

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Test References	Bevestigingen	Bedrijfstransacties met bevestigingsniveau Hoog
Notes		De intermediair heeft store-and-forward functionaliteit, en ook mogelijk enige (transport) retry functionaliteit zodat tijdelijke storingen op transportniveau (zoals HTTP connecties die niet kunnen worden opgezet) kunnen worden afgevangen. Omdat de intermediair geen verantwoordelijkheid kan en wil nemen voor de betrouwbaarheid van eindpunten, is gekozen voor end-to-end reliability op ebXML niveau. Eindpunten moeten zelf ebXML reliable messaging (retries, duplicate elimination) toepassen als dat nodig is.

Profile Requirement Item: Acknowledgements

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Specification Feature	Bedrijfstransacties met bevestigingsniveau Basis	Bedrijfstransacties met bevestigingsniveau Hoog
Header elements: Eb:MessageHeader/		
Specification Reference		
ebMS 2, section 10.1.1, 10.1.3		
Profiling (a)	Must each intermediary request acknowledgment from the next MSH?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging.
Profiling (b)	Must each intermediary return an Intermediate Acknowledgment Message synchronously?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging.
Profiling (c)	If both intermediary (multi-hop) and endpoint acknowledgments are requested of the To Party, must they both be sent in the same message?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging. Endpoint message handlers dienen geen intermediaire ontvangstbevestigingen te vragen.
Alignment		
Test References		
Notes		

SOAP Extensions

Profile Requirement Item: #wildCard, Id

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0
--

Specification Feature	Header elements:	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, section 2.3.6, 2.3.7, 2.3.8			
Profiling (a)	(Section 2.3.6) #wildcard Element Content: Are additional namespace-qualified extension elements required? If so, specify.	Er zijn geen aanvullende namespace-gekwalificeerde extensie-elementen. Ontvangende message handlers moeten onbekende extensie elementen negeren.		
Profiling (b)	(Section 2.3.7) Is a unique "id" attribute required for each (or any) ebXML SOAP extension elements, for the purpose of referencing it alone in a digital signature?	Niet van toepassing. ID attributen zijn niet verplicht.		
Profiling (c)	(Section 2.3.8) Is a version other than "2.0" allowed or required for any extension elements?	Deze specificatie is beperkt tot versie 2 van de ebXML Messaging specificatie.		
Alignment				
Test				
References				
Notes				

MIME Header Container

Profile Requirement Item: charset

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0				
Bevragingen		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog	
Specification Feature	MIME Header elements: Content-Type			
Specification Reference	ebMS 2, section 2.1.3.2			
Profiling	Is the "charset" parameter of Content-Type header necessary? If so, what is the (sub)set of allowed values? Example: Content-Type: text/xml; charset="UTF-8"	UTF-8		
Alignment				

Test References	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
	Bevestigingen	Bedrijfstransacties met beveiligingsniveau Hoog
Notes		

HTTP Binding

Profile Requirement Item: HTTP Headers

Specification Feature	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
	Bevestigingen	Bedrijfstransacties met beveiligingsniveau Hoog
Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.2.2.	
Profiling (a)	Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities?	
Profiling (b)	If other than "ebXML" what must the SOAPAction HTTP header field contain?	
Profiling (c)	What additional MIME-like headers must be included among the HTTP headers?	
Alignment		
Test References		
Notes		

Profile Requirement Item: HTTP Response Codes

Specification Feature	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
	Bevestigingen	Bedrijfstransacties met beveiligingsniveau Hoog
Header elements, MIME parts		

Specification Reference	ebMS 2, Appendix B.2.3.	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling	What client behaviors should result when 3xx, 4xx or 5xx HTTP error codes are received?		
Alignment			
Test References			
Notes			

Profile Requirement Item: HTTP Access Control

Specification Feature	Header elements, MIME parts	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, Appendix B.2.6.		
Profiling	Which HTTP access control mechanism(s) are required or allowed? [Basic, Digest, or client certificate (the latter only if transport-layer security is used), for example. Refer to item 4.1.4.8 in Security section.	Niet van toepassing. HTTP access control wordt niet toegepast.	
Alignment	Appears as AccessAuthentication elements in CPA.]		
Test References			
Notes			

Profile Requirement Item: HTTP Confidentiality and Security

Specification Reference		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0	
		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Specificatie Feature Specification Reference	Header elements, MIME parts ebMS 2, Appendix B.2.7.	Bedrijfstransacties met beveiligingsniveau Basis
		Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	Is HTTP transport-layer encryption required? What protocol version(s)? [SSLv3, TLSv1, for example. Refer to item 4.1.4.6 in Security section.]	Het gebruik van HTTPS op basis van TLS 1.0 [RFC 2246] is verplicht bij: - het profiel Bedrijfstransacties met beveiligingsniveau Hoog - berichtuitwisseling in een niet besloten netwerk(segment) TLS implementaties moeten kunnen opereren in backwards compatibility modus met SSLv3.
Profiling (b)	What encryption algorithm(s) and minimum key lengths are required?	Nader te bepalen.
Profiling (c)	What Certificate Authorities are acceptable for server certificate authentication?	PKI overheid houdt een lijst toegetroden certificatedienstverleners bij. Zie URL http://www.pkioverheid.nl/voor-certificaatverleners/toegetroden-certificaatverleners/ .
Profiling (d)	Are direct-trust (self-signed) server certificates allowed?	Nee
Profiling (e)	Is client-side certificate-based authentication allowed or required?	Client-side authenticatie is vereist bij het gebruik van HTTPS.
Profiling (f)	What client Certificate Authorities are acceptable?	Een CA die in de "chain of trust" voor de keten is opgenomen: PKI overheid.
Profiling (g)	What certificate verification policies and procedures must be followed?	De gangbare richtlijnen voor PKI moeten gehanteerd worden.
Alignment		
Test		
References		
Notes		Een gangbare aanbeveling is om een minimale sleutellengte van 1024 bits te hanteren [NIST-Keys] en waar mogelijk 2048.

SMTP Binding

Profile Requirement Item: MIME Headers

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Beveiligingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0			
Specificatie Feature	Header elements, MIME parts	Bevestigingen	
		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specificatie Reference	ebMS 2, Appendix B.3.2.	In onderzoek voor toekomstige versies. Deze versie van de Justitiestandaard Asynchrone Berichtenuitwisseling ondersteunt uitsluitend HTTP en HTTPS transport protocollen. In onderzoek.	
Profiling (a)	Is any specific content-transfer-encoding required, for MIME body parts that must conform to a 7-bit data path? [Base64 or quoted-printable, for example.]		
Profiling (b)	If other than "ebXML" what must the SOAPAction SMTP header field contain?		
Profiling (c)	What additional MIME headers must be included among the SMTP headers?		
Alignment			
Test			
References			
Notes			

Profile Requirement Item: SMTP Confidentiality and Security

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0			
Specificatie Feature	Header elements, MIME parts	Bevestigingen	
		Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specificatie Reference	ebMS 2, Appendix B.3.4, B.3.5	Niet van toepassing. In onderzoek	
Profiling (a)	What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]		
Profiling (b)	Is transport-layer security required for SMTP, and what are the specifics of its use? [Refer to item 4.1.4.6 in Security section.]		
Alignment			
Test			
References			
Notes			

Operational Profile

This section defines the operational aspect of the profile: type of deployment that the above profile is supposed to be operated with, expected or required conditions of operations, usage context, etc.

Deployment and Processing requirements for CPAs

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevestigingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Is a specific registry for storing CPAs required? If so, provide details.	Nader in te vullen		
Is there a set of predefined CPA templates that can be used to create given Parties' CPAs?	CPA templates zijn beschikbaar voor alle drie de sjablonen die in dit document zijn gedefinieerd.		
Is there a particular format for file names of CPAs, in case that file name is different from CPAId value?	Nader in te vullen		
Others			

Security Profile

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevestigingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Which security profile(s) are used, and under what circumstances (for which Business Processes)? [Refer to Appendix C of Message Service Specification. May be partially captured by BPSS isConfidential, isTamperproof, isAuthenticated definitions.]	Security profile 3: "Sending MSH authenticates and both MSHs negotiate a secure channel to transmit data" wordt toegepast. Security profile 0: "No security services are applied to data" is toegestaan indien gebruik wordt gemaakt van een beveiligde VPN of in besloten netwerksegmenten waar het beveiligingsbeleid vereist of toestaat om geen versleuteling toe te passen.	Bovenop de transportbeveiliging wordt Security profile 14: "Sending MSH applies XML/DSIG structures to message and applies confidentiality structures (XML-Encryption) and Receiving MSH returns a signed receipt" toegepast	
(section 4.1.5) Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message?	Niet van toepassing. Er zijn geen aanvullende beveiligingsmaatregelen aan MIME headers.		
Are any specific third-party security packages approved or required?	Nader in te vullen		
What security and management policies and practices are recommended?	Nader in te vullen		
Any particular procedure for doing HTTP authentication, e.g. if exchanging name and password, how?	Niet van toepassing		
Others			

Reliability Profile

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0			
Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog	Bedrijfstransacties met beveiligingsniveau Hoog
If reliable messaging is required, by which method(s) may it be implemented? [The ebXML Reliable Messaging protocol, or an alternative reliable messaging or transfer protocol.]	Niet van toepassing	Door middel van het ebXML reliable messaging protocol.	
Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]		Betrouwbaar berichtenverkeer profiel 2: Duplicate elimination Y AckRequested ToPartyMSH Y AckRequested NextMSH N	
Others			

Error Handling Profile

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0			
Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog	Bedrijfstransacties met beveiligingsniveau Hoog
(Section 4.2.4.2) Should errors be reported to a URI that is different from that identified within the From element? What are the requirements for the error reporting URI and the policy for defining it?	Nader in te vullen		
What is the policy for error reporting? In case an error message cannot be delivered, what other means are used to notify the party, if any?	Operationeel beheer is verantwoordelijk voor het doorlopend monitoren van de message logs van eindpunten en intermediairs.		
(Appendix B.4) What communication protocol-level error recovery is required, before deferring to Reliable Messaging recovery? [For example, how many retries should occur in the case of failures in DNS, TCP connection, server errors, timeouts; and at what interval?]	Nader in te vullen.		
Others			

Message Payload and Flow Profile

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0			
Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog	Bedrijfstransacties met beveiligingsniveau Hoog

Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
What are typical and maximum message payload sizes that must be handled? (maximum, average)	Toepassingen waarin berichten die ontvangen worden door een message handler verder gerouteerd moeten worden via een andere berichteninfrastructuur die een maximum omvang van berichten heeft, zullen dat maximum ook aan ebXML berichten op willen leggen. Dit beperkt (bij protocollen als JMS, MQSeries) berichtomvang tot enkele megabytes. HTTP Proxy servers en firewalls hebben ook beperkingen op omvang. Deze verschillen van organisatie tot organisatie. De Justitie Berichtenservice (JUBES) maakt ook gebruik van een HTTP Proxy.	
What are typical communication bandwidth and processing capabilities of an MSH for these Services?	Nader in te vullen.	
Expected Volume of Message flow (throughput): maximum (peak), average?		
(Section 2.1.4) How many Payload Containers must be present?	Berichten anders dan op zich zichzelf staande foutmeldingen en ontvangstbevestigingen hebben minimaal een payload bedrijfsdocument. Sommige toepassingen zullen een aantal al dan niet samenhangende bedrijfsdocumenten in een enkel bericht willen versturen.	
What is the structure and content of each container? [List MIME Content-Types and other process-specific requirements.] Are there restrictions on the MIME types allowed for attachments?	Aantal, aard en (betekenis van een) volgorde van Payload Containers die zijn toegestaan in berichten zijn nader te bepalen op het niveau van systemen ter ondersteuning van specifieke interactieprocessen.	
How is each container distinguished from the others? [By a fixed ordering of containers, a fixed Manifest ordering, or specific Content-ID values.]. Any expected relative order of attachments of various types?	Er is geen aanbevolen semantiek voor de volgorde van containers, Manifest elementen of waarden van Content-Id. Toepassingen wordt aanbevolen hiervoor aanvullende restricties op te stellen	
Others	De te ondersteunen Content-Typen zijn afhankelijk van de specifieke toepassing.	
What are typical and maximum message payload sizes that must be handled? (maximum, average)		
Additional Messaging Features beyond ebMS Specification		
Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Are there additional features out of specification scope, that are part of this messaging profile, as an extension to the ebMS profiling?		
Additional Deployment or Operational Requirements		
Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		

Operational or deployment aspects that are object to further requirements or recommendations.	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

References

Normative

- [FIPS 197] NIST FIPS 197. Advanced Encryption Standard (AES).
URL <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [Canonical XML] Canonical XML. URI <http://www.w3.org/TR/xml-c14n>
- [EPV-TA-1] Uitwerking technische architectuur van de berichtenuitwisseling — korte termijn. Versie 1.0 beta.
URL http://www.e-pv.nl/groepen/Architectuur_Infrastructuur/Technische_Architectuur/EPV_TA_1_0_beta
- [ETSI TS 102 176-1] Electronic Signatures and Infrastructures (ESI). Algorithms and Parameters for Secure Electronic Signatures. Part 1: hash functions and asymmetric algorithms.
URL <http://www.etsi.org/>
- [ISO 14662] ISO 14662. Open-edi reference model.
URL <http://www.iso.ch/>
- [ISO 15000-2] ISO 15000-2 *ebXML Message Service Specification*.
URL <http://www.oasis-open.org/specs/index.php#ebxmlmsgv2>.
- [RFC 2246] The TLS Protocol.
URL <http://www.ietf.org/rfc/rfc2246.txt?number=2246>
- [RFC 2392] Content-ID and Message-ID Uniform Resource Locators URL URL URL
<http://www.ietf.org/rfc/rfc2392.txt>
- [RFC 2437] PKCS #1: RSA Cryptography Specifications. IETF RFC 2437.
URL <http://www.ietf.org/rfc/rfc2437.txt>.
- [SOAP1.1] Simple Object Access Protocol (SOAP) v1.1. W3C Note 08 May 2000.
URL <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>
- [SYSDA] SYSDA instantiatietabel van organisaties in de strafrechtsketen.
- [XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification.
URL <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>.
- [XML Encryption] XML Encryption Syntax and Processing. W3C Recommendation.
URI <http://www.w3.org/TR/xmlenc-core/>

Non-normative

- [Deployment Guide 1.1] Pete Wenzel, Jacques Durand. *Deployment Profile Template For OASIS ebXML Message Service 2.0*. OASIS Committee Draft 1.1, 20 June 2005.
URL http://www.oasis-open.org/apps/org/workgroup/ebxml-iic/download.php/13750/ebxml-iic-ebms2_deploy_template-spec-cd-11-final.doc
- [Deployment Guide 1.0] P. Wenzel. *ebXML Deployment Guide Template*. OASIS Committee Draft 1.0 28 March 2003.
URL http://www.oasis-open.org/committees/download.php/1713/ebMS_Deployment_Guide_Template_10.doc
- [ebBP] ebXML Business Process Specification Schema Technical Specification
URL http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-bp#technical.
- [EPV-TA-2] EPV Technische Architectuur Berichtenuitwisseling Politie OM Routinezaken
URL http://www.e-pv.nl/groepen/Architectuur_Infrastructuur/EPV-TA-2/EPV_TA_2
- [FIPS 180-2] NIST FIPS 180-2 Secure Hash Standard
URL <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>
- [ISO 15000-1] ISO 15000-1 ebXML Collaboration Protocol Profile and Agreement Specification. OASIS ebXML Collaboration Protocol Profile and Agreement Specification (2.0).
URL <http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf>

- [JAB 1.0] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Technische
Standaarden ebXML Configuratiegids.
URL http://justitiweb.minjus.nl/040_bedrijfsvoering/ict/Beleid_en_standaarden/Standarden/Infrastructuur.asp
- [JAB 1.0 Func] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Functionele Standaard.
URL http://justitiweb.minjus.nl/040_bedrijfsvoering/ict/Beleid_en_standaarden/Standarden/Infrastructuur.asp
- [JAB 2.0 Func] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Onderbouwing en
toelichting.
- [NIST-Keys] NIST Key Management Guideline. .
URL [http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-\(workshop\).pdf](http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf).
- [SBG-IBS] Expertteam Framework Draft Intersectorale Berichtenstandaard. Deel B.
Technische Specificatie. Programma Stroomlijnen Basisgegevens.

6 JUstitie BErichten Service (JUBES)

J U B E S

(JUstitie BErichten Service)

Informatie & Voorwaarden

***Auteurs:
Competence Center Integratie - CCI***

Algemeen

Dit document beschrijft de JUstitie BErichten Service (JUBES) dienstverlening. Aan bod komen:

- een functionele beschrijving van de technische infrastructurele dienstverlening
- een beschrijving van de organisatorische ondersteuning
- de aansluitvoorwaarden
- additionele dienstverlening
- nuttige informatie

Voor meer informatie kunt u altijd terecht bij de ondersteunende organisatie.

NB:

Verzekert u ervan dat u de **meeste actuele versie** van dit document “Informatie & Voorwaarden” voor u hebt.

Een nieuwere versie **vervangt altijd** een oudere.

Beschrijving dienst JUBES

Algemeen

De centrale Justitie Berichten Service "**JUBES**" is een Justitiebrede voorziening, die al het elektronische berichtenverkeer tussen de verschillende Justitieonderdelen en tussen Justitie en haar (keten)partners buiten Justitie faciliteert.

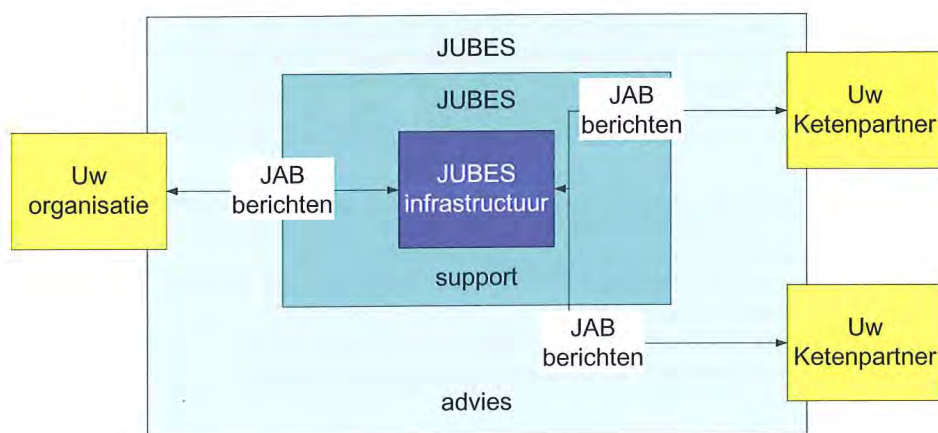
Het berichtenverkeer via **JUBES** maakt daarbij gebruik van de, op 7 april 2005 door het BVO tot standaard verheven, **Justitiestandaard Asynchrone Berichtenuitwisseling (JAB)** en past volledig binnen het Justitie Brokerconcept.

De JUBES dienstverlening bestaat uit twee componenten:

- Het technische infrastructurele deel dat de berichten service implementeert.
- Het organisatorische ondersteunende deel.

JUBES is gebaseerd op / vereist de JAB standaard.

Deze aspecten komen in de volgende paragrafen aan bod en zijn in onderstaande figuur schematisch weergegeven.



Door de inzet en het gebruik van de dienst **JUBES** wordt de beheersbaarheid van het elektronische berichtenverkeer aanzienlijk verbeterd (slechts één verbinding naar de **JUBES** infrastructuur i.p.v. meerdere 1- op -1 verbindingen naar de verschillende partners) en zijn aspecten als betrouwbare aflevering gerealiseerd.

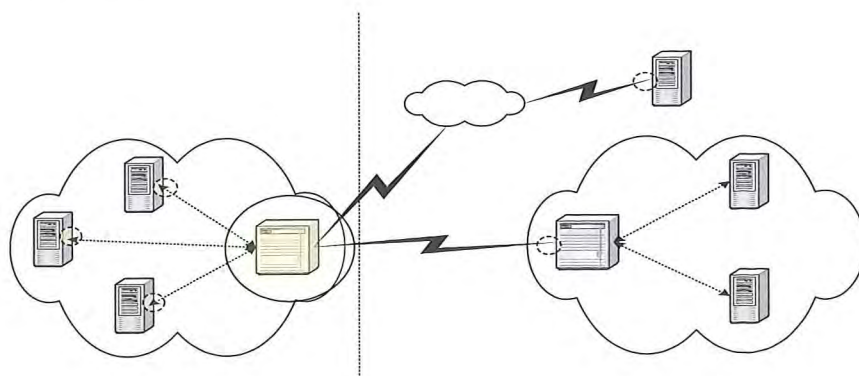
JAB standaard

De Justitiestandaard Asynchrone Berichtenuitwisseling (JAB-standaard) vormt de basis waarop de dienstverlening is gebaseerd. Deze JAB standaard wordt in andere documenten uitgebreid beschreven. Kort samengevat beschrijft de JAB standaard een manier van berichten transport (protocol) en een standaard envelop voor de berichten. Doordat de JAB standaard gebaseerd is op de open standaard e-business XML messaging standaard (ebMS) zijn er diverse producten in de markt die dit ondersteunen en is een grote mate van interoperabiliteit gegarandeerd.

Met ebMS zijn verschillende manieren van versturen mogelijk. Denk hierbij aan gewone brievenpost met gewoon en aangetekend versturen. De huidige JAB standaard beperkt de mogelijkheden tot betrouwbaar versturen (aangetekend). Er wordt nu gewerkt aan een nieuwe uitgebreidere vorm van de JAB standaard, waarin het onder andere mogelijk wordt niet aangetekend te versturen.

Waar in de technische beschrijving van JUBES sprake is van betrouwbaar afleveren, is dit alleen van toepassing op aangetekend versturen.

