het RMA kunnen gebruiken dan hoeft deze functionaliteit niet in het RMA gerealiseerd te worden.

Op basis van de classificatie van stukken en de selectielijsten wordt bepaald hoe lang een stuk of zaakdossier (inclusief zaakgegevens) bewaard moet worden. Per zaakstroom wordt een afweging gemaakt waar de bewerking belegd wordt:

Actie	Kan belegd worden bij	Opmerking
Niet bewaren (vernietigen)	RMA	Vernietiging wordt geregistreerd
Kortstondig bewaren	CDD+	Toekomstvast formaat niet relevant
Langdurig bewaren	CDD+, NA	Toekomstvast formaat relevant

Vanuit de Raad van de Rechtspraak (CEO) is de afspraak gemaakt met justitie dat de Rechtspraak aansluit bij de ketenvoorzieningen van justitie voor archiveren. Dat betekent in de praktijk dat de digitale archiefstukken van de Rechtspraak in de ketenvoorziening van justitie worden ondergebracht, conform hetgeen gesteld wordt in [IDDA]. Als er besloten wordt met welke reden dan ook dat er moet worden afgeweken van deze afspraak dan moet besluitvorming op het juiste niveau plaats vinden. Dat betekent dat er nieuw beleid moet worden vastgesteld en dat afspraak tussen de Raad van de Rechtspraak (CEO) met justitie herzien moet worden. Het project DAR zal in dat geval hiertoe adviseren. Merk op dat het voor het bouwblokken zoeken, opvragen en verstrekken niet uit mag maken bij welke partij de archiefinhoud is belegd, noch hoe dit technisch is gerealiseerd.

Communicatie

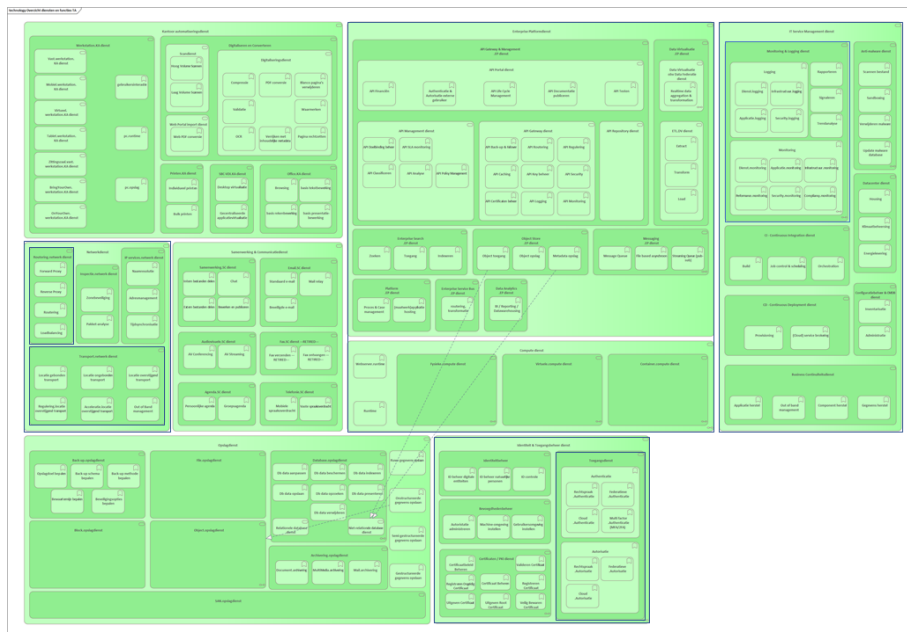
Het moet mogelijk zijn voor een verscheidenheid aan systemen om met het digitaal archief te koppelen. Het digitaal archief zal om de koppelingen mogelijk te maken een aantal gestandaardiseerde koppelvlakken realiseren, door het realiseren van de standaard koppelvlakken is dat het aansluiten van de systemen minder werk is.