JUBES infrastructuur



De JUBES infrastructuur bestaat de 'datacommunicatievoorziening' en de 'communicatiefunctie', gezamenlijk te noemen de 'communicatie infrastructuur'.

Dit betekent dat JUBES de eigenlijke verzending volledig voor u regelt en verantwoordelijk is:

vanaf het moment dat de zendende partner een bericht aanbiedt aan de JUBES-infrastructuur **tot en met** het moment dat JUBES het bericht heeft afgeleverd bij de ontvangende partner **en** daarvan een ontvangstbevestiging heeft afgeleverd bij de verzender.

Dit impliceert dan ook dat de zendende en de ontvangende partners zelf verantwoordelijk zijn voor het volgens de JAB standaard aanmaken en aanleveren van het bericht enerzijds en het oppakken en verwerken van het bericht anderzijds in de achterliggende applicaties. Het aanleveren en oppakken zijn grensfuncties die raken aan zowel de applicatie als JUBES, we noemen dit ook wel de integratiefuncties. Het CCI kan u in adviserende zin bijstaan om te beziën welke integratiefunctie het best past bij de gewenste werkwijze (zie ook 0).

Om, ingeval van een tijdelijke onbeschikbaarheid aan de kant van de ontvanger, het bericht nogmaals aan te kunnen bieden, wordt het bericht binnen de JUBES-infrastructuur maximaal 24 uur bewaard.

Als een bericht na een tussen partners afgesproken tijd niet afgeleverd kan worden, zal de verzendende partij hiervan door JUBES op de hoogte worden gesteld. De zendende partij kan nu actie ondernemen (opnieuw zenden, ontvangende partij raadplegen, etc.).

De JUBES infrastructuur maakt geen onderscheid tussen de berichten. Berichten kunnen zowel operationele als test berichten zijn. Onderscheid moet door de partners en applicaties worden gemaakt door bijvoorbeeld andere adressen of cpa id's etc.

De JUBES infrastructuur wordt technisch beheerd door **KPN_Verbint** en functioneel door het voorlopig virtuele **Competence Center Integratie (CCI)**.

T.z.t. is het de bedoeling de dienst onder te brengen bij het SSC-ICT.

JUBES support door het CCI

Nadat een berichtenstroom via JUBES tot stand gekomen is (de organisatie is in productie) is de support op de dienst JUBES als volgt geregeld:

Organisatie van de support

Bij de organisatie van de support wordt uitgegaan van een standaard verdeling in drie niveaus, nl:

1^e lijn:

Dit betreft vragen en problemen met de integratie software binnen uw organisatie, dus daar waar de berichten klaargemaakt worden voor verzending en de verzending zelf, inclusief de gratis end-point software Cyclone Activator.

Voor dit niveau support moet uw organisatie altijd zelf zorgdragen. Het wordt aanbevolen om hiervoor meer dan één beheerder aan te stellen en op te leiden.

Worden de berichten verzonden via de Activator van Cyclone, dan kan de Cyclone cursus hiervoor een goede basis zijn.

Worden de berichten verzonden via een andere 'Adapter' (bv. van uw eigen EAI-leverancier), dan moet daar ook de kennis vandaan worden gehaald.

2^e lijn:

Dit betreffen vragen en/of problemen die verder gaan dan de eigen integratiesoftware of problemen die niet zelf opgelost kunnen worden.

Er kan in dit geval een beroep gedaan worden op het **Competence Center Integratie (CCI)**. Het CCI zal proberen de vraag te beantwoorden of het probleem op te lossen. Indien noodzakelijk, dan zal het CCI de 3^e lijn inschakelen (Cyclone of KPN).

T.z.t. (bij 7x24 support) zal het ook mogelijk worden om, voor technische problemen, rechtstreeks de KPN te benaderen (gelijk de SLA's rond Verbint). De KPN fungeert hierbij dan als 2^e lijn (en zonodig 3^e lijn) en heeft contacten met Cyclone.

3^e lijn:

Dit betreffen de vragen/problemen die direct betrekking hebben op de software of de techniek (verbinding), die niet opgelost kunnen worden door 1^e en 2^e lijn. Hiervoor worden afhankelijk van de problematiek KPN en/of Cyclone ingeschakeld.

Escalatie:

Indien bovenstaande niet tot bevredigend resultaat leidt moet daarvoor CCI/DI worden aangesproken. Zij zullen alles in het werk stellen om de problematiek zo snel mogelijk te (laten) verhelpen en maatregelen treffen om dit in de toekomst te voorkomen.

Zoals al is aangegeven bent U als organisatie zelf verantwoordelijk voor het correct volgens JAB communiceren met de JUBES infrastructuur. U dient hiervoor zelf de benodigde software te installeren en een beheer organisatie in te richten. Indien er problemen zijn met de communicatie tussen Uw organisatie en de JUBES infrastructuur dan beperkt ondersteuning vanuit het CCI zich tot de JUBES kant. U zult zelf zorg moeten dragen voor uw eigen software. Uiteraard gebeurt foutanalyse wel in onderlinge samenwerking.

Niveau van dienstverlening

De technische infrastructuur van de dienst *JUBES* is onder gebracht in de bestaande mantelovereenkomst Verbint. Hieruit vloeit voort dat de dienstverlening voor *JUBES* op hetzelfde niveau wordt geleverd als het dienstenniveau voor Verbint.

Voor gedetailleerdere informatie wordt dan ook verwezen naar:

1. Diensten Niveau Overeenkomst, versie 4.2
2. Dossier Afspraken en Procedures, versie 1.2
3. Producten- en dienstencatalogus, versie 2.2

En aanvullend naar:

4. De aanbidding Dienstverlening Messagebroker onder Verbint, d.d. 29 augustus 2005, versie 1.0, met het kenmerk: SC5 074184/188
5. Nadere overeenkomst Broker dienstverlening.

Enkele highlights van dit dienstniveau:

- De dienst wordt ondersteund van ma. t/m vr. van 8.00 — 18.00 uur. Als optie is ook mogelijk een ondersteuning van 7 x 24 uur (uiteraard heeft dit ook consequenties voor uw eigen beheerorganisatie als 1^e lijn support)
- De maximale onbeschikbaarheid van de dienst per maand is 4 uur.
- Rapportages over aantal berichten per bron/bestemming en totalen berichtgrootte.
- Een eerste veiligheids audit is gehouden kort na het akkoord verklaren van het in productie gaan met *JUBES*. Zoals ook beschreven in de DAP zullen op regelmatige basis audits blijven worden uitgevoerd om de veiligheid te waarborgen.

JUBES advies door het CCI

Naast de support rol van het CCI is er ook een advies rol. Deze omvat:

- *Functioneel en technische vraagbaak*
Vanuit de kennis en ervaring van de leden van het CCI ('best practices' en trainingen) zullen zij zo goed mogelijk uw vragen beantwoorden of zonodig antwoorden halen bij de leverancier.
- *Advies met betrekking tot te koppelen/integreren toepassing(en)*
Vanuit de kennis en ervaring van de leden van het CCI kan door hen meestal goed aangegeven worden wat de meest effectieve manier is om te integreren. De feitelijke realisatie van de koppeling is de verantwoordelijkheid van eigen organisatie.
- *Indien toepasbaar ondersteuning bij de installatie van de gratis beschikbare Cyclone endpoint software (De Activator)*
Dit kan door het aanvragen van een gratis licentie voor de Activator m.b.v. het formulier 'Aanvraag licentie Activator basis'.
- *Ondersteuning bij definiëren van partner agreements (afspraken tussen zendende en ontvangende partij)*

Dit gebeurt bij voorkeur op basis van de daarvoor bedoelde CPA standaard. Op basis van al bestaande CPA's kan het CCI u helpen om de voor uw verkeersstroom specifieke CPA aan te maken en te implementeren. Maakt uw ebMS software geen gebruik van CPA's dan beperkt de ondersteuning zich tot concepten.

- *Ondersteuning bij opvoeren organisaties/partijen als "Partner" binnen JUBES*
De leden van het CCI kunnen u helpen met het verzamelen van de informatie die nodig is het formulier 'opvoeren/wijzigen/verwijderen Partner' in te vullen. Dit formulier is nodig om de verkeersstroom binnen JUBES kenbaar te maken.
- *Ondersteuning (adviserend) bij het openstellen van firewalls etc.*
Om berichten de organisatie uit te krijgen of te ontvangen moet er veelal in het netwerk van de organisatie e.e.a. geconfigureerd/aangepast worden. Daar heeft het CCI enige ervaring mee, die zij graag willen delen.
- *Ondersteuning bij de acceptatietests aansluiting JUBES*
Om van JUBES gebruik te kunnen en mogen maken, moet via acceptatietests bewezen worden dat de standaards op de juiste wijze zijn gebruikt. Het CCI zal met uw organisatie de noodzakelijke tests uitvoeren en de resultaten beoordelen.
- *Bemiddelen bij training in Nederland*
Indien een training gewenst is, wordt in principe verwezen naar het trainingsschema van de leverancier (UK of USA). Indien gewenst kan bij voldoende deelname bemiddeld worden bij een training op locatie in Nederland.

Versiebeleid

Nieuwe updates en versies van de applicatie- en systeemsoftware zullen altijd eerst beoordeeld worden op hun functionele en technische meerwaarde.

Omdat we binnen Justitie uitsluitend willen werken met 'bewezen technologie', zullen versies dan pas worden geïnstalleerd als zij bewezen stabiel zijn of als het om functioneel/technische redenen noodzakelijk is.

Nieuwe versies zullen worden geïnstalleerd binnen het daartoe afgesproken maandelijkse service window (1^e of 2^e woensdag van de maand tussen 00.00 — 7.00 uur).

Gebruik van de dienst JUBES

Is het gebruik van JUBES vrijblijvend?

Het gebruik van de dienst *JUBES* is **niet** vrijblijvend!

Indien u informatie/berichten wilt versturen buiten uw sector (andere Justitie onderdelen) of naar Partners buiten Justitie, is het verplicht hiervoor gebruik te maken van de dienst *JUBES* met de onder deze dienst vallende standaarden (JAB-standaard). Dit volgt o.a. uit het BVO besluit van 7 april 2005 en het Justitie Brokerconcept.

Hoe kunt u gebruikmaken van deze dienst

Indien u als organisatie *informatie* wilt over de dienst JUBES,

of u wilt berichten gaan *versturen* via JUBES en daarvoor *aansluiten* op JUBES, dan kunt u contact opnemen met het CCI-loket:

p.pauk@minjus.nl

of

070-3709023

Er zal dan een afspraak gemaakt worden met één of meerdere leden van het CCI en uw organisatie om de mogelijkheden en de verdere stappen te bespreken.

De hele doorlooptijd van een dergelijk traject (van aanmelden tot daadwerkelijk in productie draaien) kan variëren van enkele weken tot enkele maanden en hangt sterk af van de fase waarin de te koppelen partner zich bevindt (zijn berichtstromen al gedefinieerd, applicaties al ontwikkeld, etc) en de integratiewijze die gekozen wordt.

Het CCI zal proberen dit alles met u in kaart te brengen en u daar waar mogelijk en gewenst te ondersteunen in het te lopen traject.

De inzet van CCI leden is zonder kosten en vindt plaats in overleg met uw organisatie. De inzet is op basis van beschikbare capaciteit en in volgorde van aanvraag.

NB:

Het moge duidelijk zijn dat kennis binnen het CCI van ebXML-adapters (endpoint software) van andere leveranciers dan Cyclone niet is gegarandeerd.

Aansluitvoorwaarden

Om als organisatie/Partner aan te kunnen sluiten op *JUBES* moet aan de volgende voorwaarden worden voldaan:

Gebruik JAB-standaard

De via *JUBES* te verzenden elektronische berichten moeten voldoen aan de in april 2005 vastgestelde Justitiestandaard Asynchrone Berichtenuitwisseling, de JAB-standaard (ebXML).

Gebruik gecertificeerde ebMS software

De JABstandaard is gebaseerd op de ISO 15000-2 gecertificeerde versie van ebXML Message Service, ebMS. Dit betekent dat de aan te leveren berichten verstuurd moeten worden d.m.v. gecertificeerde ebMS software (zoals de Activator van Cyclone). Indien een (niet gecertificeerde) ebXML adapter van een andere leverancier wordt gebruikt zullen hiervoor extra acceptatie tests moeten worden uitgevoerd.

Beheerorganisatie

De eigen (sectorale) beheersorganisatie zal enkele medewerkers (meer dan één) opleiden om als 1^e lijns support, hulp te kunnen bieden bij vragen over en/of problemen met het versturen van berichten. Alleen deze organisatie kan de 2^e lijns ondersteuning inschakelen.

Deze beheerorganisatie dient ook beschikbaar te zijn om, *binnen 2 werkdagen*, door/via het CCI aangeleverde oplossingen voor hoge prioriteit problemen uit te testen.

Acceptatietest

Een acceptatie test van ontwikkelde te verzenden berichten moet positief zijn beoordeeld door het CCI.

Vaste IP adressen

Uw sectorale messagebroker dient van een vast IP adres voorzien te zijn. Wel is het toegestaan van load balancers gebruik te maken.

Viruscontrole op eigen endpoint

U bent er zelf voor verantwoordelijk dat u een betrouwbare partner bent in de informatie uitwisseling met andere partners. Dit houdt in dat u zelf verantwoordelijk bent voor een 'schone' berichtenuitwisseling en daarvoor dus maatregelen treft als bv. Viruscontrole op de endpoints.

Servercertificaten op eigen endpoint

Op de centrale JUBES infrastructuur zijn servercertificaten aangebracht gebaseerd op PKIoverheid, waarmee een hoog veiligheidsniveau kan worden gegarandeerd. Afhankelijk van de noodzakelijke vertrouwelijkheid van de berichten en het segment waarover berichten worden uitgewisseld moeten ook op de endpoints (op PKIoverheid gebaseerde) certificaten worden aangebracht. De JABstandaard zegt hierover:

"Het gebruik van HTTPS op basis van TLS 1.0 [RFC 2246] met 2-zijdige authenticatie is verplicht bij:
- *het profiel Bedrijfstransacties met beveiligingsniveau Hoog*
- *berichtuitwisseling in een niet besloten netwerk (segment)*

Bij uitzondering is, wanneer de gebruikte ebXML Messaging software geen TLS client authenticatie biedt en alleen voor zover niet uitgesloten door de andere Justitie-beveiligingsrichtlijnen, client authenticatie niet vereist als client IP nummer toegangscontrole is geïmplementeerd en het aantal client IP adressen beperkt is tot een zeer gering aantal.

TLS implementaties moeten kunnen opereren in backwards compatibility modus met SSLv3."

PKIoverheid servercertificaten zijn zonodig te betrekken bij o.a. DigiNotar.

Uitvoeren keten/capaciteitstest

Het kan op enig moment wenselijk en zinvol zijn om een ketentest uit te voeren. Dit is eigenlijk een connectiviteitstest, met de bedoeling om te bezien of de partner in de keten is te bereiken.

Met in acht neming van bovenstaande punten is dit uiteraard toegestaan.

Het is echter **niet toegestaan** een stresstest over JUBES uit te voeren.

Een stresstest op JUBES is door het CCI reeds uitgevoerd (rapportage beschikbaar).

Het uitvoeren van een capaciteitstest is wel toegestaan onder de volgende voorwaarden:

- Het CCI moet hiervoor uitdrukkelijk toestemming hebben verleend
- De hoeveelheid te versturen berichten is maximaal 2x het verwachte aantal te versturen berichten per tijdseenheid.
- Het project dat de capaciteitstest uitvoert is volledig aansprakelijk voor ontstane problemen cq. productieverstoringen, indien de test uitgevoerd wordt zonder toestemming van het CCI.

Gebruik Gratis Activator

Als dienstverlening rond JUBES is ook gratis ebMS software beschikbaar in de vorm van de Cyclone Activator basis. Deze software kunt u eenvoudig aanvragen bij het CCI.

Bij het gebruik van de Cyclone Activator basis (CA) moet met het volgende rekening worden gehouden:

- De huidige versie van de Cyclone Activator basis draait onder Windows (vanaf 2003), Unix-versie? en Linux-versie?
- De CA is single endpoint software, dus draait op 1 systeem, 1 cpu, etc.
- De CA ondersteund dus per definitie geen 7x24 beschikbaarheid bij hoge verkeersstromen
- De CA ondersteund geen fail-over faciliteiten

Indien u gebruik maakt van deze gratis end-point software dient u hier zelf het support voor in te richten. Bij gebleken bugs in de Cyclone software kunnen deze via het CCI worden doorgegeven aan de leverancier.

In gevallen dat bovenstaande voor u tot problemen kan leiden moet worden overgegaan tot de aanschaf van een zwaardere versie van de Activator, de Activator+, of wellicht zelfs tot de Interchange Advanced Server, het zwaarste product van Cyclone.

Deze zijn uiteraard niet gratis.

7 Justitie ICT-standaarden

Inleiding

In het Justitie standaardenbeleid is aangegeven waarom Justitiebrede standaarden van belang zijn, hoe het standaardisatieproces is ontstaan en hoe de implementatie van de rapportage over de ICT-standaarden geregeld is. In het najaar van 2007 is het gebruik van de standaarden van de standaardenlijst onderzocht bij de Justitiesectoren; het blijkt dat deze standaarden en de standaardenlijst nog steeds en zelfs in toenemende mate een toegevoegde waarde hebben voor de samenwerking in het intra-Justitiedomein.

De standaardisatiecommissie heeft de oude ICT-standaarden van 2007 voor 2008 herijkt en zij heeft de nieuwe standaarden van het standaardisatie college GBO.Overheid getoetst op gebruik bij Justitie. De nieuwe standaarden die van belang zijn voor het Justitiedomein voor 2008 zijn, na consultatie van ODB en I&A board, opgenomen in deze lijst. Het BVO heeft deze lijst op in 2008 vastgesteld.

Inhoud standaardenlijst

Deze standaardenlijst bevat de Justitie Informatievoorziening standaarden en in de bijlage zijn de relevante Justitie ICT contracten opgenomen.

Dit document bevat de standaarden op hoofdlijnen. Op het Justitie intranet zijn deze standaarden verder uitgewerkt. Per standaard is achtergrondmateriaal opgenomen en beschikbaar voor de bevoegde gebruiker.

Ga daarvoor naar:

<http://justitiweb.minjus.nl/ict=> beleid en standaarden => standaarden>

Binding standaarden

Als gevolg van de rapportageplicht voortkomend uit het kabinetsbeleid ten aanzien van het gebruik van (open) standaarden is per standaard ook de beoogde waarde van het gebruik en daaraan gekoppelde rapportage daarover opgenomen:

Verplicht Organisaties hebben deze standaard onverkort doorgevoerd. Hier wordt geen rapportage op verwacht

Comply or explain Organisaties voeren in principe deze standaard door. Organisaties melden of dat deze standaarden zijn doorgevoerd of niet. Zo niet wordt aangegeven wanneer dit wel het geval zal zijn.

Facultatief Organisaties wordt aangeraden deze standaard te gebruiken. Hierover wordt geen rapportage verwacht.

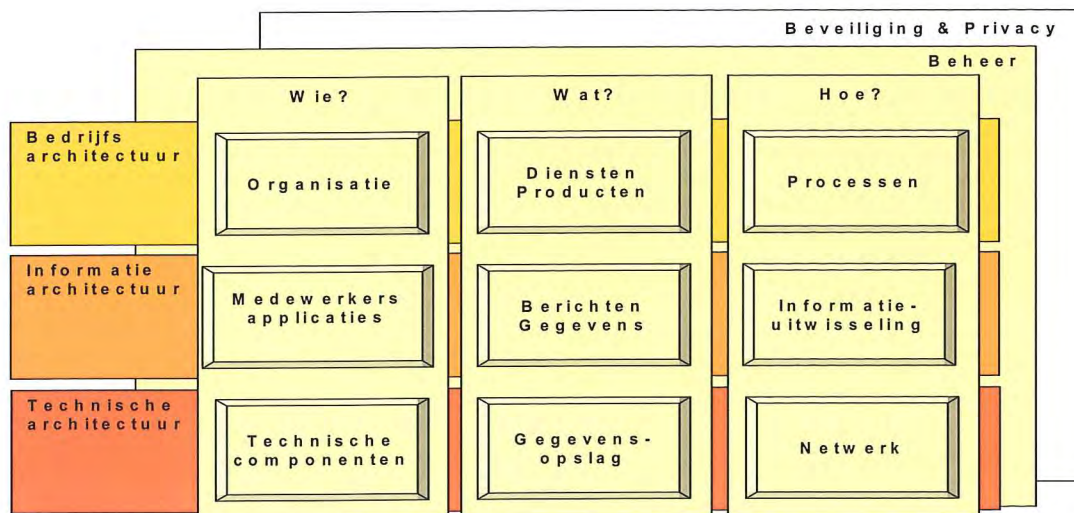
De rapportageplicht

Binnen Justitie bestaat reeds de plicht voor de Justitie sectoren om te rapporteren in hun 2^e viermaandrapportage over het gebruik van de Justitie standaarden.

Deze plicht wordt nu uitgebreid. In het jaarplan moet worden aangegeven, welke acties in het komende jaar ondernomen zullen worden ten aanzien van de comply or explain standaarden, die nog niet zijn ingevoerd. Daarnaast moet in het jaarverslag verantwoord worden, in hoeverre de voorgenen acties hierop daadwerkelijk zijn doorgevoerd.

De indeling

Om aan te sluiten bij de NORA en de MARIJ is de oorspronkelijke hoofdstukindeling van de standaardenlijst omgezet, naar analogie van het 11-vlaks model van de NORA, naar de hoofdstukken Bedrijfsarchitectuur, Informatie architectuur, Technische Architectuur, Beheer, Beveiliging & Privacy.



De standaarden zijn in deze hoofdstukken geplaatst daar waar zij de grootste werking hebben. Standaarden kunnen echter op meerdere plekken binnen het NORA model van kracht zijn. Voor het totaal overzicht is, bijgevoegd als bijlage 1, de mapping gemaakt op welke plekken binnen dit model de individuele standaarden ook effect hebben.

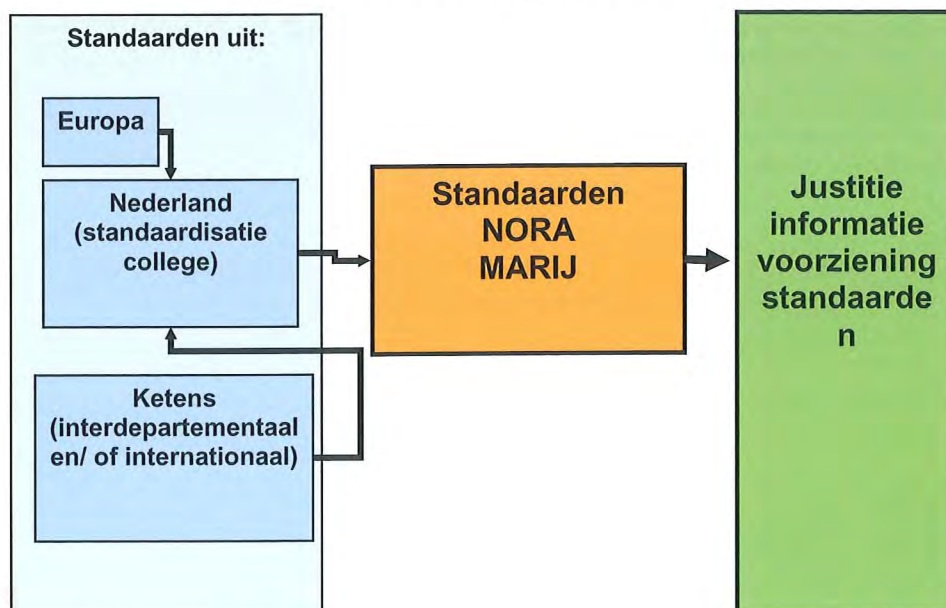
Opneming standaarden in de standaardenlijst

Uitgangspunt is dat de Justitie de vastgestelde standaarden uit internationaal, overheidsbreed of interdepartementaal verband overerft.

Ambitie van NORA is dat geldende standaarden met een overheidsbrede werking daarin opgenomen zullen zijn. In de MARIJ zullen de standaarden met een Rijksbrede werking opgenomen moet zijn. Uiteindelijk zullen alleen de door het forum standaardisatie gepubliceerde standaarden een overheidsbrede cq Rijksbrede werking (vastgesteld door het college standaardisatie) hebben daarin opgenomen kunnen zijn.

In huidige versie van de NORA is nu een verzameling van alle in gebruik zijnde standaarden opgenomen, deze bestaat uit formeel vastgestelde standaarden alsook informeel in gebruik zijnde standaarden en de MARIJ heeft nog geen formele status.

Dit is de reden, dat deze buiten Justitie vastgestelde standaarden met een daadwerkelijke werking op het Justitie domein, nog in dit document zijn opgenomen.



De Justitie specifieke standaarden worden vanuit de Justitie standaardisatie commissie, na consultatie ODB, voorgedragen aan de I&A board. De voorzitter van de I&A board brengt nieuwe standaarden aan ter besluitvorming aan BVO. Deze besluit of een Justitie specifieke standaard een standaard wordt of dat deze specifieke standaard opgeheven wordt. In enkele gevallen kan het zijn dat het BVO het besluit daarover doorzet naar de bestuursraad. De in dit document opgenomen Justitiespecifieke standaarden zijn allen besproken in BVO of bestuursraad.

Werkingsgebied

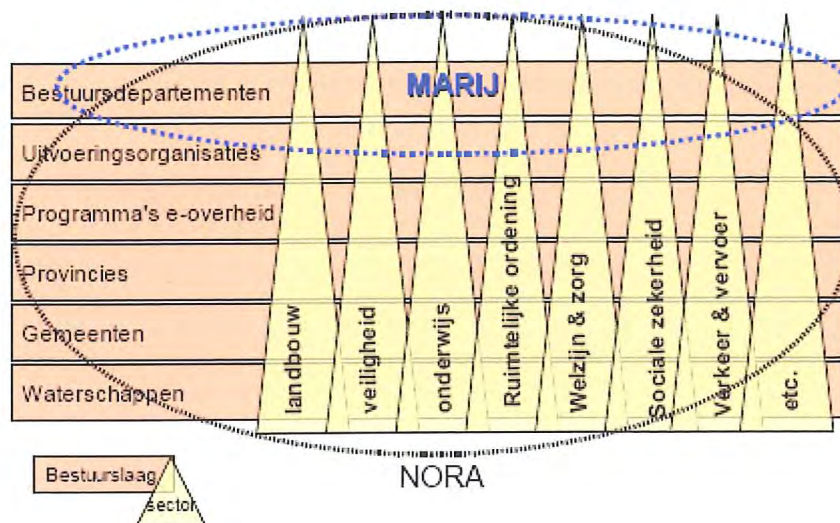
De standaarden hebben in principe het brede Justitie domein als werkingsgebied. In enkele gevallen is een standaard alleen benoemd als standaard benodigd voor de samenwerking (interoperabiliteit standaard) of deelgebied binnen dit domein.

In de voorkomende gevallen is dit werkingsgebied specifiek benoemd.

Mevr. van Zanen-Nieberg

Bedrijfsarchitectuur standaarden

Overheidsbrede standaarden



BA 2008-1 De NORA als referentie architectuur voor de overheid

[Comply or explain Standaard](#)

Interdepartementaal is afgesproken de NORA (Nederlandse Overheid Referentie Architectuur) voor de opbouw van de informatievoorziening als uitgangspunt te hanteren.
(Besluit College Standaardisatie)

BA 2008-2 De MARIJ als architectuur voor de Rijksoverheid

Facultatieve standaard

Vanuit ministerie van Binnenlandse Zaken is de opdracht gegeven om een specifieke Model Architectuur Rijksdienst MARIJ te ontwikkelen, gebaseerd op de NORA.
(gebruik nog niet vastgesteld)

BA 2008-3 De Webrichtlijnen

[Verplichte Standaard](#)

Overheidswebsites dienen toegankelijk te zijn voor alle burgers en organisaties in Nederland. Binnen Nederland is dit vastgelegd in de Webrichtlijnen.
(Besluit College Standaardisatie 2007)

BA 2008-4 Archiefstandaarden

[Comply or explain Standaard](#)

De Minister van BZK, in overleg met de Staatssecretaris van Cultuur, heeft in 2001 voorgeschreven dat ISO 15489 de basis is voor de functionele eisen tav informatie- en archiefbeheer.
(Wettelijke verplichting)

Justitie standaarden

BA 2008-5 Baseline ICT management

[Comply or explain Standaard](#)

Ten aanzien van ICT management heeft het Bedrijf Voering Overleg op basis van breed gedeelde inzichten normen opgesteld ten aanzien van ICT 'in control'.
(BVO besluit)

BA 2008-6 Kwaliteitsbeoordeling en beheersing Justitie

[Comply or explain Standaard](#)

Justitie heeft gekozen voor INK als de standaard voor de kwaliteitsbeoordeling en beheersing van de totale organisatie.
(BVO besluit)

BA 2008-7 Projectmanagement methode Justitie

Comply or explain Standaard

Justitie heeft gekozen voor Prince2 als de projectmanagementmethode voor het besturen en uitvoeren van Justitiebrede projecten met een ICT component.
(BVO besluit)

BA 2008-8 Testmethode Justitie

Comply or explain Standaard

Justitie heeft gekozen voor TMAP als de testmethode voor het testen van elektronische berichtuitwisseling tussen Justitiepartijen of voor het testen van applicaties die Justitiebreed worden gebruikt.
(BVO besluit)

Informatiearchitectuur Standaarden

Overheidsbrede richtlijnen op het gebied van Informatiearchitectuur

IA 2008-9 Rijksweb

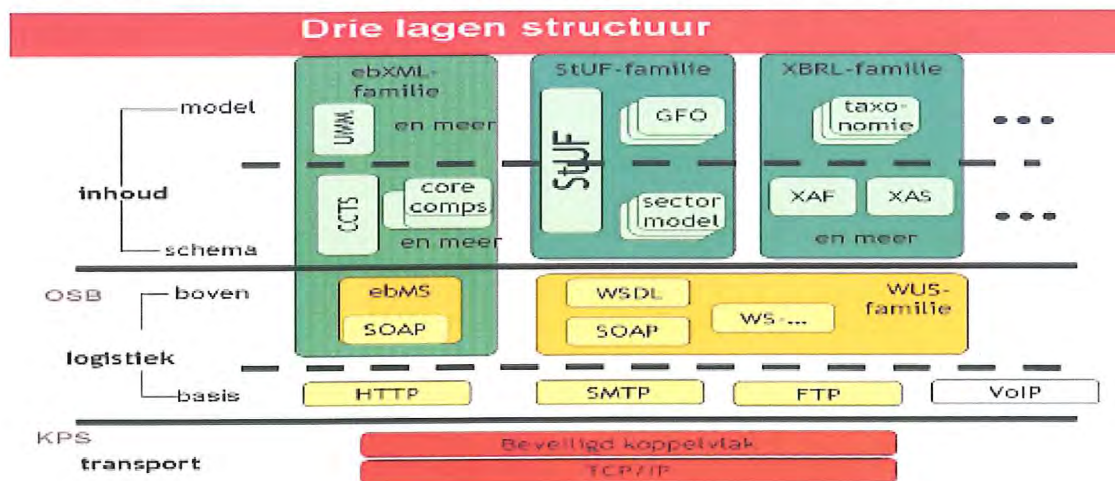
Verplichte Standaard

Rijksweb biedt de rijksmedewerkers toegang tot rijksbrede informatie. Rijksbreed is afgesproken (en verplicht gesteld), dat alle Rijksoverheidsmedewerkers toegang hebben tot de informatie op het Rijksweb.
(Besluit Bestuursraad)

Rijksweb biedt daarnaast de webdiensten: hosting van intra en internetten, wikipedia beheer, beveiligd e-mail, samenwerkruimtes.
Deze diensten zijn facultatief. Ten aanzien van het gebruik hiervan zijn interdepartementaal nog geen afspraken gemaakt.
Justitie neemt de dienst beveiligd e-mail tussen overheidsorganisaties al wel af.

Informatie uitwisseling

Het uitgangspunt "éénmaal aanleveren van gegevens, meervoudig gebruik" noodzaakt tot het maken van afspraken over de wijze waarop de elektronische berichten worden uitgewisseld en de wijze waarmee interconnectiviteit tussen bedrijfsnetwerken wordt vormgegeven binnen de overheid.



IA 2008-10 Overheid Service Bus

Verplichte Standaard

Voor de uitwisseling van berichten en services tussen organisaties in verschillende sectoren, moet gebruik gemaakt worden van de Overheid Service Bus.
(Besluit College Standaardisatie)

IA 2008-11 Koppelnetwerk Publieke Sectoren (KPS)

Verplichte Standaard

De Rijksoverheid is verplicht om voor haar elektronische Rijksoverheid-Rijksoverheid verkeer gebruik te maken van het KPS (met daarin opgenomen de Haagsche Ring).
(Besluit College Standaardisatie)

IA 2008-12 DIGid

Facultatieve standaard

Binnen de overheid is afgesproken, dat DigiD in principe wordt gebruikt om de digitale identiteit van burgers in digitale burger-overheid contacten vast te stellen.

(Nog niet vastgesteld)

De Basisregistraties

Een overheid (Balkenende 4) die: niet naar de bekende weg vraagt; klantgericht is; zich niet voor de gek laat houden; weet waar ze het over heeft; haar zaken op orde heeft en niet meer uitteeft dan nodig is, moet kunnen beschikken over betrouwbare en hoogwaardige geautomatiseerde gegevens. Basisregistraties zijn daarvoor het fundament.

Alle overheidsorganisaties zijn **verplicht** gebruik te gaan maken van de authentieke basisregistraties. De inhoud van dit **verplichte** gebruik is vastgelegd in de wet.

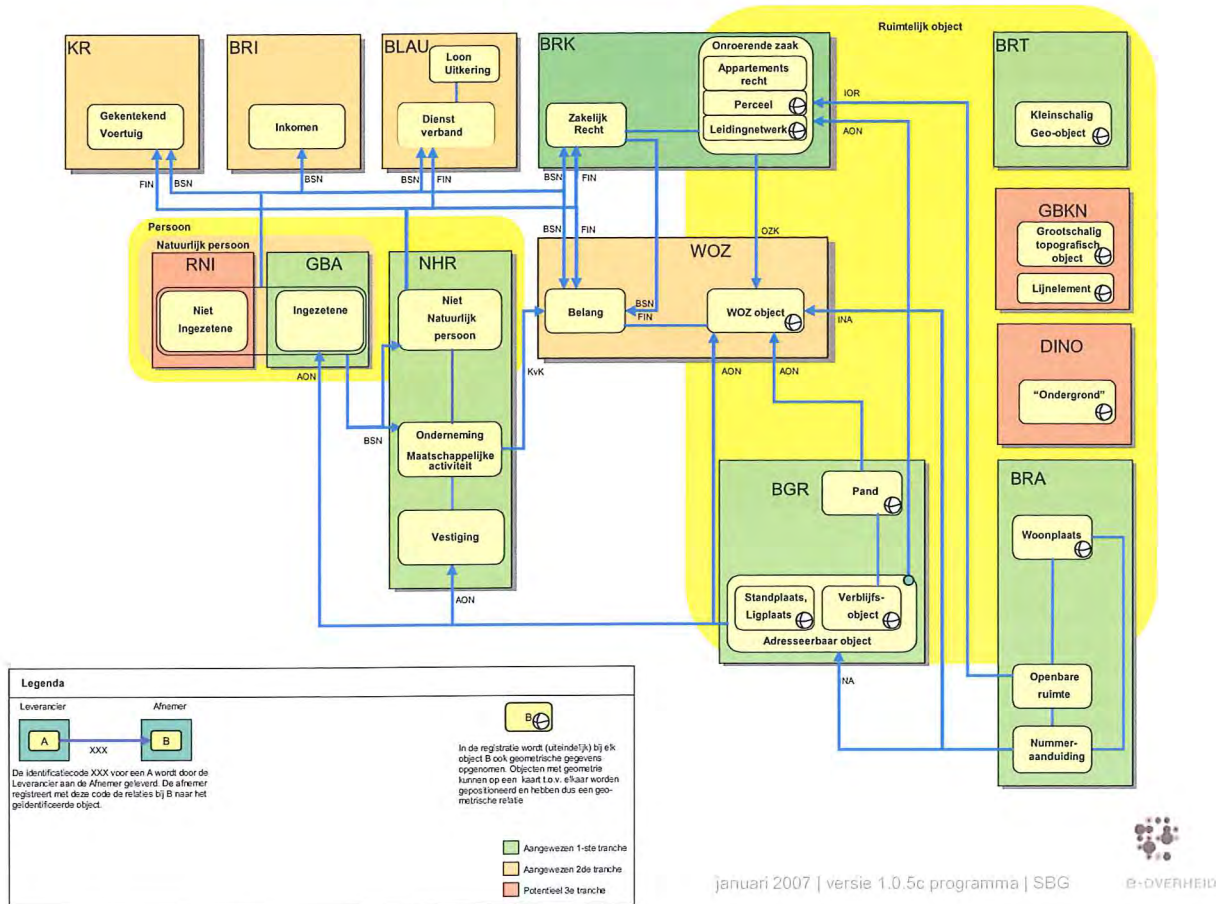
Er zijn inmiddels dertien basisregistraties aangewezen:

Gemeentelijke Basisadministratie personen (GBA); Handelsregister (NHR); Basis Gebouwen Registratie (BGR); Basis Registratie Topografie (BRT); Grootschalige Basiskaart Nederland (GBKN); Basisregistratie Adressen (BRA); Basis Registratie Kadaster (BRK); Kenteken Register (KR); Basis Registratie Inkomen (BRI); Basisregistratie WOZ (WOZ); Basisregistratie Lonen, Uitkeringsrelaties & Dienstverbanden (LUID), Register Niet Ingezetenen (RNI).

Zij zijn aan elkaar gekoppeld door Burgerservicenummer (BSN); Woonplaats Identificatie (WIN); Kamer van Koophandelnummer (KVK); Fiscaalnummer (FIN); Adresseerbaar Object Nummer (AON); Identificatie Nummer Aanduiding (INA); Identificatiecode Openbare Ruimte (IOR); Onroerend Zaak Kadastrale aanduiding (OZK). Deze basisregistraties met de unieke codes zullen in 2012 alle in gebruik zijn.

Het merendeel van de basisregistraties raakt het Justitiedomein te weten GBA; NHR; BGR; BRA; BRK; KR; BRI; LUID en RNI.

De ingebruikstelling van deze basisregistraties is stapsgewijs. In 2007 is de basisregistratie personen in gebruikgesteld met het BSN-nummer, in 2008 wordt de Basis Administratie Gebouwen in gebruik gesteld met het AONnummer.



IA 2008-13 Basisregistratie Personen

Verplichte Standaard

Sinds 1 januari 2007 is de authentieke basisregistratie personen in gebruik. Hierin staan de persoonsgegevens van alle in het GBA ingeschreven inwoners van Nederland. Het gebruik van deze basisregistratie is vanaf 2010 verplicht. (wettelijke verplichting)

IA 2008-14 Gebruik Burger Service Nummer

Verplichte Standaard

Ten behoeve van de ontsluiting van deze basisregistratie is de burger service nummer ontwikkeld. Burgers krijgen door middel van het burger service nummer een digitale, unieke identiteit. Dit BSN dient maximaal door overheidsorganisaties te worden toegepast. De minister van Binnenlandse Zaken heeft expliciet gemaakt in welk geval er gebruik van gemaakt moet worden. (wettelijke verplichting)

Justitie richtlijnen op het gebied van Informatiearchitectuur

Justitie applicaties t.b.v. overkoepelend beheer

Het overkoepelende beheer van het Justitiedomein wordt ondersteund met algemene beheersystemen. Deze vervullen een essentiële ondersteunende functie voor het management van het departement en daarmee voor de sturing van het departement als totaal. De zekerheid van de informatievoorziening via deze systemen is een hoofdprioriteit. Dit is de reden, waarom voor de beleidslijn is gekozen om het eigenaarschap van een algemeen beheersysteem te leggen bij de informatiemanager en in het onderhavige geval bij het functionele hoofd van het betreffende gebied. Aan dit eigenaarschap is onlosmakelijk gekoppeld de ontwikkeling van het systeem. Er zijn drie beheergroepen benoemd in deze:

IA 2008-15 Financiële systemen

Verplichte Standaard

Voor de financiële informatievoorziening en administratie wordt gebruik gemaakt van de door directie FEZ aangegeven applicaties.
(BVO besluit)

IA 2008-16 Personele systemen

Comply or explain Standaard

Voor de P-administraties wordt gebruik gemaakt van de door de afdeling DP&O aangedragen applicaties
(BVO besluit)

IA 2008-17 Documentaire informatiesystemen

Comply or explain Standaard

Er start een onderzoek of CDD toepasbaar is binnen de Justitie organisatie. JustID zal hierbij ondersteuning verlenen.
In de tussentijd zullen de Bestuursraad-leden geen eigen ontwikkelingen op dit gebied (digitaal archiveren) starten. Hierbij wordt, ter verduidelijking, opgemerkt dat dit inhoudt dat indien er andere nieuwe initiatieven worden aangeboden, de Bestuursraad-leden voorafgaand overleg hierover met JustID hebben.
(Bestuursraad besluit)

De Justitie informatie uitwisseling

Zoals bij het interdepartementale informatiebeleid is ook bij Justitie de focus van het informatiebeleid gericht op faciliteren van de interoperabiliteit tussen de verschillende autonome Justitiebedrijven onderling en tussen Justitie als bedrijf met de buitenwereld.
De onderlinge Justitie informatie-uitwisseling heeft echter door zijn aard additionele eisen aan robuustheid, betrouwbaarheid en informatiebeveiliging gesteld. Deze komen terug in de onderliggende standaarden.

IA 2008-18 Justitie Service Bus

Comply or explain Standaard

Voor de applicatie - applicatie communicatie tussen de systemen van de verschillende Justitiebedrijven wordt er binnen Justitie in principe gebruik gemaakt van de Justitie Service Bus. Deze Justitie Service Bus bestaat uit de volgende componenten:

- **Gebruik van één Justitie netwerk (Verplichte Standaard)**
Justitie heeft ervoor gekozen om alle Justitielocaties in één beveiligd netwerk aan elkaar te koppelen (WAN). Alle onderlinge (data) communicatie tussen de Justitieonderdelen vindt plaats via dit netwerk. (BVO besluit)
- **Justitie A-synchrone Berichtenstandaard (Comply or explain Standaard)**
JAB is de Justitie invulling van de overheidsstandaard eBMS. Alle nieuw te ontwikkelen applicaties maken voor hun verbindingen met andere applicaties gebruik van dit protocol. (BVO besluit)
- **Beveiligd koppelvlak (Verplichte Standaard)**
Er is één koppelpunt tussen het Justitienetwerk en de buitenwereld voor:
 - ⇒ verbindingen met (externe) websites op het internet;
 - ⇒ de uitwisseling van e-mail met het internet;
 - ⇒ de uitwisseling van bestanden met het internet;
 - ⇒ Tevens kan het koppelvlak voorzien in hosting en housing voorzieningen (openbaar en gesloten);
 - ⇒ alsmede koppeling met andere netwerken en systemen (bijvoorbeeld Haagse Ring en/of ketenpartners)(BVO besluit)
- **Justitie berichtenmakelaar (Comply or explain Standaard)**

Het gebruik van de JUBES is verplicht gesteld voor de Justitiepartijen binnen de strafrechtketen (DG RR besluit). Het gebruik van de JUBES is aanbevolen voor al het andere Justitie applicatie-applicatieverkeer (BVO besluit).