De volgende koppelvlakken worden onderkend:

Koppelvlak	Omschrijving
Import koppelvlak	Een gestandaardiseerd koppelvlak voor het importeren van digitale zaakgegevens en digitale stukken.
Ontsluiten koppelvlak	Een gestandaardiseerd koppelvlak met als doel zaakdossiers en/of individuele stukken te kunnen ontsluiten voor partijen of vertegenwoordigers.
Uitplaatsen koppelvlak	Een gestandaardiseerd koppelvlak met als doel zaakgegevens, -dossiers en bijbehorende stukken te verzenden aan andere archiefdiensten.

7. Technische architectuur

Voor in technische inrichting wordt gebruik gemaakt van de volgende bouwblokken die in het landschap beschikbaar zijn.



Bouwblok	Functionies	REA	Toelichting
IT service mangement dienst		Ja	
	Monitoring en logging	Ja	Het vastleggen van gebeurtenissen en het observeren en controleren van een dienst, een applicatie of de infrastructuur t.b.v. het signaleren van gedrag dat afwijkt van een vooraf bepaalde norm. Een dienst kan hier zowel een infrastructuur dienst zijn als een business dienst. Bij archiveren moeten op basis van het logging beleid de volgende gegevens centraal beschikbaar zijn: - Audit logging: Wie heeft wanneer waar toegang toe gehad; - Security incidenten en aanvallen, om forensisch onderzoek te kunnen doen moet minimaal achterhaald kunnen worden wanneer de aanval plaats heeft gevonden, hoe lang de aanval heeft geduurd en waar de aanval vandaan is gekomen; - Performance incidenten: Bij niet beschikbaar zijn moet achterhaald kunnen worden hoe lang het probleem zich heeft voorgedaan.

Identiteit en toegangsbeheer		Ja	Identiteits- & Toegangsbeheer is het framework van policies & technologieën voor het vastleggen van identiteiten en het verlenen van toegangsrechten tot IT diensten, componenten en applicaties. Medewerkers van de Rechtspraak worden geauthenticeerd met hun Rechtspraak identiteit
	Toegangsdienst	Ja	De toegangsdienst biedt functies voor het controleren van identiteiten (authenticatie) en verleende bevoegdheden (autorisatie) op basis waarvan toegang kan worden gegeven tot (Rechtspraak-)bronnen als IT-diensten, applicaties, systemen en/of gegevens. Op basis van de toegangsdienst wordt de identiteit vastgesteld.
Netwerkdienst		Ja	Netwerkdienst is de dienst die de digitale communicatie tussen hardware componenten realiseert
	Routing	Ja	
	Transport	Ja	Archiveren levert grote datastromen op het netwerk op, deze moeten ondersteund worden.
Enterprise platform		Ja	De enterprise platform dienst levert integratie platformdiensten voor business applicaties en data. Afhankelijk van de gedetailleerde invulling worden hier meer, of minder functies van afgenomen.
SaaS dienst		Nee	Voor het archiveren van digitale producten wordt een SaaS dienst als oplossing voorgedragen. In de onderstaande paragraaf worden de voor- en nadelen van een cloud product beschreven.
	RMA	Nee	De dienst die verantwoordelijk is voor de opslag en het overbrengen naar CDD+. Deze dienst wordt binnen de kaders van dit statement gerealiseerd.

SaaS

Het voordeel van een SaaS oplossing is dat de leverancier volledig verantwoordelijk is voor de geleverde dienst, de inspanning binnen de Rechtspraak verschuift van technisch beheer naar controleren en auditen van de leverancier. De Rechtspraak doet dit op basis van een SLA. Op het moment dat de leverancier niet aan de voorwaarden van de Rechtspraak voldoet wordt hier actie op ondernomen door bijvoorbeeld de dienst bij een andere leverancier af te nemen. In het kader van archiveren is het van belang dat alleen medewerkers van de Rechtspraak toegang hebben tot de gegevens die in de dienst zijn opgenomen, dit moet te achterhalen zijn op basis van de audit log die beschikbaar wordt gesteld door de leverancier. Bij het beheer dient de Rechtspraak rekening te houden met het verander tempo van de RMA SaaS dienst (leverancier). Het implementeren van security updates zal over het algemeen alleen technische impact hebben op de dienst, nieuwe features hebben ook functionele impact, hierin is het van belang deze tijdig te

communiceren naar de eindgebruikers. Bij het afnemen van de SaaS dienst moet ook opgelet worden dat de kosten verschuiven van Capex naar Opex.