De Justitie Meta gegevens

Binnen Justitie is een set van Justitie basisgegevens (thesaurus; metadata woordenboeken en de ingevulde referentiegegevens) benoemd. Deze set van basisgegevens wordt centraal beheerd.

IA 2008-19 Justitie Metadata woordenboek

[Comply or explain Standaard](#)

Het Justitie Metadata woordenboek is momenteel ingevuld met het kernwoordenboek van Justitie, het gegevenswoordenboek informatievoorziening Vreemdelingenketen en het gegevenswoordenboek Strafrechtketen. In dit woordenboek zijn de basisgegevens en metadata (gehanteerde gegevensmodellen met de bijbehorende gegevensdefinities) over deze gegevens opgenomen.

Het Justitie Metadata woordenboek wordt gebruikt voor de ontsluiting van de 'gestructureerde' Justitie data.
(BVO besluit)

IA 2008-20 Justitie Thesaurus

[Comply or explain Standaard](#)

De Justitie Thesaurus bevat termen die de beleidsterreinen van Justitie inhoudelijk beschrijven. De thesaurus kan als een hiërarchische lijst maar ook als een omvangrijke termenlijst worden toegepast. De thesaurus herkent en verwerkt synoniemen en homoniemen.

De Justitie Thesaurus wordt gebruikt voor de ontsluiting van de 'ongestructureerde' data.
(BVO besluit)

IA 2008-21 Justitie referentie gegevens

[Comply or explain Standaard](#)

Binnen Justitie is de set van Justitie referentiegegevens benoemd. Deze set referentiegegevens wordt centraal beheerd. In deze set zijn de Strafrecht referentiegegevens + Vreemdelingenketen referentiegegevens + naamconventies opgenomen.

De Justitieonderdelen zijn verplicht om in hun externe digitale communicatie gebruik te maken van deze vastgestelde Justitie referentiegegevens.
(BVO besluit)

De Justitie identiteit gegevens

Om de juiste identiteit van een persoon, die met Justitie in aanraking komt te kunnen vaststellen, wordt er gebruik gemaakt van een standaard Justitie toolset met vingerafdrukken en frontale foto vereisten.

Justitie heeft vooralsnog één normenset vastgesteld. Voor opsporingsdoeleinden door Politie en Justitie gelden ingeval van foto's aanvullende normen betreffende het tweeluik en drieluik.

IA 2008-22 Justitie frontale foto vereisten

[Comply or explain Standaard](#)

De normen zijn gebaseerd op de volgende bronnen:

- Fotomatrix van paspoorten (BZK) die gebaseerd is op ISO/IEC nr952. Norm voor de identiteitsvaststelling.

- Forensisch Technische-norm. Norm voor de forensische opsporing. Kwaliteitsnorm van FCM.

Norm voor de foto's in Foto Confrontatie Module.

Besloten door de Coördinatiegroep Informatievoorziening Strafrechtsketen (CIS) op 5 september 2007. In beheer bij het programmabureau Progis (DGRR/DIRR/KIV).

IA 2008-23 Justitie vingerafdruk normen

[Comply or explain Standaard](#)

De normen zijn gebaseerd op de volgende bronnen:

- De ANSI-NIST-ITL-1-2007 standaard is leidend zoals gebruikt voor het nieuwe Havank. Hiervan is een Nederlandse implementatie die door de dNRI wordt beheerd (Interface Control Document SK-000056402-02).
- CJIS-RS-0010 (V7) Appendix F (image quality specifications). De inhoudelijke kwaliteit van de digitale afbeeldingen wordt vastgesteld met het kwaliteitsalgoritme NFIQ (NISTIR 7151) waarbij op een schaal van 1 tot 5 de kans is aangegeven dat de afbeelding kan worden teruggevonden (1= hoogste terugvindkans).

Besloten door de Coördinatiegroep Informatievoorziening Strafrechtsketen (CIS) op 5 september 2007. In beheer bij het programmabureau Progis (DGRR/DIRR/KIV).

Technische architectuur Standaarden

Overheidsbrede richtlijnen op het gebied van de technische architectuur

De technische componenten

TA 2008-24 Open Source Software

Facultatieve standaard

Het gebruik van open source software wordt door het kabinet krachtig gestimuleerd, maar niet als norm gesteld. Met een business case worden de kosten en baten van migratie in kaart gebracht, waarbij het Kabinet de voorkeur uitspreekt om bij gelijke geschiktheid te kiezen voor open source software. Aanbevolen wordt in de business case expliciet de Justitie Open Source Checklist op te nemen.

Gegevensopslag

TA 2008-25 Open Document Format (ODF)

Comply or explain Standaard

Het Kabinet heeft ODF (ISO 26300) benoemd als de overheid formaat (tekst, rekenbladen en presentaties) voor documenten in bewerking. Rijksdiensten moeten vanaf april 2008 ten minste ODF ondersteunen voor lezen, schrijven en uitwisselen van reviseerbare documenten; dit naast hun huidige standaarden.

(Besluit College Standaardisatie)

TA 2008-26 Portable Document Format (PDF)

Comply or explain Standaard

De toename van informatie die elektronisch opgeslagen wordt in documenten maakt het noodzakelijk die documenten goed te archiveren. Er is geen bezwaar om deze documenten in ODF op te slaan, maar in het geval van documenten waarvan het onwenselijk is dat ze reviseerbaar zijn, is het aan te bevelen een ander formaat te hanteren. PDF/A-1a (NEN-ISO 19005-1:2005 EN) is gekozen als standaard welke ODF gehanteerd worden voor de lange termijn archivering, specifiek voor niet-reviseerbare documenten.

(Besluit College Standaardisatie)

TA 2008-27 Portable Network Graphics (PNG)

Comply or explain Standaard

Portable Network Graphics (ISO/IEC 15948:2003) is het formaat van grafische afbeeldingen (lossless compressie) die gebruikt dient te worden binnen de ODF-documenten.

(Besluit College Standaardisatie)

TA 2008-28 Joint Photographic Experts Group (JPEG)

Comply or explain Standaard

Joint Photographic Experts Group (ISO/IEC IS 10918-1) is het formaat van grafische afbeeldingen (lossy compressie) die gebruikt dient te worden binnen de ODF- documenten.

(Besluit College Standaardisatie)

Justitie richtlijnen op het gebied van de technische architectuur

De technische componenten:

TA 2008-29 Justitie Identity Management

[Comply or explain Standaard](#)

Binnen Justitie is de afspraak gemaakt om op eenduidige wijze relevante attributen van alle Justitiemedewerkers (intern en extern) in één centraal informatiesysteem (Identity Store (Identity Management)) te verzamelen, synchroniseren en ter beschikking te stellen, bijvoorbeeld aan de sectorale Active Directories (AD), de Justitie Adressengids en Rijksweb. Bronsystemen, zoals het HRM systeem (SAP HR), leveren de informatie aan de Identity Store.

Het BSN mag gebruikt worden als key om deze administratie te ontsluiten.

Deze standaard is verplicht voor alle Justitie onderdelen uiterlijk op 31-12-2008.
(Besloten door BVO)

TA 2008-30 Justitie Extranet Portal

[Comply or explain Standaard](#)

De JEP is de enige voorziening, die Justitie applicaties met de daarbij behorende informatie via internet ter beschikking mag stellen. Deze voorziening is ingericht om Justitie medewerkers en partnerorganisaties, die zich buiten het Justitiedomein bevinden, te faciliteren.

De JEP maakt het mogelijk om een externe gebruiker (eigen medewerker of partner) op een transparante wijze toegang te geven tot informatie van Justitie. De JEP zorgt ervoor dat de identiteit van de gebruiker wordt vastgesteld en dat hij/zij alleen toegang krijgt tot de informatie waar hij/zij toe gerechtigd is.

(BVO besluit)

TA 2008-31 Justitie Browsers

[Comply or explain Standaard](#)

De binnen Justitie in gebruik zijnde browsers en plugins moeten zo zijn ingericht dat zij de inzage en het gebruik van de Justitiebrede en alle overheidsbrede intranetten (Justitiweb, P-direct en Rijksweb) veilig faciliteren, als ook de corporate internetsite van Justitie met de daarop aangeboden applicaties ondersteunen. Uitgangspunten zijn Firefox (open source) en MS Explorer (beiden in de laatste en voorlaatste versies).

(BVO besluit)

TA 2008-32 Diakrieten UTF-8

Facultatief

Binnen Justitie is als voorsortering op de afkondiging van een overheidsstandaard gekozen om nu al te standaardiseren op gebruik van UTF-8 als de verzameling van tekens.
(Standaardisatie commissie advies)

Standaarden voor beheer

Justitie standaard op het gebied van Beheer

Beh2008-33 IT beheermethode

[Comply or explain Standaard](#)

Justitie heeft gekozen voor ITIL als de Justitiebrede beheermethode voor de technische infrastructuur.
(BVO besluit)

Informatiebeveiliging Standaarden

Overheidsbrede richtlijnen op het gebied van Informatiebeveiliging

Voor de overheid is informatiebeveiliging een belangrijke kwestie. In dit verband zijn er 3 wetten in gebruik, zijn er 2 voorschriften voor de Rijksoverheid bepaald en 2 standaarden rijksbreed op dit gebied vastgesteld.

Bev2008-34 WBP

[Verplichte Standaard](#)

De belangrijkste regels voor het vastleggen en gebruiken van persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (WBP).
(Wettelijke verplichting)

Bev2008-35 Wet elektronische handtekening

[Verplichte Standaard](#)

Deze wet is de implementatie van de Europese richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
(Wettelijke verplichting)

Bev2008-36 Wet elektronisch bestuurlijk verkeer

Verplichte Standaard

Deze wet bevat de regels voor het verkeer langs elektronische weg tussen burgers/bedrijven en bestuursorganen en tussen bestuursorganen onderling (de zogenaamde Wet Elektronisch Bestuurlijk Verkeer, hierna te noemen: WEBV).
(Wettelijke verplichting)

Bev2008-37 VIR

Verplichte Standaard

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR), in 2007 geheel herzien, geldt als verplicht voor de gehele Rijksoverheid.
(NORA principe)

Bev2008-38 VIR BI

Verplichte Standaard

Voorschrift Informatiebeveiliging Rijksdienst, bijzondere informatie vastgesteld in maart 2004, geldt als verplicht voor de gehele Rijksoverheid
(NORA principe)

Bev2008-39 Code voor informatie beveiliging

Comply or explain Standaard

Deze bestaat uit de volgende normen:

- NEN-ISO/IEC 27001:2005.nl is de specificatie van management systemen van informatiebeveiliging
- NEN-ISO/IEC 27002:2007.nl is de set van best practices in informatiebeveiliging en dient in samenhang met de NEN-ISO/IEC 27001:2005.nl gehanteerd te worden.
(Besluit College Standaardisatie)

Bev2008-40 PKI-Overheid

Verplichte Standaard

PKI voor de overheid maakt het mogelijk om elektronisch betrouwbaar te communiceren met en binnen de overheid. Op basis van de PKI voor de overheid zijn overheidsinstanties onder meer in staat e-mailberichten en documenten te ondertekenen en versleutelen. Met behulp van certificaten kunnen medewerkers en burgers betrouwbaar via internet met de overheid en met elkaar communiceren. Speciaal daartoe aangewezen partijen geven deze certificaten (op een smartcard) uit aan personen en organisaties.
(Kabinet besluit)

Justitiebrede Informatiebeveiliging standaarden

Bev2008-41 Basisvoorziening informatiebeveiliging

Comply or explain Standaard

Alle Justitieorganisaties moeten aan Handboek beveiliging van Justitie concern voldoen. Dit document over basisvoorzieningen bevat een pakket aan maatregelen, die minimaal moeten worden getroffen voor de daarbij aangegeven situaties.
(Bestuursraad besluit)

Bijlage Mapping standaarden op de verschillende NORA-lagen

In de standaardenlijst op de NORA lagen 'gemapt'			Standaarden met een meervoudige relatie op andere NORA lagen	
Bedrijf architectuur	2008.1	2008.6	2008.9	2008.34
	2008.2	2008.7	2008.13	2008.35
	2008.3	2008.8	2008.14	2008.36
	2008.4		2008.24	2008.37
	2008.5		2008.30	2008.39
Informatie architectuur	2008.9	2008.14	2008.19	2008.4
	2008.10	2008.15	2008.20	2008.10
	2008.11	2008.16	2008.21	2008.24
	2008.12	2008.17	2008.22	2008.30
	2008.13	2008.18	2008.23	2008.31
Technische architectuur	2008.24	2008.29		2008.10
	2008.25	2008.30		2008.11
	2008.26	2008.31		2008.19
	2008.27	2008.32		2008.20
	2008.28			2008.21
Beheer	2008.33			2008.6
				2008.7
				2008.8
				2008.10
				2008.41
Beveiliging	2008.34	2008.39		2008.6
	2008.35	2008.40		
	2008.36	2008.41		
	2008.37			
	2008.38			

8 Gevraagde dienstverlening beheer tijdens project

8.1 De componenten van de gevraagde dienstverlening

De door de Opdrachtgever te verwerven dienstverlening omvat de volgende componenten:

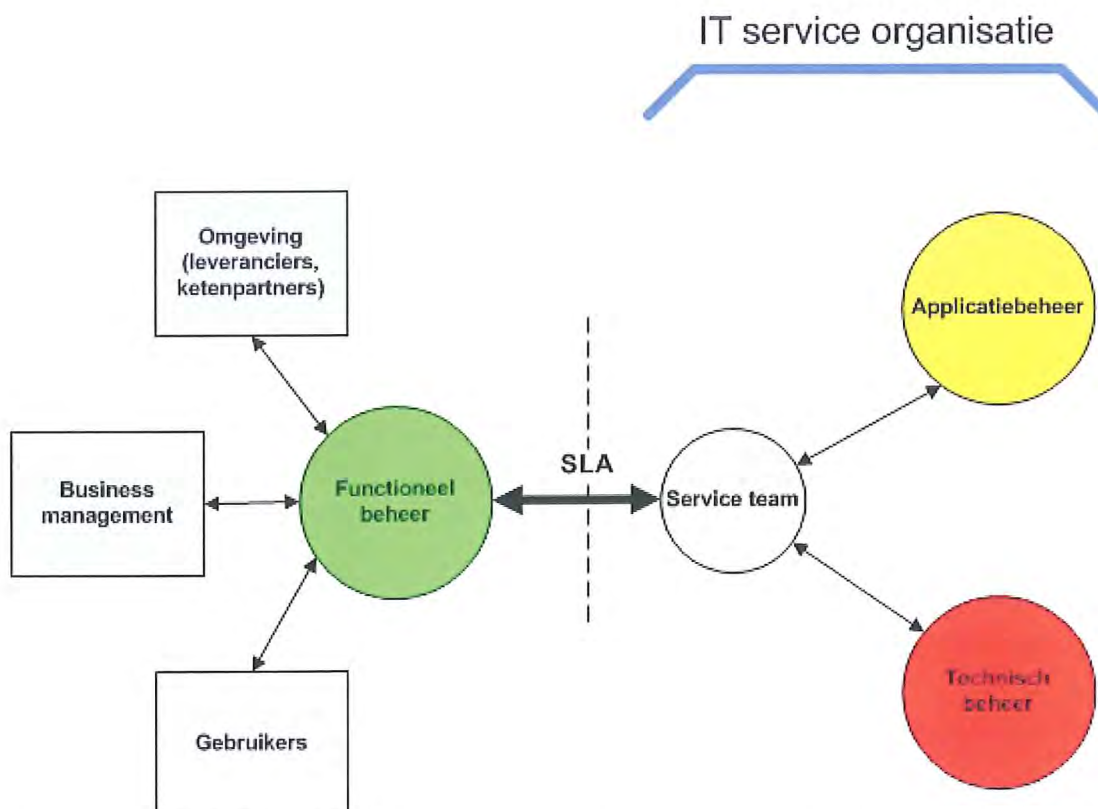
- Functioneel Beheer (deels)
- Technisch Applicatiebeheer
- Functioneel Applicatiebeheer

Bij Functioneel Beheer staat de opmerking “deels” omdat Functioneel Beheer voor een deel binnen de gebruikersorganisatie wordt uitgevoerd. Dit deel hoeft niet te worden meegenomen in de aanbidding. De aspecten van Functioneel Beheer welke momenteel door de huidige Beheerorganisatie worden ingevuld, dienen echter wel te worden meegenomen. Dit wordt hieronder verder uitgewerkt.

De component Technisch Beheer valt buiten de vraagstelling.

8.1.1 Functioneel Beheer

De drie onderkende vormen van beheer staan niet los van elkaar. Tussen het Functioneel Beheer domein en de andere twee beheerdomeinen bestaan nauwe relaties; in onderstaande figuur is de positionering van het Functioneel Beheer weergegeven.

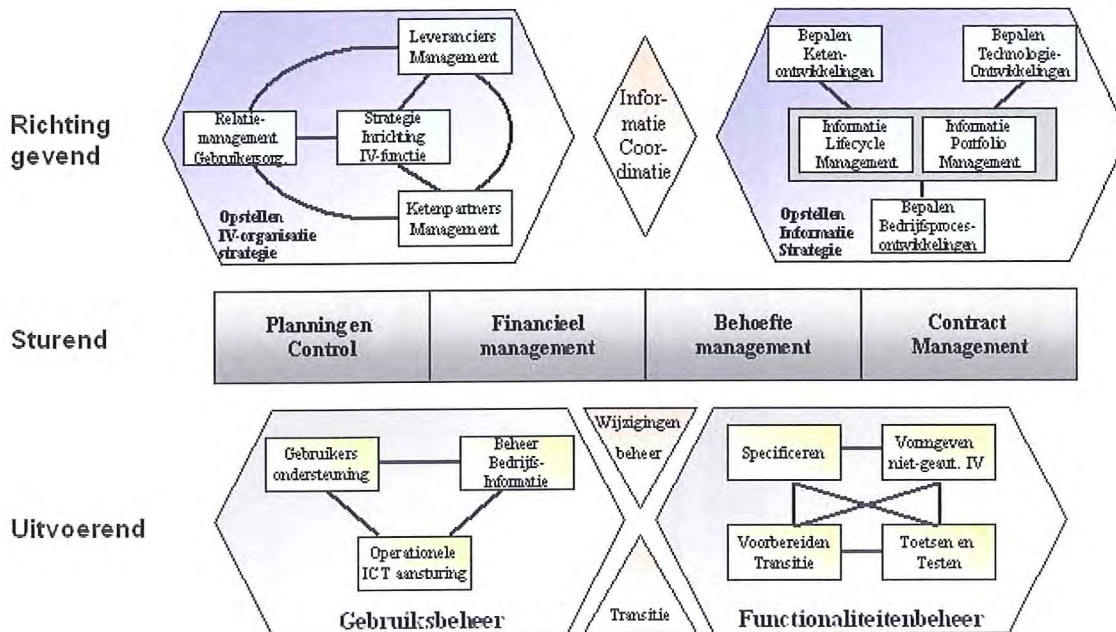


Functioneel Beheer is nadrukkelijk gepositioneerd als onderdeel van de gebruikersorganisatie.

Het domein van Functioneel Beheer is breed; het BISL framework onderkent 3 lagen:

- De uitvoerende laag: processen die zich bezig houden met het gebruik van de informatievoorziening en het definiëren van de eisen waaraan deze informatievoorziening inhoudelijk moet voldoen.
- De sturende laag: houdt zich bezig met kosten, opbrengsten, contracten en planningen.
- De richtinggevende laag: houdt zich bezig met het schetsen waar de informatievoorziening heen moet.

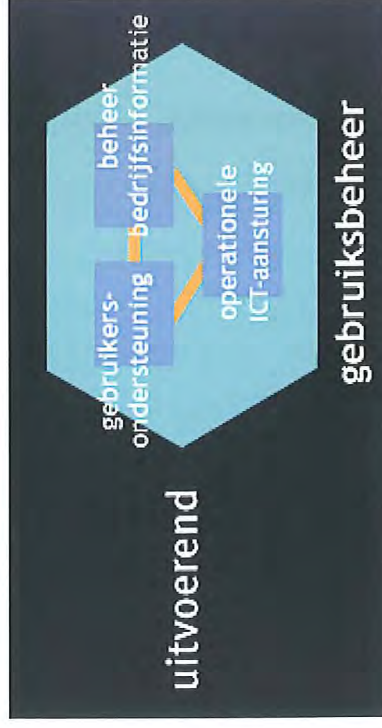
Binnen het model voor Functioneel Beheer worden clusters van processen onderscheiden:



In onderstaande tabellen wordt per cluster aangegeven welke processen relevant zijn (de processen die geheel binnen de gebruikersorganisatie vallen zijn niet verder beschreven). Van deze processen wordt de doelstelling genoemd, de activiteiten per (deel)proces, de producten en een toelichting. In deze toelichting wordt onder meer aangegeven hoe op dit moment invulling wordt gegeven aan dit proces.

De taken die momenteel worden uitgevoerd door de huidige Beheerorganisatie moeten worden meegenomen in de Inschrijving (vallen onder de Dienstverlening).