Naast de voordelen van de cloud zijn er ook aandachtspunten:

- Minder controle op updates. Updates en changes worden door de leverancier uitgevoerd, hier heb je als organisatie minder controle over. Hier moeten we wel de kanttekening plaatsen dat tijdig updaten een belangrijke security maatregel is ter voorkoming van cyber aanvallen.
- De leverancier levert het volledige platform, als gevolg hiervan moet getoetst worden of het geleverde platform aan de security en compliance eisen van de Rechtspraak voldoet. Belangrijke aandachtspunten zijn:
 - Locatie van de gegevens. De gegevens moeten binnen de EU opgeslagen worden en mogen bijvoorbeeld ook niet naar een andere locatie gerepliceerd worden die buiten de EU ligt;
 - De privacy moet gegarandeerd worden;
 - De leverancier moet voldoen aan de veiligheidseisen die de Rechtspraak stelt aan het product;
 - Het moet mogelijk zijn om een onafhankelijke check te doen op de beveiligingsmaatregelen van dienst;
 - Het moet mogelijk zijn om een exit strategie toe te passen, de gegevens moeten op ieder moment uit het systeem op te halen zijn.

8. Security en Privacy

De informatie die binnen het Digitaal archief gebruikt wordt neemt de classificatie over van het aanleverende systeem. Doordat de classificatie van de aangeleverde informatie erg kan verschillen gaan we er van uit dat het hoogst opgeslagen niveau dat voor kan komen in het archief Geheim.

Indien een hoger niveau aan de orde is zullen andere (bijv. procesmatige) voorzieningen getroffen moeten worden, die nu niet in de eisen zijn meegenomen. De griffie is verantwoordelijk voor de rubricering van berichten en documenten.

Door de Rechtspraak zijn in het Normenkader Informatiebeveiliging de volgende richtlijnen geformuleerd die gelden als kader voor het beheren van interne autorisaties:

- Toegang tot informatie(systemen) wordt uitsluitend verleend op basis van de zakelijke behoefte ('need-to-know' / 'need-to-use').
- De toegangsbeveiliging voor informatie(systemen) is ingericht volgens het principe: 'alles is verboden, tenzij het uitdrukkelijk is toegestaan'.
- Er zijn procedures vastgesteld voor het registreren en afmelden van gebruikers en voor het verlenen en intrekken van toegangsrechten tot informatie(systemen).

- De diverse rollen in het kader van het verlenen van toegang tot informatie(systemen) zijn duidelijk vastgesteld en in de organisatie belegd (aanvragen, goedkeuren, daadwerkelijk toekennen van rechten, administreren, controleren, etc.).
- Er vindt een formele registratie plaats van alle gebruikers van informatie(systemen).
- Het gebruik van functionele (unnamed) accounts is niet toegestaan. Functionele accounts die toch noodzakelijk zijn (bijv. voor gastsprekers, vergaderzalen, externe docenten en bibliotheken), worden (na vaststelling van de identiteit) administratief gekoppeld aan een natuurlijke persoon. Een functioneel account geeft alleen de noodzakelijke rechten op data en functionaliteit van de Rechtspraak.
- Toegangsrechten worden (zoveel mogelijk) uitgegeven op basis van vastgestelde autorisatiematrices en toegangsprofielen en alleen bij uitzondering op individuele basis.
- Gebruikersaccount worden niet gebruikt voor beheertaken. Systeem- en applicatiebeheerders hebben aparte beheeraccounts voor beheertaken.
- De verantwoordelijken voor het toekennen van rechten aan gebruikers controleren halfjaarlijks of de gebruikers aan de juiste rollen en rechtensets gekoppeld zijn.
- De uitgegeven speciale bevoegdheden worden (tenminste) maandelijks gecontroleerd.
- Fouten dienen centraal gelogd te worden,
- Alle handelingen in het systeem dienen centraal gelogd te worden,
- Er dient bijgehouden te worden welke acties binnen het archief zijn uitgevoerd voor alle informatieobjecten. Van deze acties moet achterhaald kunnen worden wie de actie heeft uitgevoerd en of de persoon hiervoor op dat moment geautoriseerd was.
- Toegang wordt alleen verleend op basis van Rechtspraak account,
- De Rechtspraak beheert de autorisaties tot de gegevens;
- De login gebeurt op basis van een federatieve koppeling (bijvoorbeeld OAuth, of SAML),
- De gegevens zijn zowel bij het transport als tijdens de opslag encrypted,
- De Rechtspraak heeft de regie over de data;
- De Rechtspraak blijft eigenaar van de data;
- Binnen de applicatie mogen geen gegevens verwerkt worden met de classificatie staatsgeheim;

Binnen het Digitaal Archief moet worden vastgesteld of gebruikers over de juiste autorisaties beschikken om toegang te krijgen tot specifieke gegevens of functies. Hiervoor wordt intern een aparte autorisatie database (ACL) bijgehouden waarin de volgende gegevens aan elkaar worden gerelateerd:

- ID gebruiker
- Rol van de gebruiker
- Autorisaties waarover de gebruiker beschikt

De rubricering is tot stand gekomen op basis van onderstaand Rubriceringsschema uit hiervoor genoemde bron.

8.2 BIV-P classificatie

In onderstaande tabel is de BIV-P classificatie voor DAR weergegeven.

Beschikbaarheid: Tussen het opvragen van informatie en het uitgeven van informatie kan enige tijd tussen zitten, ook in het proces. Bij het aanbieden van de gegevens is er een copy aanwezig, totdat het aangeboden stuk succesvol is opgeslagen.

Integriteit: Het doel van het archief is het langdurig opslaan van gegevens om zo onder andere aan wettelijke regels te voldoen. Uitgangspunt hierbij is dat de opgeslagen gegevens aantoonbaar niet gewijzigd mogen worden en zijn in te zien.

Vertrouwelijkheid: De vertrouwelijkheid van de gegevens in het systeem is afhankelijk van de aangeleverde dossiers. In de verschillende aanleverende systemen is bepaald wat de vertrouwelijkheid is van de inhoudelijke gegevens. Op basis van wat eerder in het [GPSA](#) beschreven is gaan we er van uit dat de maximale vertrouwelijkheid van de gegevens geheim is. Het archief zal de daarvoor benodigde autorisaties en beveiliging ondersteunen.

Aspect	Niveau
Beschikbaarheid	2 Noodzakelijk
Integriteit	2 Hoog
Vertrouwelijkheid	2 Vertrouwelijk
Privacy	3 Ernstig

Tabel 4: BIV-P classificatie

8.4 Privacy eisen

Bij het archiveren is de inhoud van het dossier niet bekend. De grondslag, doelbinding en andere eisen over eventueel opgeslagen gegevens moeten vastgesteld worden in de verschillende bron systemen. Binnen het DAR komen dan alleen zal alleen dossiers en stukken waar de wettelijke noodzaak tot bewaren bestaat bestaat. Indien de noodzaak vervalt doordat bijvoorbeeld de bewaartermijn verloopt dan biedt het archief de mogelijkheid om de gegevens uit het archief te verwijderen. Het archief logt de actie die tot het verwijderen heeft geleid. Vanuit de bronsystemen wordt de noodzaak tot opslaan vastgesteld en hier een termijn aan gekoppeld.

Binnen het Digitale archief is het niet mogelijk om anoniem gegevens te benaderen.

Toegang tot de gegevens is altijd op basis van expliciete autorisaties.

Alle relevante handelingen binnen het archief worden gelogd:

- Inzien van gegevens;
- Wijzigen autorisaties;

- etc.