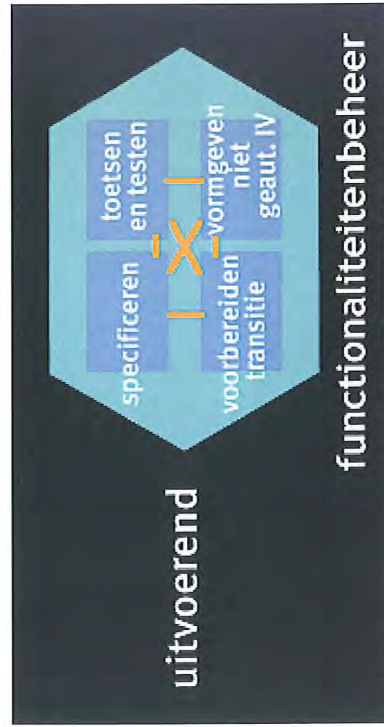
Uitvoerende processen



Cluster Gebruiksbeheer				
Hoofddoelstelling: Ondersteuning gebruikers				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Gebruikersondersteuning	Zorgdragen dat gebruikers optimaal kunnen werken met de bestaande informatievoorziening	A. Deelproces Call-registratie en —afhandeling A1. Registratie van een call A2. Beoordelen en Toewijzen van een call A3. Beantwoorden en afhandelen van een call A4. Terugkoppelen aan de melder A5. Afsluiten call B. Deelproces Gebruikers-communicatie B1. Gebruikers informeren (veranderingen, releases, e.d.) B2. Verzorgen en openstellen	A5.1 Afgehandelde calls B2.1 Communicatie met	Alle activiteiten van het deelproces Call-registratie en afhandeling (A1 tm A5) worden momenteel volledig door de Beheerorganisatie uitgevoerd. Hierbij vindt wel contact plaats met de gebruikers-organisatie (specificeren van de call, terugmelden van de call). De activiteiten van het deelproces Gebruikers-communicatie worden momenteel door de Beheerorganisatie en de gebruikersorganisatie geleverd.

Cluster Gebruiksbeheer				
Hoofddoelstelling: Ondersteuning gebruikers				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
		van communicatiekanalen, zoals nieuwsbrieven B3. Verzorgen van gebruikersoverleggen e.d.	gebruikersorganisatie (zoals releasekalenders, nieuwsbrieven ed) B3.1 Functioneel Beheerders overleg / kerngebruikers overleg	De Beheerorganisatie stelt nieuwsbrieven beschikbaar en stuurt per mail meldingen naar de Functioneel Beheerders (B1 en B2). Daarnaast neemt de Beheerorganisatie deel aan overleggen (B3). Hierbij heeft de Beheerorganisatie een adviserende rol. De overleggen worden georganiseerd door de gebruikersorganisatie.
		C. Deelproces Call-rapportage C1. Opstellen rapportages C2. Bespreken rapportages	Cl.1 Rapportages ten behoeve van sturende processen: de servicerapportages (v.w.b. gebruikersondersteuning)	De activiteiten van het deelproces Call-rapportage worden momenteel door de Beheerorganisatie en de gebruikersorganisatie geleverd. Het opstellen van de rapportages (C1) gebeurt door de Beheerorganisatie waarna deze gezamenlijk worden besproken (C2).
Beheer bedrijfsinformatie	Zorgdragen voor de correcte opzet en inhoud van de gegevens in de informatievoorziening	A. Deelproces Informeren en rapporteren A1. Het verstrekken van informatie over gegevens, gegevensdefinities, stuurparameters etc. A2. Periodiek verzorgen van overzichten en rapportages A3. Ad hoc gegevensverstrekkingen B.	A1.1 Informatieverstrekking m.b.t. gegevens	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie (A3 en B1) en de gebruikersorganisatie geleverd.

Cluster Gebruiksbeheer				
Hoofddoelstelling: Ondersteuning gebruikers				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
		Deelproces Wijzigen B1. Wijzigen van diverse soorten gegevens (stuurgegevens, gewone gegevens) n.a.v. vragen, veranderingen, wijzigingen of knelpunten/verstoringen B2. Het controleren van de correcte doorvoering ervan	B1.1 Aangepaste gegevens in systemen	



Cluster Functionaliteitenbeheer				
Hoofddoelstelling: Het komen tot wijzigingen in de informatievoorziening				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Vormgeven niet geautomatiseerde IV	Vervaardigen en onderhouden van de relevante documentatie voor het gebruik en Functioneel Beheer van het informatiesysteem (procedures, werkinstructies, handleidingen, etc)	A. Deelproces Uitwerken van het niet geautomatiseerde IV-proces B. Deelproces Vastleggen van het nieuwe werkproces	A1. Gebruikersdocumentatie A2. Werkinstructies B1. Handboeken B2. Formulieren	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie (A) en de gebruikersorganisatie (B) geleverd.
Voorbereiden transitie	Zorg dragen voor een probleemloze effectuering van de gewijzigde functionaliteit door het invullen van alle benodigde randvoorwaarden. 1. Uitvoeren van activiteiten voorafgaand aan de transitie 2. Voorbereiden activiteiten tijdens	A. Deelproces Plannen voorbereiding transitie A1. Opstellen implementatieplan B. Deelproces Uitvoering B1. Implementatie ICT B2. Implementatie in de gebruikersorganisatie	A1.1 Plan voorbereidings-activiteiten B1.2 Voorbereide ICT-organisatie B2.1 Voorbereide gebruikers-organisatie (incl. opleidingen)	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie (A1, B1, B2 en C1) en de gebruikersorganisatie (B2 en C1 v.w.b. de interne afstemming) geleverd. In sporadische gevallen wordt bij het proces A1 door de Beheerorganisatie een beroep

Cluster Functionaliteitenbeheer				
Hoofddoelstelling: Het komen tot wijzigingen in de informatievoorziening				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
	transitie	C. Deelproces Plannen transitie C1. Opstellen transitieplan	C1.1 Transitieplan (incl. Conversieplan / draaiboeken)	gedaan op de applicatie-leverancier.
Toetsen en testen	Zorgdragen dat de verandering op een vlekkeloze wijze wordt doorgevoerd en dat de gebruikte instrumenten, hulpmiddelen en andere ondersteuningsvormen correct zijn en correct werken	A. Deelproces voorbereiden toetsen en testen	A1. Testaanpak en —opzet	De gebruikersorganisatie is verantwoordelijk voor het organiseren en uitvoeren van de test (A). De Beheerorganisatie adviseert hierin desgewenst en ondersteunt bij de uitvoering van de acceptatietesten (B).
		B. Deelproces Uitvoeren acceptatietest (tevens ondersteuning)	B1. Test- en toetsresultaten	



Cluster Verbindende processen
Hoofddoelstelling: Koppeling gebruikersorganisatie met functionaliteitenbeheer

Cluster Verbindende processen				
Hoofddoelstelling: Koppeling gebruikersorganisatie met functionaliteitenbeheer				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Transitie	Daadwerkelijke effectivering van de veranderingen voor de eindgebruikers en feitelijk ingebruikname gewijzigde informatievoorziening	C2. Analyseren en beoordelen van afwijkingen die optreden bij de uitvoering A. Deelproces Uitvoeren A1. Communicatie A2. (doen) uitvoeren van gegevensconversies A3. Distributie benodigde materialen en procedures B. Deelproces Bewaken B1. Bewaking of voor alle onderkende objecten alle voorbereidende werkzaamheden juist en volledig zijn uitgevoerd en afgerond B2. Terugkoppeling over de voortgang van de transitie B3. Het registreren en doorgeven van eventuele knelpunten C. Deelproces Bijstellen C1. Extra conversieactiviteiten C2. Extra documentatie C3. Aanvullende kennisoverdracht C4. Nazorgactiviteiten na effectivering van de wijziging C5. Aangepaste opdracht naar de ICT-leverancier	Gewijzigde IV (informatie voorziening)	bijstellen worden momenteel door de Beheerorganisatie geleverd. De activiteiten van het deelproces Uitvoeren worden momenteel door de Beheerorganisatie (A1 en A2) en de gebruikersorganisatie (A1 en A3) geleverd. De activiteiten van het deelproces Bewaken is een samenspel tussen de Beheerorganisatie en de gebruikersorganisatie; de Beheerorganisatie bewaakt de uitvoering maar doet dit in samenspraak met de gebruikersorganisatie. De activiteiten van het deelproces Bijstellen worden momenteel door de Beheerorganisatie en de gebruikersorganisatie geleverd. Omdat de huidige beheerder calls m.b.t. gebruikers-ondersteuning voor haar rekening neemt is zij ook vaak de eerste die constateert dat extra maatregelen benodigd

Cluster Verbindende processen

Hoofddoelstelling: Koppeling gebruikersorganisatie met functionaliteitenbeheer

Processen	Doelstelling	Activiteiten	Producten	Toelichting
				zijn.

Sturende processen



sturende processen

Hoofddoelstelling: Bewaken activiteiten

Processen	Doelstelling	Activiteiten	Producten	Toelichting
Contractmanagement	Maken en bewaken van adequate afspraken t.a.v. de geautomatiseerde IV en de dienstverlening van ICT-leveranciers. Vastlegging van de afspraken in ICT-service contracten en SLA's	A. Deelproces Plannen B. Deelproces Controleren C. Deelproces Evalueren	A1. Afspraken (in de vorm van Service Level Agreements) C1. Dienstverleningrapportages (in de vorm van Service-rapportages)	De activiteiten van de deelprocessen Plannen / Controleren / Evalueren worden momenteel door de Beheerorganisatie en de gebruikersorganisatie geleverd. Er worden afspraken m.b.t. de dienstverlening gemaakt welke worden vastgelegd in SLA's. Over de dienstverlening wordt vervolgens maandelijks gerapporteerd door de Beheerorganisatie in de vorm van service-rapportages. Deze

Hoofddoelstelling: Bewaken activiteiten				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Planning en control	Het plannen, bewaken en bijsturen van de activiteiten van de organisatie die te maken hebben met het verzorgen van de informatievoorziening, zodat noodzakelijke inzet van informatievoorziening in de organisatie op tijd gerealiseerd wordt met een optimale inzet van capaciteit.	A. Deelproces Plannen B. Deelproces Controleren C. Deelproces Evalueren	A1. Plannings- en inzetoverzichten C1. Kengetallen (bijvoorbeeld doorlooptijden)	worden ook maandelijks besproken met de systeemeigenaren. De activiteiten van de deelprocessen Plannen / Controleren / Evalueren worden momenteel door de gebruikersorganisatie geleverd. De Beheerorganisatie levert een bijdrage in de vorm van de inplanning van de gebruikersondersteuning en het evalueren hiervan (in de vorm van overzichten en kengetallen).
Behoeftemanagement	Het zorgdragen dat de bedrijfsprocessen van een organisatie ondersteund of ingevuld worden door een goede informatievoorziening en Functioneel Beheerorganisatie.	A. Deelproces Plannen B. Deelproces Controleren C. Deelproces Evalueren	C1. Kengetallen (bijvoorbeeld aantallen calls, herkomst van de calls)	De activiteiten van de deelprocessen Plannen / Controleren / Evalueren worden momenteel door de gebruikersorganisatie geleverd. De Beheerorganisatie levert een bijdrage in de vorm van overzichten/kengetallen.

Bovenstaande tabellen laten zien dat de huidige Beheerorganisatie in de huidige situatie een substantieel deel van de operationele processen en een beperkt deel van de sturende processen van Functioneel Beheer voor haar rekening neemt, ook al vallen deze 'theoretisch' onder de verantwoording van de gebruikersorganisatie.

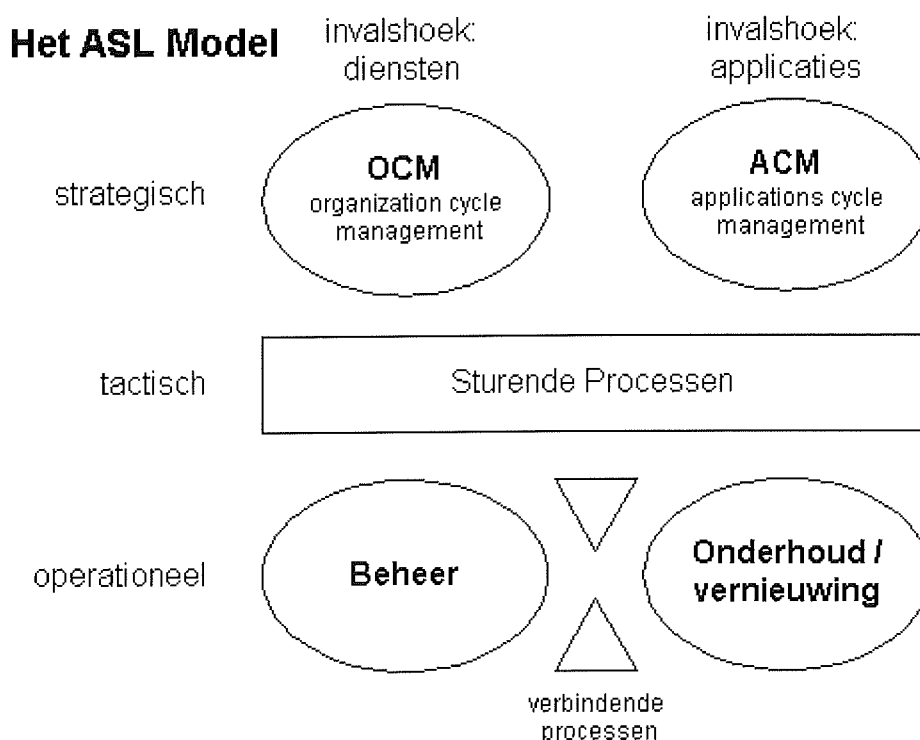
8.1.2 Applicatiebeheer

Het applicatiebeheer omvat het functioneel- en het technisch applicatiebeheer.

ASL kent, net zoals BSL, drie niveaus van processen:

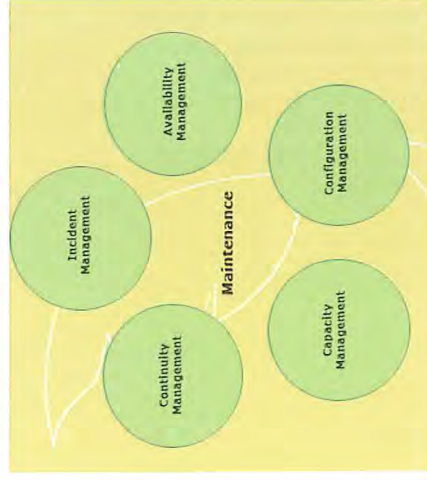
- Uitvoerend (de operationele processen)
- Sturend (de tactische processen)
- Beleidsbepalend (de strategische processen)

Binnen het model voor applicatiebeheer worden clusters van processen onderscheiden:



In onderstaande tabellen wordt per cluster aangegeven welke processen relevant zijn (de processen die geheel binnen de gebruikersorganisatie vallen zijn niet verder beschreven). Van deze processen wordt de doelstelling genoemd, de activiteiten per (deel)proces, de producten en een toelichting. In deze toelichting wordt onder meer aangegeven hoe op dit moment invulling wordt gegeven aan dit proces. Hier geldt wederom, met uitzondering van de clusters "onderhoud en vernieuwing" en "verbindende processen", dat de taken van de huidige Beheerorganisatie onder de gewenste dienstverlening vallen. De clusters "onderhoud en vernieuwing" en "verbindende processen" zijn optioneel en vallen buiten de fixed price. Tot aan de overdracht van het beheer aan de Beheerorganisatie worden wijzigingsverzoeken via de wijzigingsprocedure (zie de Overeenkomst) ingediend en voorzover niet vallend onder de garantie, als meerwerk beschouwd.

Operationele processen



Cluster Operationeel Beheer (Maintenance)				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Incidentbeheer	Zorgdragen voor continuïteit in de dienstverlening door een zo spoedig mogelijk herstel van het afgesproken servicelevel, wanneer hierop een afwijking wordt geconstateerd en het toegankelijk zijn voor vragen, opdrachten en opmerkingen van klanten m.b.t. te realiseren en gerealiseerde dienstverlening.	A. Proactieve communicatie naar gebruikers/ Functioneel Beheerders m.b.t. ondersteuning, informatie over wijzigingen en status applicatie B. Incidentaafhandeling: aannemen, registreren, evalueren, classificeren van meldingen/incidenten. Afhandelen, terugkoppelen en afsluiten meldingen /incidenten. C. Incidentenrapportage:	A1. Communicatie t.a.v. de applicatie en de diensten en informatie over wijzigingen en status applicatie. B1. Geregistreerde en afgehandelde incidenten B2. Meldingen naar andere beheerprocessen B3. Geregistreerde problemen C1. Servicerapportages	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B en C) In noodzakelijke gevallen wordt bij dit proces (afhandeling van B3) door de Beheerorganisatie een beroep gedaan op de applicatieleverancier.

Cluster Operationeel Beheer (Maintenance)				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Beschikbaarheidsbeheer	Het verzekeren dat de applicaties en diensten volgens de overeengekomen afspraken in staat zijn de gewenste functionaliteiten te bieden tijdens een bepaalde periode (beschikbaarheid) en overeenkomstig de verwachte functionaliteit (betrouwbaarheid).	A. Opstellen beschikbaarheidplan B. Beschikbaarheidsrealisatie C. Beschikbaarheidsbewaking D. Beschikbaarheidssturing	A1. Beschikbaarheids- en betrouwbaarheidseisen en maatregelen richting Technisch Beheer, onderhoud en Functioneel Beheer B1. Specificaties en maatregelen om genoemde eisen te realiseren B2. Verwerkingsplanning B3 Eisen (SLA's)richting onderaannemers C1. Beschikbaarheidsmetingen D1. Beschikbaarheidsrapportages	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B, C en D).
Capaciteitsbeheer	Doel is het op het juiste moment toewijzen van de juiste resources(mensen en middelen) en in juiste hoeveelheden aan de rondom het beheren, gebruiken en exploiteren van het systeem te leveren diensten, zodat een kosteneffectieve inzet van capaciteit bestaat en ook zal bestaan in relatie tot toekomstige behoeften van de organisatie.	A. Capaciteitsplanning B. Capaciteitsrealisatie C. Capaciteitsbewaking D. Capaciteitsrapportage	A1. Capaciteitsplan met daarin uitgangspunten en te bereiken doelstellingen A2. Vereiste performance B1. Maatregelen t.b.v extra capaciteit of om hogere prestaties te bereiken C1. Beheer van werklust en resources C2 Geregistreerde en afgehandelde 'capaciteits-incidenten' D1. capaciteitsoverzichten, gebruiksoverzicht en tendensoverzicht D2. rapportage tijdsbesteding en	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B, C en D).

Cluster Onderhoud en vernieuwing (Enhancement and Renovation)				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
	te zetten naar concrete en correcte wijzigingen in het geautomatiseerde informatiesysteem	impact B. Ontwerp technische oplossing C. Realisatie van de gewenste opzet D. Testen van de programma's E. Besturing	B1. Technisch ontwerp B2. Programma en productiedocumentatie B3. Technische testspecificaties C1. Nieuwe/ gewijzigde programmatuur C2. Nieuwe/ gewijzigde gegevensdefinities C3. Gewijzigde inrichtingsdocumentatie D1. Testresultaten E1. Voortgangsrapportage E2. Evaluatieverslag	door de Beheerorganisatie geleverd (A, B, C, D en E).
Testen	Het borgen dat de gewenste wijzigingen conform specificatie zijn gerealiseerd en dat de applicatie (na wijziging) correct gedrag vertoont.	A. Technische systeemtest B. Functionele (logische) systeemtest C. Ondersteuning productietest D. Besturing	A1/B1. Testresultaten A2/B2. Testverslagen D1. Voortgangsrapportage D2. Evaluatie	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B, C en D).
Implementatie	Het invullen van de noodzakelijke randvoorwaarden om te komen tot een foutloos gebruik van de nieuwe versie van de applicatie en afronding van het onderhoudsproces	A. Voorbereiden van de exploitatie B. Voorbereiding gebruikersorganisatie	A1. Ondersteuning bij voorbereiding en uitvoering acceptatietest B1. Ondersteuning Functioneel Beheer t.b.v. invoering in	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd. Hierbij vindt wel intensief contact plaats met de gebruikersorganisatie.

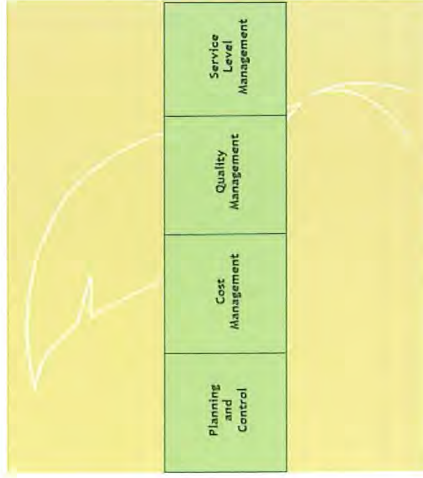
Cluster Onderhoud en vernieuwing (Enhancement and Renovation)				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
		C. Voorbereiding van de afronding van de release D. Afronding van de opdracht E. Sturing	gebruikersorganisatie C1. Aanpassing fouten uit acceptatietest D1. Opdracht decharge E1. Voortgangsrapportage E2. Evaluatie	



Cluster Verbindende processen				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Wijzigingenbeheer	Doel van het proces is ervoor zorg dragen dat een gestandaardiseerde werkwijze wordt gebruikt voor het doorvoeren van wijzigingen aan applicaties zodat afgestemd en geprioriteerd wijzigingen kunnen worden	A. Registratie (beheer) van wijzigingen B. Voorbereiden/inplannen releases	A1. Wijzigings-administratie B1. Release administratie	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B, C en D).

Cluster Verbindende processen				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
	doorgevoerd, om zodoende de geboden functionaliteit van de applicatie te verbeteren.	C. Bijstelling en bewaking releases D. Sturing en rapportage	C1. Informatie over wijzigingen en releases D1. Sturingsinformatie	
Programmabeheer en distributie	Het ter beschikking stellen van de juiste applicatie-objecten (of informatie daarover) aan de juiste processen op het juiste tijdstip	A. Registratie van objecten in het onderhoudsproces B. Uitgifte van objecten C. Informatieverstrekking naar onderhoudsproces D. Overzetten naar productieomgeving	A1. Applicatieobject-leveringen B1. Ondersteuning overgang tussen omgevingen en fasen C1. Informatie over objecten en statussen D1. Besturing	De activiteiten van deze deelprocessen worden momenteel door de Beheerorganisatie geleverd (A, B, C en D).

Sturende processen



Cluster Sturende processen				
Processen	Doelstelling	Activiteiten	Producten	Toelichting
Planning en Control	P&C kent als doelstelling het ervoor zorgdragen dat de afgesproken dienstverlening met de juiste capaciteit en conform oplevertijd gerealiseerd wordt door de juiste inzet van (mens)capaciteit op de juiste tijdstippen.	A. Planning B. Control C. Review	A1. Besturingsplannen (jaarplannen, projectplannen, releaseplannen) A2. Planningen A3. Middelen C1. Kengetallen C2. Rapportages	Dit sturende proces vindt binnen de huidige Beheerorganisatie plaats zodat kan worden voldaan aan de gemaakte afspraken met de klant.
Kosten management	Het ervoor zorgdragen dat de kosten van de applicaties en applicatiebeheer inzichtelijk en kosteneffectief zijn, de financiële informatie aanwezig is om verantwoord investeringen te kunnen doen en dat de financiële afspraken met de klant bewaakt worden, zodat er een kosteneffectieve	A. Budgettering B. Budgetbewaking C. Budgetreview	A1. Factuurinformatie A2. Financiële plannen B1. Uitputting C1. Financiële expertise	Dit sturende proces vindt binnen de huidige Beheerorganisatie plaats zodat de kosten inzichtelijk kunnen worden gemaakt en kunnen worden doorbelast aan de klant.

Cluster Sturende processen				
<i>Processen</i>	Doelstelling	Activiteiten	Producten	Toelichting
Kwaliteitsmanagement	Het zorgdragen voor de inzet van applicaties en applicatiebeheer geboden wordt. Het zorgdragen voor de (interne) kwaliteit van proces en product door deze te definiëren en te bewaken.	A. Kwaliteitsplanning B. Kwaliteitsbewaking C. Kwaliteitsreview	A1. Kwaliteitssysteem (hulpmiddelen, methoden, technieken, tools) A2. Kwaliteitsplan A3. Beheerplan C1. Problemen / toetsingen/ verbeteringen	Dit sturende proces vindt binnen de huidige Beheerorganisatie plaats zodat de dienstverlening naar de klant op een zo goed mogelijke manier kan plaatsvinden.
Service Level management	Het bewaken en verbeteren van de klanttevredenheid en het verbeteren van de aan klant geleverde dienstverlening.	A. Service definition: bedenken/bijstellen van afspraken B. Service control: bewaken en bijstellen C. Service review: evalueren	A1. Service level agreement A2. Realisatie B1. Service rapportages C1. Informatie over dienstverlening	Dit sturende proces vindt binnen de huidige Beheerorganisatie plaats zodat de dienstverlening naar de klant op een zo goed mogelijke manier kan plaatsvinden.

Bovenstaande tabellen laten zien dat de huidige Beheerorganisatie in de huidige situatie alle operationele processen van applicatiebeheer voor haar rekening neemt. Daarnaast zijn er de sturende processen die worden ingezet met het oog op de resultaatverantwoordelijkheid.

8.1.3 Technisch Beheer

Het Technisch Beheer valt buiten de gevraagde dienstverlening. Omdat Opdrachtnemer wordt gevraagd een beeld te schetsen van de wisselwerking met Technisch Beheer, wordt in deze paragraaf wel kort beschreven hoe het Technisch Beheer momenteel is ingericht.

Om dit te beschrijven wordt gebruik gemaakt van ITIL. ITIL is toegespitst op de IT-infrastructuur. Hieronder verstaat ITIL het geheel van apparatuur, programmatuur en datacommunicatiefaciliteiten plus de daarop van toepassing zijnde procedures, vaardigheden en documentatie die nodig zijn voor de IT dienstverlening.

ITIL bestaat uit 9 sets; 6 sets gaan over het dienstenbeheer en 3 sets over omgevingsbeheer.

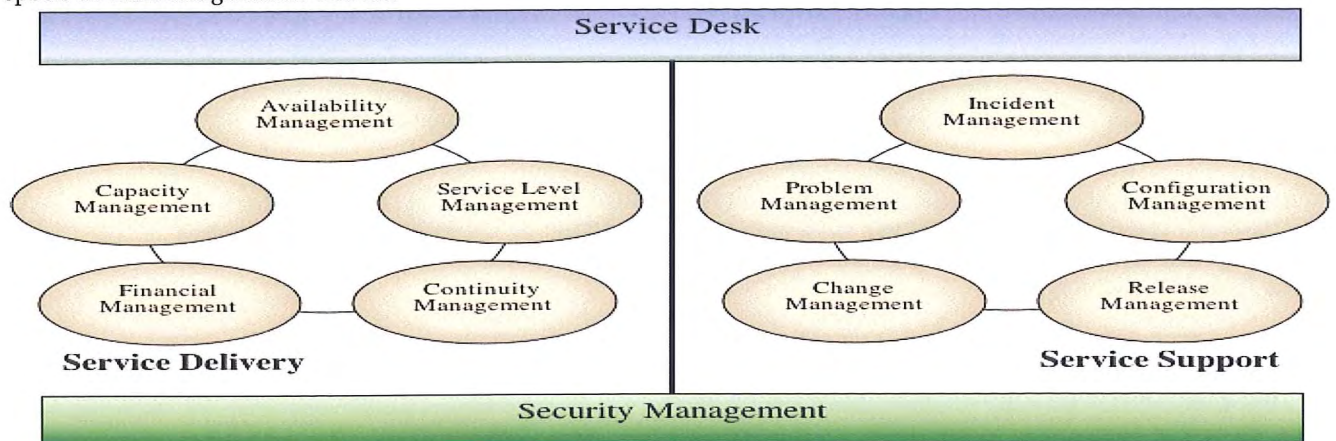
Hieronder wordt het dienstenbeheer verder uitgewerkt.

De sets over dienstenbeheer (service management) zijn:

1. Management (Managers Set)
 - Planning en rapportage IT dienstverlening
 - Organisatie van de IT dienstverlening
 - Kwaliteitsbeheer van de IT dienstverlening
 - Uitbesteden van het beheer
 - Relatiebeheer leveranciers
 - Relatiebeheer afnemers
2. Operationele processen (Service Support Set)
 - Configuratiebeheer
 - Probleembeheer
 - Wijzigingsbeheer
 - Helpdesk
 - Programmatuurbeheer en -distributie
3. Beheer van de IT dienstverlening (Service Delivery Set)
 - Dienstenniveaubeheer
 - Capaciteitsbeheer
 - Calamiteitenplanning
 - Beschikbaarheidsbeheer
 - Kostenbeheer
4. Software ondersteuning (Software Support)
 - Software lifecycle ondersteuning
 - Testen software voor operationeel gebruik
5. Netwerken (Networks Set)
 - Netwerkbeheer
 - Lokaal beheer
6. Rekencentrum (Computer Operation Set)
 - Computerbeheer
 - Geautomatiseerde werkprocessen
 - Onderhoudsbeheer
 - Installatie en acceptatie van apparatuur

De Beheerorganisatie richt zich met name op set 2 (de operationele processen) en set 3 (beheer van de IT dienstverlening); deze processen worden dan ook verder toegelicht. Maar ook in de overige sets

speelt de Beheerorganisatie een rol.



Set Operationele Processen (Service Support)			
Processen	Doelstelling	Activiteiten	Toelichting
Configuratiebeheer (Configuration Management)	Het doel van configuratie-beheer is het onder controle brengen van de IT infrastructuur en het verzorgen van de informatievoorziening over de IT infrastructuur.	• Identificatie van de configuratie items (CI's) • Beheer van de Configuratie Management Database • Statusbewaking van de CI's • Verificatie • Informatievoorziening	De Beheerorganisatie werkt met CI's en beheert deze in een CMDB. De CI's worden ook gebruikt voor rapportage naar de klant (bijvoorbeeld signaleren van trends in calls / incidenten).
Helpdesk (Incident Management)	Continuïteit van de dienstverlening door een zo spoedig mogelijk herstel van het afgesproken dienstenniveau wanneer een afwijking hierop wordt geconstateerd. De IT afdeling toegankelijk maken voor vragen, klachten en opmerkingen van klanten door te functioneren als dagelijks contactpunt.	• Aannemen en afhandelen van incidenten • Aannemen en beantwoorden van vragen • Bewaken van de voortgang van incidenten • Escaleren na incidenten • Signaleren van incidenten • Informeren van klanten • Configuratiebeheer van decentrale CI's • Verschaffen van management informatie • Het incident afhandelingproces reviewen	De Beheerorganisatie registreert calls m.b.t. de IT infrastructuur en de betreffende specialisten proberen de vragen dan wel incidenten zo goed en snel mogelijk af te handelen. Gegevens m.b.t. deze call-afhandeling (aantallen, behalen van normen ed.) wordt maandelijks gerapporteerd naar de klant.
Probleem beheer (Problem Management)	Het doel van probleembeheer is een zo hoog mogelijke stabiliteit van de IT dienstverlening na te streven door het achterhalen en wegnemen van fouten in de IT infrastructuur.	• Incidentbeheer • Probleemidentificatie en registratie • Classificatie • Allocatie mensen en middelen • Onderzoek en diagnose • Foutbeheer • Rapporteren aan management • Preventie	De Beheerorganisatie probeert problemen te signaleren (door het uitvoeren van controles) en registreert en behandelt problemen die door de gebruikers worden aangemeld. Hierbij kan een beroep worden gedaan op de applicatieleverancier.
Wijzigingsbeheer (Change Management)	Het doel van wijzigingsbeheer is de noodzakelijke veranderingen in de IT infrastructuur zodanig onder controle te brengen dat nieuwe fouten voorkomen worden.	• Acceptatie • Classificatie • Beoordeling en planning • Coördinatie • Rapportage	Verzoeken tot wijzigingen in de IT infrastructuur worden door de Beheerorganisatie geregistreerd en doorgevoerd.
Programmatuurbeheer en —distributie (Release Management)	Het doel van programmatuurbeheer en —distributie is het zekerstellen van alle programmatuuritems en de garantie dat alleen geteste en juiste versies van geautoriseerde	• Fysieke opslag van software • Acceptatietesten • Distributie van software • Implementatie van software items • Rapportage	Het programmatuurbeheer wordt momenteel door de Beheerorganisatie uitgevoerd. In de nieuwe situatie zal dit proces echter onder de verantwoordelijkheid van

Set Operationele Processen (Service Support)			
Processen	Doelstelling	Activiteiten	Toelichting
	programmatuur beschikbaar wordt gesteld voor exploitatie.		de toekomstige Beheerorganisatie vallen (v.w.b. de Leonardo-programmatuur). Dit wordt gezien als applicatiebeheer. Het Technisch Beheer (huidige Beheerorganisatie) is en blijft wel verantwoordelijk voor scripts e.d. op OS-niveau.

Set Beheer van de IT dienstverlening (Service Delivery)			
Processen	Doelstelling	Activiteiten	Toelichting
Dienstenniveaubehaar (Service Level Management)	Dienstenniveaubehaar is het proces van het beheer van de kwaliteit en de kwantiteit van de IT dienstverlening met het oog op de veranderende bedrijfsbehoeften en de behoeften van de gebruikers. Het doel is het komen tot een zakelijke vorm van dienstverlening die gebaseerd is op geschreven overeenkomsten tussen klanten en de IT organisatie over de kwaliteit van dienstverlening.	• Identificeren van IT behoeften • Verifiëren van de haalbaarheid • Het opstellen van Service Level Agreements (SLA's) • Het bewaken van de in de SLA's overeengekomen normen • Rapportage	De Beheerorganisatie heeft een aantal service level managers welke met de klant overleggen over de gewenste dienstverlening, ook met betrekking tot de IT; deze afspraken worden vastgelegd in SLA's en hierover wordt maandelijks gerapporteerd.
Capaciteitsbeheer (Capacity Management)	Het doel van capaciteitsbeheer is het scheppen van een optimale capaciteit, op het juiste moment, op de juiste plaats, tegen gerechtvaardigde kosten.	• Prestatiebeheer ◦ Zorgdragen voor naleving en nakoming van sla's ◦ Zorgdragen voor volledige benutting van de systeemelementen • Vraagbeheer (bijsturen van de vraag naar capaciteit) ◦ Analyse van bedrijfsactiviteiten van de klant ◦ Segmenteren van gebruikersgroepen ◦ Identificeren van informatiesystemen ◦ Voorspellen van gebruikersgedrag ◦ Bepalen van nieuwe behoeften ◦ Inschatten van de effecten van de gestelde bedrijfs-prioriteiten	De Beheerorganisatie richt zijn bedrijfsprocessen zodanig is dat het capaciteit optimaal wordt aangewend. Streven is om te voldoen aan de afspraken in de SLA's. Hiervoor is het nodig de vraag te bepalen door te kijken naar welke ontwikkelingen en welke druk de applicatie gaat krijgen de komende periode. Met deze informatie maakt de Beheerorganisatie een analyse waarna de capaciteitsrealisatie plaatsvindt. In dit proces worden verschillende zaken bewaakt: de

Set Beheer van de IT dienstverlening (Service Delivery)			
Processen	Doelstelling	Activiteiten	Toelichting
		• Werklustbeheer ◦ Identificeren en beschrijven van de werklusten ◦ Maken en onderhouden van een catalogus van de te verwachten werklusten ◦ Maken van voorspellingen over de werklust • Systeemelementenbeheer ◦ Opslagbeheer van data ◦ Plan van maken het opnieuw ter beschikking stellen van de systeemelementen na een calamiteit ◦ Aangeven wanneer nieuwe hardware aangeschaft moet worden ◦ Beoordelen van nieuwe hardware ◦ Onderhoud van configuratie schema's in samenwerking met configuratiebeheer ◦ Documenteren van systeemelementen ◦ Onderhouden van klantcontacten ◦ Public Relations van nieuwe technische mogelijkheden	werklust (zichtbaar maken van tendensen, veranderingen in aantallen gegevens/gebruikers), de resources (m.b.v. Configuratiebeheer inzicht krijgen in de benodigde capaciteit aan middelen voor applicaties en infrastructuur) en de prestaties (volgt de resultaten van de applicaties, signaleert trends en doet aanbevelingen). Als prestatiebeheer goed wordt uitgevoerd kan er pro-actief gereageerd worden. Veel input voor dit proces komt van Functioneel Beheer, verder is ook veel communicatie met Technisch Beheer (zij zorgen ook voor veranderingen aan de capaciteit).
Calamiteiten planning (Continuity Management)	Het doel van calamiteiten planning is zorg te dragen voor zo spoedig mogelijk herstel van de IT dienstverlening na een calamiteit.	• Risico analyse • Risico beheersing • Calamiteiten planning • Rapportage	De Beheerorganisatie heeft een calamiteitenplan en faciliteert een uitwijkomgeving.
Beschikbaarheidsbeheer (Availability Management)	Het doel van beschikbaarheidsbeheer is ondersteuning te verlenen in de verbetering van de beschikbaarheid van IT diensten voor gebruikers.	• Planning van de beschikbaarheid van IT • Bewaking • Toezicht • Samenwerking met probleembeheer om op pro-actieve wijze voorzorgsmaatregelen te nemen	De Beheerorganisatie heeft afspraken m.b.t. de beschikbaarheid van de diverse systemen vasgelegd in de SLA's. Er wordt gemonitord in hoeverre deze beschikbaarheid wordt gehaald. Dit wordt maandelijks gerapporteerd naar de klant.
Kostenbeheer van de IT diensten (Financial Management)	Het doel van kostenbeheer is het inzichtelijk maken (costing), bewaken (budgettering) en	• Opstellen van een jaarlijkse begroting • Realiseren van de begroting	De Beheerorganisatie maakt begrotingen en berekent haar kosten door naar de klanten.

Set Beheer van de IT dienstverlening (Service Delivery)			
Processen	Doelstelling	Activiteiten	Toelichting
	eventueel doorbelasten (charging) van de kosten van IT diensten aan de klanten.		

9 SLA Beheer projectfase

Dit onderdeel bevat een opzet voor de DNO (Diensten Niveau Overeenkomst) (of SLA, de engelse term: Service Level Agreement) voor het beheer van het Systeem Leonardo tijdens het project door Opdrachtnemer.

Een aantal zaken dient, na gunning, in overleg met Opdrachtnemer, nog verder te worden uitgewerkt.

9.1 Algemeen

9.1.1 Inleidende tekst

In deze overeenkomst zijn de kwalitatieve aspecten van de dienstverlening vastgelegd. Dit document schept voorwaarden en garanties zodanig dat het Systeem Leonardo voldoet aan de door DFEZ, DJI en Beheerorganisatie (lees Opdrachtnemer) vastgelegde niveau's van dienstverlening ten aanzien van het Beheer en Onderhoud.

Op basis van de hier afgesproken servicelevels vindt monitoring plaats van het geleverde dienstenniveau in relatie met het afgesproken niveau.

De kwantitatieve afspraken worden in de Nadere Overeenkomst (NOK) vastgelegd en zijn gebaseerd op de bedragen uit de aanbidding tijdens de Europese Aanbesteding van Opdrachtnemer. De procedures volgens welke de processen worden afgehandeld zijn vastgelegd in de Bijlagen bij deze DNO.

In deze DNO is DFEZ de systeemeigenaar van Leonardo. Hierna wordt Leonardo "het Systeem" genoemd.

9.1.2 DNO en gerelateerde documenten

Gerelateerde documenten zijn;

- Nadere Overeenkomsten (NOK). In de NOK staan afspraken over de kwantiteit en prijs van de door de Opdrachtnemer te leveren diensten.
- Leveringsvoorwaarden. Nog op te leveren.

In de Bijlagen bij deze DNO worden de procedures beschreven die niet in de DNO of NOK zijn vastgelegd. Een Bijlage kan gewijzigd worden na toestemming van de opdrachtgever DFEZ en de Service Level Manager van Opdrachtnemer.

9.1.3 Beschrijving van het systeem

Hieronder volgt een korte beschrijving van het Systeem en de bijhorende functionaliteiten.

Algemeen

<Uitwerken na gunning>

Leonardo

<Uitwerken na gunning>

9.1.4 Dienstverlening Opdrachtnemer

Het beheer van het systeem door Opdrachtnemer bestaat in het kort uit de volgende activiteiten:

1. Bieden van een **centrale helpdesk** voor de kernebruikers/functioneel beheerders van het systeem.
2. **Beschikbaarheid waarborgen** van het systeem.
3. Het **oplossen van technische applicatie storingen** ten behoeve van het systeem.
4. Het **instandhouden van de bestaande functionaliteit** van het systeem.
5. Het **instandhouden van capaciteit voor vernieuwingen en aanpassingen van de diensten**, inclusief de ontwikkel-, test- en acceptatieomgevingen. Tevens wordt de opleidingsomgeving in stand gehouden.

Optioneel (buiten fixed price):

6. Het uitvoeren van **wijzigingsbeheer**. Deze activiteit heeft betrekking op wijzigingen die niet worden toegewezen aan het project. Deze wijzigingen worden bij voorkeur releasematig uitgevoerd en in overleg met het projectteam.

Een uitgebreider overzicht is weergegeven in hoofdstuk 8.

Beperkingen en afhankelijkheden

Buiten de scope van deze DNO vallen:

- Informatiebeheer/contentbeheer, m.u.v. contentbeheer voor catalogi.
- Projecten en inbeheernames.

Op verzoek kan deze dienstverlening door Opdrachtnemer worden uitgevoerd en zal hiervoor een offerte worden opgesteld.

Buiten de dienstverlening van Opdrachtnemer vallen:

- Operationeel beheer JustitieNet. Door de individuele sectoren worden hiervoor aparte contracten afgesloten.
- Lokale automatisering binnen de sectoren/organisatieonderdelen.
- Eindgebruikerscursussen.
- Technisch Beheer

Randvoorwaarden en afhankelijkheden:

- Het aantal gebruikers is als volgt:
 - Hangt af van Plan van Aanpak en grootte eerste tranche.
- Gebruikers van het systeem dienen aangesloten te zijn op de justitiebrede centrale DNS structuur.
- Opdrachtgever dient zelf zorg te dragen voor een ongestoorde toegang voor de gebruikers tot het Justitienet (denk bv. aan firewall).
- Bij E-Factuur is Opdrachtnemer verantwoordelijk voor het beheer van het centrale gedeelte en zijn de organisatieonderdelen van Justitie (gedeeltelijk) verantwoordelijk voor het beheer van het decentrale gedeelte. De afspraken hierover zijn opgenomen in Bijlage 10.

Als niet voldaan wordt aan bovenstaande randvoorwaarden kan Opdrachtnemer de afgesproken servicelevels niet garanderen.

9.1.5 Looptijd

De looptijd van deze DNO is van de eerste go-live (de pilot) van het project Leonardo tot aan de afronding van de overdracht van het beheer aan de beheerorganisatie van Justitie.

Tussentijdse veranderingen in de DNO zijn in overleg mogelijk en worden tijdens het tactisch overleg, zie paragraaf 2.5 "Communicatie", besproken.

9.1.6 Verantwoordelijkheden

Van beide partijen wordt verwacht dat zij gezamenlijk verantwoordelijkheid dragen voor het realiseren van de in de overeenkomst vastgestelde dienstverlening en voor de instandhouding van de onderlinge communicatie. Daarnaast dienen partijen kennis te hebben van de vastgestelde procedures (zie Bijlagen) en deze na te leven.

Regie

De aansturing van de dienstverlening is samengevat onder het begrip "regie".

De regie op de dienstverlening wordt belegd bij één centraal organisatieonderdeel (de "regieorganisatie"). Leveranciersmanagement, inhuur voor projecten en contractmanagement vinden centraal bij de Opdrachtgever plaats. Ten behoeve van een goede regie op de dienstverlening zijn gegevens over de bedrijfsprocessen, de performance en de kosten noodzakelijk. In de "regieorganisatie" zal ook de vraag vanuit de business worden gecoördineerd. Het gaat hier bijvoorbeeld om goedgekeurde wijzigingsverzoeken. De organisatie zal de klantvraag goed moeten specificeren.