Deze logging bevat wel gegevens die terug te herleiden zijn naar een persoon. De logging van deze gegevens is noodzakelijk om te kunnen herleiden wie een actie heeft uitgevoerd om later verantwoording af te kunnen leggen over het bewaren van de gegevens. Voor de logging wordt gebruik gemaakt van de service voor business en auditlogging zoals eerder beschreven. Deze logdata kan daarom alleen toegankelijk zijn voor personen die daar in de uitvoering van hun rol noodzaak toe hebben.

9. Kwaliteitseisen

Op de Digitale Toegankelijkheid Confluence pagina zijn de definities beschreven op de pagina [Kwaliteitseisen](#).

De volgende kwaliteitseisen zijn van toepassing en zijn weergegeven in onderstaande tabel (zie ook [Normen en standaarden, Softwarekwaliteit, in de REA](#)).

X = van toepassing of NVT wanneer niet van toepassing

ISO 25010 aspecten	Omschrijving	Invulling
Functionele geschiktheid (Functional suitability)	De mate waarin een softwareproduct of computersysteem functies levert die voldoen aan de uitgesproken en veronderstelde behoeften, bij gebruik onder gespecificeerde condities.	Het systeem moet de processen ondersteunen zoals beschreven in hoofdstuk 2 bij de business doelen. De exacte functionele requirements worden later uitgewerkt.

Prestatie-efficiëntie (performance efficiency)	De prestaties in verhouding tot de hoeveelheid middelen gebruikt onder genoemde condities.	Het systeem moet in staat zijn om > 1.000.000 dossiers per jaar te verwerken. Er mogen hierbij geen dossiers verloren gaan. Aan de response tijden worden geen eisen gesteld. In totaal moet het systeem enkele PETA Bytes kunnen verwerken
--	---	--

Uitwisselbaarheid (Compatibility)	De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of software-omgeving deelt.	Er worden standaard koppelvlakken gedefinieerd tussen de verschillende onderdelen binnen het Digitaal Archiveren. De koppelingen worden gespecificeerd volgens de geldende (open) standaarden. Door het toepassen van de koppelvlakken is het mogelijk applicaties te vervangen zonder aanpassingen in het gehele landschap. · Voor het interne koppelvlak wordt gebruik gemaakt van het LGM model. Van dit model is aangegeven welke velden verplicht gevuld moeten zijn in MetadataMapping SOS en DAR.xlsx · Extern wordt er gebruik gemaakt van TMR om te communiceren. · Voor het beschikbaar stellen van de gegevens worden API's en queues gebruikt dit om de garantie te kunnen geven dat er bij het transport geen gegevens verloren gaan. In het SAD wordt dit in detail uitgewerkt
--	--	---

Bruikbaarheid (Usability)	De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruikscontext.	De eisen m.b.t. usability zullen later in het traject worden vastgesteld.
--------------------------------------	--	--

Betrouwbaarheid (Reliability)	De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.	Op DAR is service level Goud van toepassing • 99,5% beschikbaarheid (excl. onderhoud en evt. uitwijk) Het archiveren van zaakdossiers en -stukken maakt deel uit van het primaire proces van de Rechtspraak. De dienst moet een voldoende hoog servicelevel hebben (GPSA Digitaal Archiveren Rechtspraak). Belangrijke uitgangspunten bij de opslag: • Opgeslagen gegevens mogen niet verloren kunnen gaan; • Van opgeslagen gegevens moet aangetoond kunnen worden dat deze ongewijzigd zijn.
--	---	--

Beveiligbaarheid (Security)	De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.	De classificatie en onderbouwing is uitgebreid beschreven in hoofdstuk 8 van dit document.
Onderhoudbaarheid (Maintainability)	De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden door de aangewezen beheerders.	De archief dienst bestaat uit meerdere onderdelen van verschillende leveranciers. Het onderhoud van de onderdelen moet afgestemd worden met de verschillende beheer teams.