Verantwoordelijkheden Opdrachtnemer:

- Het beheren van de systemen conform de afgesproken servicelevels in deze DNO.
- De in deze DNO vastgelegde afspraken gelden voor de productieomgevingen van de systemen. De overige omgevingen worden beheerd zodanig dat de service levels uit deze DNO gewaarborgd worden. In speciale gevallen, zoals nieuwe projecten, kunnen hier aanvullende afspraken over worden gemaakt.
- Op basis van vastgestelde prestatie indicatoren rapporteren over de voortgang aan de opdrachtgever.
- Uitvoeren van de noodzakelijke patches en updates indien dit vanuit beheer noodzakelijk/wenselijk blijkt om de *bestaande* functionaliteit van het systeem in stand te houden.

Verantwoordelijkheden systeemeigenaar:

- Volledig indienen van storingsmeldingen bij de helpdesk.
- Het vaststellen van de *functionele* architecturen en standaarden.
- Benoemen van een opdrachtgever, gebruikerscoördinatoren en gebruikersorganisatie.

9.2 Service Level Management

9.2.1 Inleiding

Het Service Level Management is het proces van het besturen en beheersen van de kwaliteit en kwantiteit van de geleverde service zoals in deze DNO vastgelegd.

Dit document beschrijft het niveau van de kwaliteit van de dienstverlening ten aanzien van het onderhoud zoals dat door Opdrachtnemer wordt uitgevoerd.

De bepaling van de door Opdrachtnemer geleverde kwaliteit vindt plaats aan de hand van de indicatoren. De indicatoren zijn hieronder weergegeven.

9.2.2 Indicatoren

De volgende indicatoren worden onderkend, in hoofdstuk 2 worden de bijbehorende normen beschreven. Op een aantal indicatoren wordt maandelijks in de servicerapportage aan de opdrachtgever gerapporteerd, op de andere indicatoren wordt alleen gerapporteerd indien van toepassing.

Helpdesk en Incidentmanagement (zie 0 en 2.2)	
	Aantal en ingekomen, afgesloten en openstaande service calls.
	Onderverdeling van calls naar categorie
	Onderverdeling van calls naar organisatie-onderdeel
	Aantal gemiste telefoontjes t.o.v. de norm
	Percentage calls opgelost binnen de streeftijd
	Gemiddelde telefonische wachttijd helpdesk
Continuïteitsbeheer (zie 0)	
	Uitwijk
Beschikbaarheidsbeheer (zie 2.4)	
	Beschikbaarheid applicaties en databases
	Totale beschikbaarheid per applicatie
	Totale beschikbaarheid systeem
Capaciteitsbeheer (zie 2.5)	
	Dialoog Respons Tijd
Wijzigingsbeheer (zie 2.6)	

	Uitgesplitst naar wijzigingen die vallen onder verantwoordelijkheid van het project en wijzigingen die vallen onder verantwoordelijkheid van beheer. De SLA normen hebben slechts betrekking op laatstgenoemde categorie. Eerstgenoemde categorie mag worden gefilterd.
	Aantal uitgevoerde R&I's en percentage binnen de streeftijd
	Aantal doorgevoerde wijzigingen en percentage binnen de streeftijd
	Aantal openstaande wijzigingen
	Percentage aangeboden wijzigingen
	Percentage wijzigingen uitgevoerd conform de R&I
Klachten (zie 2.6.1)	
	Aantal klachten en afhandeling van klacht conform de klachten procedure

9.2.3 Rapportages

Servicerapportage

De opdrachtgever ontvangt maandelijks op de 14^e de Servicerapportage over de voorafgaande periode. In verband met weekeinden en feestdagen kan enigszins worden afgeweken van de 14^e; zie Bijlage 12 voor de planning.

Indien normen niet gehaald worden zal op de 7^e een zogeheten rookmelding gedaan worden. Dit houdt in dat uitsluitend gemeld wordt dat de norm niet is gehaald, zonder toelichting. De toelichting wordt opgenomen in de Servicerapportage.

Escalatie rapportage

Na een escalatie wordt een escalatierapportage opgeleverd, waarin de productieverstoring, de oorzaak, de genomen maatregelen tijdens de escalatie en zonodig preventieve maatregelen worden vermeld. De escalatierapportage wordt opgeleverd binnen 2 weken na afronding van de escalatie.

9.2.4 Communicatie

Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken servicelevels en het doorvoeren van veranderingen en verbeteringen (vastgelegd in eventuele verbeterplannen) is regelmatig overleg op diverse organisatie niveaus noodzakelijk.

De overlegstructuur tussen de Opdrachtgever en de Opdrachtnemer voorziet in 3 overlegvormen:

- strategisch overleg;
- tactisch overleg;
- operationeel overleg

De Opdrachtnemer is verantwoordelijk voor de vastlegging van elk van deze overlegvormen (notulen).

Dit overleg vindt plaats zoals weergegeven in onderstaande matrix:

Overlegstructuur	Aanwezigen	Onderwerpen	Frequentie
Strategisch overleg	Directeur FEZ Directeur Bedrijfsvoering DJI Directeur Opdrachtnemer	Regie Vraagbeheersing Contractuele aangelegenheden Escalatie voor Tactisch overleg Boetes bij niet behalen normen; Doelmatigheidsafspraken	Minimaal 1 x per jaar
Tactisch overleg:	Opdrachtgever DFEZ/DJI Service Level Manager Opdrachtnemer	Monitoring dienstenniveau (DNO), kostenontwikkeling (NOK) Releaseplanning Projecten Escalatie voor Operationeel overleg	Minimaal 1 x per kwartaal
Operationeel overleg:	Opdrachtgever	Ontwikkelingen Leonardo	Ad hoc

Leonardo	Senior medewerker financieel en functioneel beheer Senior medewerker concernadministratie Service Level Manager Opdrachtnemer Senior applicatiespecialist Opdrachtnemer	Diverse operationele zaken	
Operationeel overleg: kerngebruikersoverleg	Senior medewerker financieel en functioneel beheer Vertegenwoordigers functioneel beheerders Applicatiespecialist Opdrachtnemer	Informatie uitwisseling Bespreken wijzigingen * Diverse operationele zaken	1 x per maand
Operationeel overleg: FGO (Functioneel Gebruikers Overleg)	Opdrachtgever Sectorvertegenwoordigers Service Level Manager Opdrachtnemer Senior applicatiespecialist Opdrachtnemer	Ontwikkelingen Leonardo Vaststellen releases *	1 x per maand
Operationeel overleg WAC (Wijzigings Advies Commissie) *	Opdrachtgever Sectorvertegenwoordigers Senior applicatiespecialist Opdrachtnemer Releasemanager Opdrachtnemer	Bespreken R&I's Goedkeuren wijzigingen Samenstellen releases en melden voortgang	1 x per maand

Naast bovengenoemde overleggen kan ad hoc overleg plaatsvinden tussen de opdrachtgever en de Service Level Manager, afhankelijk van de ontwikkelingen en lopende projecten.

* Aangezien deze DNO betrekking heeft op het beheer door Opdrachtnemer tijdens een deel van het project, is de verwachting dat wijzigingsverzoeken in deze periode zullen worden afgehandeld door het project volgens een vastgestelde RFC-procedure. In dat geval komen de hier beschreven onderwerpen (bespreken wijzigingen en vaststellen releases) en overlegvorm vanuit de beheerrol niet aan de orde.

9.2.5 Communicatie in geval van escalaties

a) Klachtenprocedure

Opdrachtnemer ziet een klacht als teken, dat zij het als organisatie niet goed heeft gedaan, maar ook als kans om de dienstverlening te verbeteren. Klachten over de dienstverlening van Opdrachtnemer t.a.v. het systeem kunnen schriftelijk (email, fax of brief) worden ingediend bij Opdrachtnemer. Klachten kunnen worden ingediend bij de helpdesk of bij de Service Level Manager. Opdrachtnemer zal binnen twee werkdagen contact opnemen met de indiener van de klacht. Deze ontvangt binnen een week een schriftelijke bevestiging, waarin Opdrachtnemer aangeeft hoe zij de klacht aanpakt en op welke termijn de indiener van de klacht uitsluitel kan verwachten. Welke activiteiten Opdrachtnemer uitvoert hangt af van de klacht. Bij afronding van de klacht zal Opdrachtnemer schriftelijk verslag doen. De indiener van de klacht wordt tussentijds van de status van de klacht op de hoogte gehouden. Een klacht blijft openstaan totdat de indiener aangeeft, dat hij tevreden is met de oplossing en dat hij aangeeft dat de klacht kan worden afgesloten.

Opdrachtnemer bewaakt de klachten, en hierover wordt gerapporteerd in de Serviceraapportage.

Activiteit	Doorlooptijd
Eerste reactie	Binnen 2 werkdagen
Schriftelijke bevestiging	Binnen 5 werkdagen
Definitieve afhandeling	Afhankelijk van de inhoud van de klacht

b) Escalatieplatform

Is een storing niet binnen de daartoe gestelde tijd verholpen en is er geen zicht op de termijn waarbinnen de storing kan worden opgelost, dan wordt een hoger managementniveau ingelicht. Dit

wordt aangeduid als escalatie. Een escalatie kan zowel door de klant als door Opdrachtnemer geïnitieerd worden. Escalaties worden door de opdrachtgever aangemeld bij de Service Level Manager.

Voor storingen met een hoge impact en urgentie zal altijd een escalatieteam worden gevormd.

In geval van een escalatie wordt de functionaris van de systeemeigenaar op operationeel en tactisch niveau geïnformeerd. Informeren op strategisch niveau vindt plaats als de ernst van de escalatie daartoe aanleiding geeft. In bepaalde gevallen wordt de functionaris van de systeemeigenaar gevraagd een knoop door te hakken (bv als er investeringen moeten worden gedaan). Per niveau zijn de volgende functionarissen te onderscheiden.

Niveau	Functionaris Opdrachtgever	Functionaris Opdrachtnemer
Operationeel	Gebruiker	Helpdesk
Tactisch	Opdrachtgever	Service Level Manager
Strategisch	Directeur	Directeur

9.3 Servicelevels Beheer

9.3.1 Helpdesk

De helpdesk is het loket voor de kerngebruikers voor:

- Incidentmeldingen
- Klachten
- Service Requests: restores, passwords/autorisatie aanvragen, vragen over het systeemgebruik en vragen om ondersteuning bij het systeemgebruik, of bijvoorbeeld een vraag over de status van een incident
- Wijzigingsverzoeken

Bij incidentmeldingen dient de kerngebruiker minimaal onderstaande informatie te verstrekken:

- Welke handeling
- Bedrijfsnummer
- Documentnummer
- Een volledige beschrijving van de foutmelding

Per bedrijf mogen er twee kerngebruikers worden aangewezen. In bijzondere gevallen, zoals bij zeer grote organisatieonderdelen, kunnen maximaal vier kerngebruikers worden aangewezen. De systeemeigenaar neemt hierover de beslissing.

De helpdesk is op werkdagen telefonisch en via de mail bereikbaar van 7.30 tot 17.30 uur. Alle calls worden door de helpdesk aangenomen, geregistreerd, afgehandeld en/of in gang gezet. De helpdesk bewaakt de doorlooptijd van de afhandeling.

Service element	Omschrijving	Norm
Openingstijden helpdesk		Op werkdagen van 7:30 tot 17:30
Telefonische wachttijd	Wachttijd voor de aangenomen calls tot beller met een medewerker van de helpdesk wordt doorverbonden.	Maximaal 45 seconden
Gemiste calls	Telefoontjes die niet opgenomen worden door de helpdesk	4% van het totale aantal telefonische calls

9.3.2 Incidentmanagement

Er is sprake van een incident wanneer een gebruiker geen volledig gebruik van een aangeboden dienst kan maken.

Hieronder worden de normen weergegeven voor de verschillende soorten calls.

Service element	Omschrijving	Norm
Incidentmeldingen		

Service element	Omschrijving	Norm
ACUUT (prioriteit 1 of 2)	Het systeem is (deels) niet beschikbaar	80% binnen 2 uur opgelost
Incident (prioriteit 2)	Meer dan 1% van de gebruikers kan geen volledig gebruik maken van een aangeboden dienst.	80% binnen 1 werkdagen opgelost 100% binnen 2 werkdagen opgelost
Incident (prioriteit 3 of 4)	Een gebruiker kan geen volledig gebruik maken van een aangeboden dienst.	80% binnen 2 werkdagen opgelost 100% binnen 4 werkdagen opgelost
Service requests		
Gebruikersondersteuning	Gebruiker vraagt om ondersteuning bij het gebruik van het systeem.	80% binnen 4 werkdagen afgehandeld
Vraag	Gebruiker vraagt om meer informatie of heeft vragen over de gebruikersdocumentatie, opleidingen of het systeem.	80% binnen 4 werkdagen afgehandeld Voor de overige 20% van de vragen wordt binnen 2 dagen een nader te bepalen deadline afgesproken.
Resetten password	De gebruiker is zijn password vergeten en vraagt de helpdesk dit te resetten	80% binnen 10 minuten afgehandeld 100% binnen een half uur afgehandeld
Muteren autorisatie/ afgifte password	Een verzoek tot aanpassing van een autorisatie of aanmaken van een nieuwe gebruiker voor een systeem/dienst	80% binnen 2 werkdagen afgehandeld 100% binnen 5 werkdagen afgehandeld
Muteren data voor gebruiker	Gebruiker verzoekt om data aan te passen en/of toe te voegen in een systeem/dienst wat hij zelf niet kan aanpassen of toevoegen.	80% binnen 4 werkdagen afgehandeld
Productiewerk	Gereedzetten van het salarisjournaal	90% binnen 1 werkdag afgehandeld 100% binnen 2 werkdagen afgehandeld
Tijdstip		
Incidentmelding of service request.	Het is mogelijk dat samen met de gebruiker een tijdstip wordt afgesproken waarop een bepaald incident of service request opgelost dient te zijn	80% binnen de afgesproken tijd opgelost

9.3.2.1 Prioriteitsstelling voor het oplossen van incidenten

Als er meerdere incidenten tegelijk in behandeling zijn, moeten er prioriteiten gesteld worden. De prioriteiten worden als volgt vastgesteld:

- Prioriteit 1: het gehele systeem is niet beschikbaar
- Prioriteit 2: een gedeelte van het systeem is niet beschikbaar en/of een grote groep gebruikers kan geen gebruik maken van het systeem
- Prioriteit 3: één gebruiker kan geen gebruik maken van het systeem
- Prioriteit 4: één gebruiker kan nog wel gebruik maken van het systeem maar ondervindt problemen.

De systeemeigenaar kan indien gewenst afwijken van de voor de incidenten voorgestelde prioriteiten.

9.3.3 Continuïteitsbeheer

Een calamiteit is een ongeplande situatie als gevolg van een of meerdere ernstige incidenten. Er is sprake van een calamiteit als aan de volgende twee voorwaarden¹² wordt voldaan:

- Als gevolg van een productieverstorend probleem kan niet met het systeem worden gewerkt en

¹² Informatiebeveiligingsplan DFEZ, voor nadere details wordt hier naar verwezen

- het is duidelijk geworden dat er geen (tijdelijke) oplossing gevonden kan worden binnen 3x24 uur na het optreden van het productieverstorend probleem. Een dergelijk probleem kan betrekking hebben op de beschikbaarheid, de exclusiviteit en/of de integriteit van het systeem.

Het vaststellen of een productieverstorend probleem als calamiteit wordt gezien geschiedt door de Opdrachtgever nadat een analyse is verricht door de Opdrachtnemer. Indien sprake is van een productieverstoring dan wordt dit binnen 2 uur doorgegeven aan de systeemeigenaar en Opdrachtgever. Indien een calamiteit wordt erkend, treedt de escalatieprocedure in werking.

Als een escalatieteam wordt gevormd, zal in het eerste overleg van dit team een advies aan de systeemeigenaar worden geformuleerd omtrent het wel/niet opstarten van de uitwijkprocedure. Het advies zal gecommuniceerd worden door de Service Level Manager. De systeemeigenaar neemt de beslissing om wel/niet te starten met de uitwijkprocedure. Opdrachtnemer kan de volgende adviezen geven:

- Opdrachtnemer voorziet het probleem binnen een bepaalde tijd op te kunnen lossen (deze tijd wordt vermeld) en adviseert de uitwijkprocedure niet op te starten.
- Opdrachtnemer voorziet het probleem binnen een bepaalde tijd op te kunnen lossen (deze tijd wordt vermeld) en adviseert de uitwijkprocedure wel op te starten.
- Opdrachtnemer adviseert de uitwijkprocedure op te starten.
- Opdrachtnemer kan geen oplostijd geven voor het probleem en adviseert de uitwijkprocedure op te starten.

Voor het Systeem geldt het volgende:

Momenteel staan de productieomgevingen in Maasland en de uitwijkomgevingen in Woensdrecht. Operating system en applicatie zijn voor beide omgevingen gelijk; als er een wijziging wordt doorgevoerd op de applicatie wordt deze zowel in de productie- als de uitwijkomgeving doorgevoerd. Als er moet worden uitgeweken, dan dient de meest recente intacte situatie van de database op de uitwijkomgeving te worden geplaatst. Eventuele uitwijk vindt plaats in samenwerking met Technisch Beheer dat wordt uitgevoerd door de Beheerorganisatie van Justitie.

9.3.4 Beschikbaarheidsbeheer

Opdrachtnemer is verantwoordelijk voor het bewaken en waarborgen van de overeengekomen beschikbaarheid van het systeem. Beschikbaarheid is de mate waarin de applicatie gebruikt kan worden gedurende de openstellingstijd van een dienst.

Service element	Omschrijving	Norm
Openstellingstijd (Service Window)	De periode waarin de gebruikers het systeem af kunnen nemen en de beschikbaarheid is gegarandeerd volgens onderstaande norm.	Ma t/m vrij: 7.30 uur tot 18.00 uur
Beschikbaarheid	Beschikbaarheid is de mate waarin het systeem gebruikt kan worden gedurende openstellingstijd.	> 99,5% per applicatie > 97,5% voor het Systeem in zijn totaliteit
Beschikbaarheid buiten openstellingstijd	Buiten openstellingstijd kan het Systeem in principe ook afgenomen worden. De beschikbaarheid is dan niet gegarandeerd. Het is mogelijk dat het Systeem in het geheel niet beschikbaar is vanwege bijv. onderhoud.	geen
Beschikbaarheid tijdens jaarafsluiting	De beschikbaarheid tijdens de periode waarin de jaarafsluiting plaats vindt is gegarandeerd binnen de openstellingstijd. Deze periode wordt minimaal 3 maanden voor de jaarafsluiting door Opdrachtgever aangegeven. Zie ook Bijlage 9.	Ma t/m vrij: 7.30 uur tot 18.00 uur
Onderhoud	Correctief onderhoud nodig om beschikbaarheid te kunnen garanderen	Onderhoud wordt, daar waar het de beschikbaarheid beïnvloedt, gepleegd buiten de openstellingstijd.

9.3.5 Capaciteitsbeheer

Opdrachtnemer is als tactisch beheerder verantwoordelijk voor het informeren en adviseren van de opdrachtgever over de optimale inzet van de productiemiddelen om te kunnen voldoen aan de afgesproken dienstenniveaus. Uitgangspunt is een constante adequate performance van het systeem.

Als indicator is gekozen de responstijd voor de gebruiker. De responstijd is een maat voor de performance van het systeem, is relevant voor de gebruiker en levert input voor het capaciteitsbeheer

door Opdrachtnemer. Om de responstijd voor de gebruiker te meten is gekozen voor de Dialoog Respons Tijd.

De Dialoog Respons Tijd behelst de tijdspanne vanaf het verstrekken van de verwerkingsopdracht op het werkstation, via het verwerken ervan, tot het moment dat de resultaten van de opdracht op het beeldscherm van het werkstation worden gepresenteerd.

Deze waarde bevat tevens de tijd die nodig is om de data over het netwerk van het werkstation naar de applicatieserver te versturen en terug. Hoewel dit géén capaciteit van het werkstation of van de servers vraagt, kan de performance van het netwerk dus een aanzienlijke invloed hebben op de Dialoog Respons Tijd.

Service element	Omschrijving	Service Level
Dialoog Respons Tijd	De tijdspanne tussen het verstrekken van de verwerkingsopdracht door de gebruiker tot het moment dat de resultaten van de opdracht op het beeldscherm van het werkstation worden gepresenteerd.	90% binnen 0,8 seconde
Verwerkingstijd	De tijdspanne tussen het moment van binnenkomst van een verwerkingsopdracht van de gebruiker op de server tot het moment dat de resultaten van de opdracht van de server naar de gebruiker worden gezonden bedraagt: 90% binnen 0,5 seconde	90% binnen 0,5 seconde

9.3.6 Wijzigingsbeheer

Bij wijzigingen is onderscheid te maken tussen enerzijds correctieve wijzigingen en anderzijds adaptieve en perfectieve wijzigingen. Van binnengekomen wijzigingsverzoeken wordt eerst een R&I-analyse gemaakt. Het bijwerken van systeemdokumentatie valt onder wijzigingsbeheer. De procedures m.b.t. R&I-analyse en doorvoeren van wijzigingen zijn opgenomen in Bijlagen 4, 5 en 6.

Correctieve wijzigingen

Correctieve wijzigingen zijn gericht op het herstel van de oorspronkelijke functionaliteit van de systemen en worden doorgevoerd in de releases, of na overleg met de opdrachtgever in een weekrelease. Het betreft hier correctieve wijzigingen die niet onder het project Leonardo vallen.