Overdraagbaarheid (Portability)	De mate waarin een systeem, product of component effectief en efficiënt overgezet kan worden van één hardware, software of andere operationele of gebruiksomgeving naar een andere.	In dit document wordt alleen de infrastructuur op hoofdlijnen beschreven op basis van gestelde non functionele requirements zoals bijvoorbeeld de performance van het systeem. De details worden uitgewerkt in een SD, of SAD dat later volgt. Er wordt gebruik gemaakt van de geldende afspraken rondom deployment (cloud), technologie stack en software architectuur (microservices).
------------------------------------	---	--

Bijlage 1: Woordenlijst

Begrip	Omschrijving
Archiefbescheid	Definitie in de archiefwet onder artikel 1c. luidt als volgt: 1. bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten; 2. bescheiden, ongeacht hun vorm, met overeenkomstige bestemming, ontvangen of opgemaakt door instellingen of personen, wier rechten of functies op enig overheidsorgaan zijn overgegaan; 3. bescheiden, ongeacht hun vorm, welke ingevolge overeenkomsten met of beschikkingen van instellingen of personen dan wel uit anderen hoofde in een archiefbewaarplaats zijn opgenomen om daar te berusten; 4. reproducties, ongeacht hun vorm, welke bij of krachtens de wet in de plaats zijn gesteld van de onder 1, 2 of 3 bedoelde archiefbescheiden of welke op grond van het bepaalde in artikel 7 zijn vervaardigd;

Bescheid	Zie: Archiefbescheid.
Capability	De mogelijkheid en bekwaamheid om een bepaalde dienst of functionaliteit te bieden
CAPEX	capital expenditures bedrag dat een bedrijf uitgeeft aan investeringen (van Dale)
CDD+	Centraal Digitaal Depot. Een dienst van Justid met als doel digitale dossiers en stukken uit te wisselen en bewaren conform wet- en regelgeving.
Digitaal Archief	Het geheel aan diensten, processen en systemen dat digitaal archiveren mogelijk maakt.
Digitaal dossier	Dossier waarvan de inhoud digitaal bewaard wordt.
Document	Zie: stuk.
Dossier	Een verzameling stukken of archiefbescheiden die betrekking hebben op dezelfde zaak.
GPSA	Globale Project Start Architectuur.
LGM	Zie: Logisch Gegevens Model.
Logisch Gegevens Model	Standaard model voor uitwisseling van gegevens binnen IVO Rechtspraak en opvolger van het Common Message Model (CMM).
Macroselectie	Het proces waarbij wordt bepaald welke dossiers integraal en blijvend bewaard worden, vaak op basis van maatschappelijk belang.
Metadata	Kenmerken die een entiteit (zoals een zaak) omschrijven.
Nationaal Archief	Overheidsdienst belast met het langdurig (of zelfs voor onbepaalde tijd) bewaren en toegankelijk maken van dossiers en archiefbescheiden.
Opex	Operationele uitgaven, oftewel Operating Expenditures, zijn de terugkerende kosten voor een product, systeem of onderneming.
Overbrengen	Het opslaan van dossiers, zaken en/of archiefbescheiden bij een andere partij waarbij ook het zorgdragerschap wordt overgedragen aan deze partij.
Papieren dossier	Een dossier waarvan de inhoud op papier bewaard wordt.
PPS	Zie: Primair Proces Systeem
Primair Proces Systeem	Een geautomatiseerd systeem waarin voor de afhandeling van één of meer zaakstromen zaakgegevens en/of stukken zijn opgeslagen.
RMA	Record Management Applicatie
Stuk	Een informatieobject dat deel uitmaakt van een dossier.

Uitplaatsen	Het opslaan van dossiers, zaken en/of archiefbescheiden bij een andere partij waarbij het zorgdragerschap bij de huidige partij blijft.
Zaak	Een proces of geschil.
Zaakdossier	Het dossier waarin alle stukken die betrekken hebben op een bepaalde zaak zijn opgenomen.
Zaakgegevens	De (meta-)gegevens die een zaak beschrijven, zoals zaaknummer, soort zaak, etc.
Zorgdrager	Degene die verantwoordelijk is voor het zorgdragerschap.
Zorgdragerschap	Definitie in de archiefwet onder artikel 1d .luidt als volgt: degene die bij of krachtens de wet belast is met de zorg voor archiefbescheiden.