Adaptieve en perfectieve wijzigingen

Adaptieve en perfectieve wijzigingen zijn gericht op het aanpassen dan wel verfijnen van de functionaliteit van de systemen en worden doorgevoerd in de releases. In de periode dat Opdrachtnemer het beheer doet, worden adaptieve en perfectieve wijzigingsverzoeken, die vallen buiten de specificaties van het project, via de changemanagementprocedure van het project Leonardo ingediend bij Opdrachtnemer. Dergelijke verzoeken worden behandeld op basis van nacalculatie.

In het geval ervoor wordt gekozen wijzigingsverzoeken te laten afhandelen door de Opdrachtnemer (dus buiten het project), gelden de volgende normen.

Service element	Omschrijving	Norm
Uitvoeren R&I-analyse	Risico- en Impactanalyse van de voorgestelde wijziging	Prioriteit: Normaal 70% binnen 4 weken uitgevoerd Hoog 80% binnen 2 weken uitgevoerd Urgent 90% binnen 2 dagen uitgevoerd
Uitvoeren wijzigingen	De wijziging wordt doorgevoerd	80% van de wijzigingen wordt conform plandatum doorgevoerd.

9.3.7 Client toepassingen op de werkplek

Bij client toepassingen op de werkplek kan het voorkomen dat op de werkplek aanpassingen nodig zijn als gevolg van een aanpassing aan het centrale systeem; een voorbeeld is een Graphical User Interface. Het is de verantwoordelijkheid van Opdrachtnemer om tijdige en volledige informatie aan de sectoren aan te leveren m.b.t. de aanpassingen op de werkplek en om eventuele testen te coördineren. Het is de verantwoordelijkheid van de sectoren om de aanpassingen tijdig en volledig door te voeren.

9.4 Bijlagen

9.4.1: Overzicht van Bijlagen

In de Bijlagen bij deze DNO worden de procedures beschreven die niet in de DNO of NOK zijn vastgelegd. Een Bijlage kan gewijzigd worden na toestemming van de opdrachtgevers van DFEZ en DJI en de Service Level Manager van Opdrachtnemer.

In Bijlage 1 wordt een overzicht van de Bijlagen van deze DNO gegeven. Tevens vindt het versiebeheer van de Bijlagen plaats in Bijlage 1.

Overzicht van de Bijlagen:

Bijlage	Titel	Versie	Datum goedkeuring
Bijlage 1	Overzicht van Bijlagen		
Bijlage 2	Contactenmatrix		
Bijlage 3	Definities en afkortingen		
Bijlage 4	Proces R&I-analyse en wijzigingen		
Bijlage 5	Procedure gebruikers- acceptatietests releases		
Bijlage 6	Procedure weekrelease		
Bijlage 7	Planning aanleveren Serviceraapportages		
Bijlage 8	Verantwoordelijkheden beheer E-Factuur		
Bijlage 9	Jaarafsluiting		

Goedkeuring Bijlage 1

Opdrachtgever DFEZ
Datum:
Handtekening:

Service Level Manager Opdrachtnemer
Datum:
Handtekening:

9.4.2: Contactenmatrix

Verantwoordelijkheid	Organisatie	Contactpersoon	Telefoon	Email
Directeur	DFEZ			
Systeemeigenaar	DFEZ			
Opdrachtgever	DFEZ			
Directeur	Opdrachtnemer			
Service Level Manager	Opdrachtnemer			
Algemeen nummer Opdrachtnemer	Opdrachtnemer			
Helpdesk/Meldingen	Opdrachtnemer			

9.4.3: Definities en afkortingen

Adaptieve wijziging

Een adaptieve wijziging is het toevoegen van nieuwe functionaliteit, het wijzigen van bestaande

functionaliteit of het verwijderen van functionaliteit.

Beschikbaarheid: de norm voor beschikbaarheid van de service wordt weergegeven als een percentage van de tijd waarbinnen ongestoord gebruik wordt gemaakt van de service

Correctieve wijziging

Een correctieve wijziging betreft het herstellen van een fout in het systeem om zo de oorspronkelijke functionaliteit te herstellen.

DEK-lijn

Beveiligde datacommunicatieverbinding tussen Justitienet en een partij/lokatie buiten Justitienet.

Impact

Impact 'Acuut' dient gebruikt te worden als een systeem/dienst niet beschikbaar is waardoor een gebruiker niet verder kan werken.

Impact 'Normaal' (ook impact 'Incident' genoemd) dient gebruik te worden als een gebruiker een verstoring ondervindt aan een systeem waardoor hij bepaalde taken niet kan uitvoeren maar waarbij hij wel verder kan werken.

NOK (Nadere overeenkomst)

Een overeenkomst tussen de opdrachtgever en Opdrachtnemer waarin —binnen de kaders van het opdrachtgever-convenant én binnen de afspraken over het basisniveau van dienstverlening (de DNO)— specifieke afspraken over de kwantiteit en prijs van de door Opdrachtnemer te leveren dienst gemaakt worden. De NOK wordt opgesteld zodra Opdrachtgever is geselecteerd en is gebaseerd op diens Inschrijving.

Perfectieve wijziging

Een perfectieve wijziging is een wijziging die zorgt voor een verfijning van bestaande functionaliteit van het systeem.

R&I-analyse

Een R&I analyse staat voor “risico- en impactanalyse”. Als een klant een wijziging in het systeem wil door laten voeren, zal Opdrachtnemer eerst een R&I analyse uitvoeren om te kijken wat de impact is van die specifieke wijziging op het functioneren van het systeem. De oplossingsrichtingen als een indicatie van de kosten staan ook in de R&I vermeld. Op basis van die analyse wordt samen met de klant besloten om de wijziging wel of niet door te voeren.

VIR

Voorschrift Informatiebeveiliging Rijksoverheid.

9.4.4: Proces R&I-analyse en wijzigingen

Hieronder wordt het wijzigingsproces beschreven voor de verschillende systemen.

Leonardo

1. Indienen wijzigingsverzoek

(Een beperkte groep) Functioneel beheerders mogen een wijzigingsverzoek indienen in de categorieën normaal en hoog. FGO-leden mogen een wijzigingsverzoek met de categorie urgent indienen. Een wijzigingsverzoek wordt ingediend via de helpdesk van Opdrachtnemer.

2. Opstellen R&I

De R&I-analyse wordt opgesteld door Opdrachtnemer en bevat de risico's bij doorvoeren van de wijziging en de impact op de gebruikers. R&I-analyses worden afgehandeld volgens het FIFO-principe per categorie.

3. Afstemmen R&I

Na het opstellen van de R&I wordt deze afgestemd met de indiener.

4. Goedkeuring WAC

Na afstemming met de indiener wordt de R&I voorgelegd aan het WAC. Het WAC kan de volgende besluiten nemen:

- Goedkeuring: na goedkeuring van een R&I kan deze worden ingepland in een release.
- Vervolgonderzoek: er is een uitgebreider onderzoek nodig naar impact en risico's.
- Advies door Opdrachtnemer om wijzigingsverzoek af te keuren: sommige wijzigingen worden afgekeurd omdat deze bijv. teveel maatwerk met zich meebrengen
- Afkeuren: de R&I is onvoldoende uitgewerkt en doorloopt de stappen 2 en 3 opnieuw.

Wijzigingen waarover het WAC geen beslissing kan nemen worden doorverwezen naar het FGO.

5. Bouw wijzigingen

Zodra een R&I is goedgekeurd door het WAC begint Opdrachtnemer met bouwen van de wijziging.

6. Bevriezen/vaststellen samenstelling release

Hierover dienen nader afspraken te worden gemaakt. Kleine/spoedeisende wijzigingen worden tussentijds in overleg met de systeemeigenaar uitgevoerd. Deze wijzigingen worden in principe via een weekrelease uitgevoerd. Zie hiervoor Bijlage 6.

7. Gebruikersacceptatietest

De gebruikersacceptatietest wordt uitgevoerd conform de hiervoor geldende procedures. Zie Bijlage 7.

8. Implementatie wijzigingen

Wijzigingen die zijn goedgekeurd in de gebruikersacceptatietest worden geïmplementeerd door Opdrachtnemer.

9. Evaluatie

Nader te bepalen.

9.4.5: Procedure gebruikersacceptatietests releases

Nader uit te werken na gunning.

9.4.6: Procedure weekreleases

Nader uit te werken na gunning.

9.4.7: Planning aanleveren Service- en Financiële rapportages

Rookmelding vindt in principe plaats op de 7^e van de maand.

Servicerrapportages worden in principe op de 14^e van de maand verstuurd.

Hierin kan enige verschuiving plaatsvinden vanwege weekeinden en feestdagen. Hieronder wordt de precieze planning weergegeven: <Nader uit te werken na gunning>.

Voor de financiële rookmeldingen en rapportages is de intentie om deze op dezelfde data te versturen als de servicerrapportages.

9.4.8: Verantwoordelijkheden beheer E-Factuur

In deze bijlage worden de afspraken m.b.t. decentraal beheer opgenomen. Deze komen tot stand in overleg met sectoren.

Nader uit te werken na gunning.

9.4.9: Jaarafsluiting

Werkinstructies jaarovergang

De werkinstructies jaarovergang Leonardo zijn te vinden op een nader te bepalen locatie.

Beschikbaarheid jaarafsluiting

Een beschikbaarheid van 100% is niet te garanderen, zelfs niet als gebruik wordt gemaakt van een aantal redundante systemen. Daarbij nemen de kosten sterk toe bij gebruik van redundante systemen.

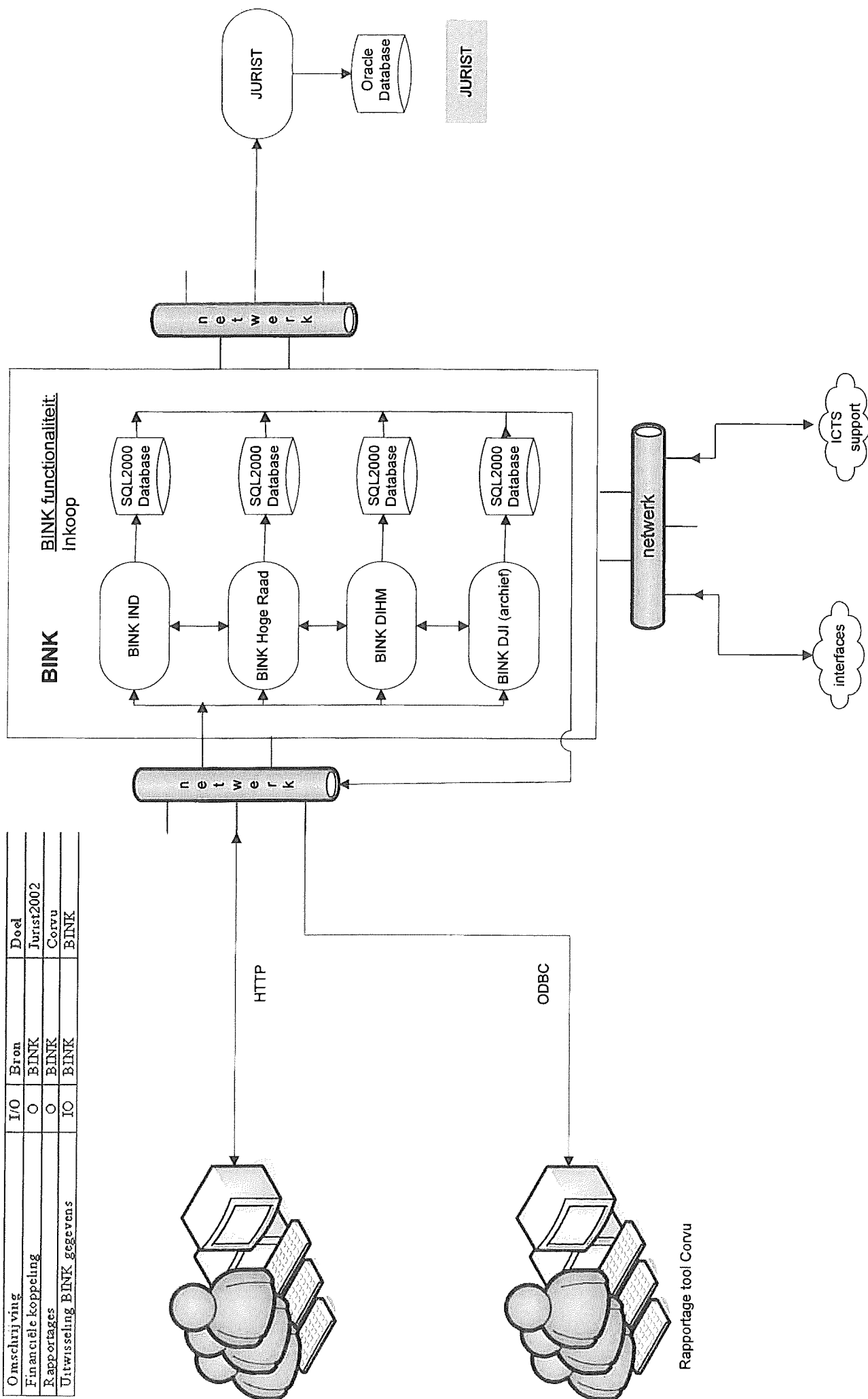
De achtergrond van de vraag naar 100% beschikbaarheid is het belang van de jaar- en maandafsluitingen in het financiële proces en het afbreukrisico als de systemen niet beschikbaar zijn in deze periodes. Opdrachtnemer onderkent dit belang en adviseert om een aantal procedurele maatregelen te nemen in de genoemde periodes om de beschikbaarheid zo groot mogelijk te maken.

Om zorg te dragen voor een zo groot mogelijke beschikbaarheid in de perioden van de maand- en jaarafsluitingen neemt Opdrachtnemer de volgende maatregelen:

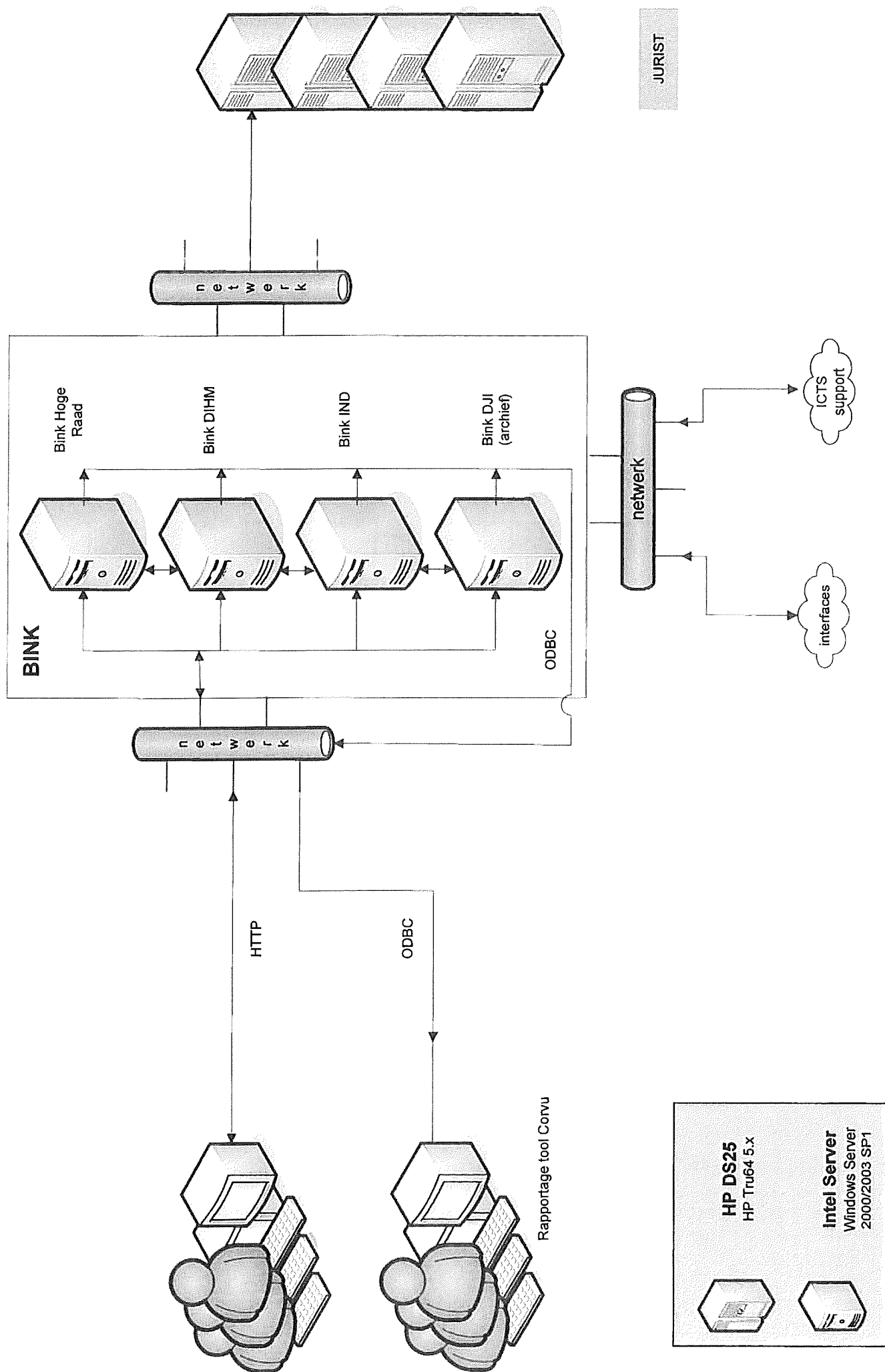
- Applicatie:
 - Op applicatieniveau geldt tijdens de jaarafsluiting een verhoogde staat van paraatheid. Dit betekent bijvoorbeeld een strakkere monitoring van de applicaties.
 - Gedurende twee weken voor en na de jaarafsluiting een ontwikkelstop met uitzondering voor urgente wijzigingen.

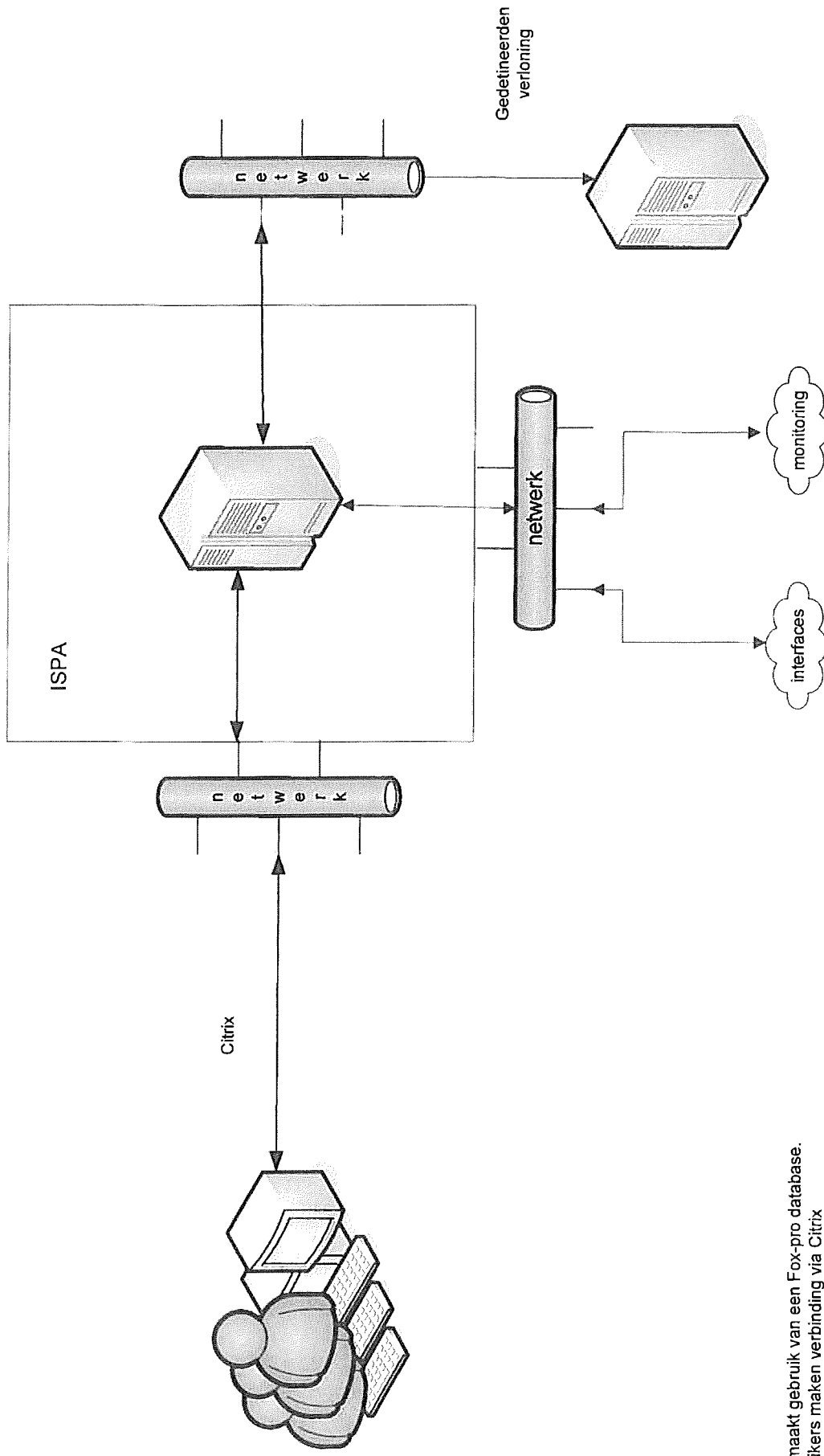
BINK Applicatiestructuur Productie

Omschrijving	I/O	Bron	Doel
Financiële koppeling	O	BINK	Jurist2002
Rapportages	O	BINK	Corvu
Uitwisseling BINK gegevens	IO	BINK	BINK



BINK Infrastructuur Productie

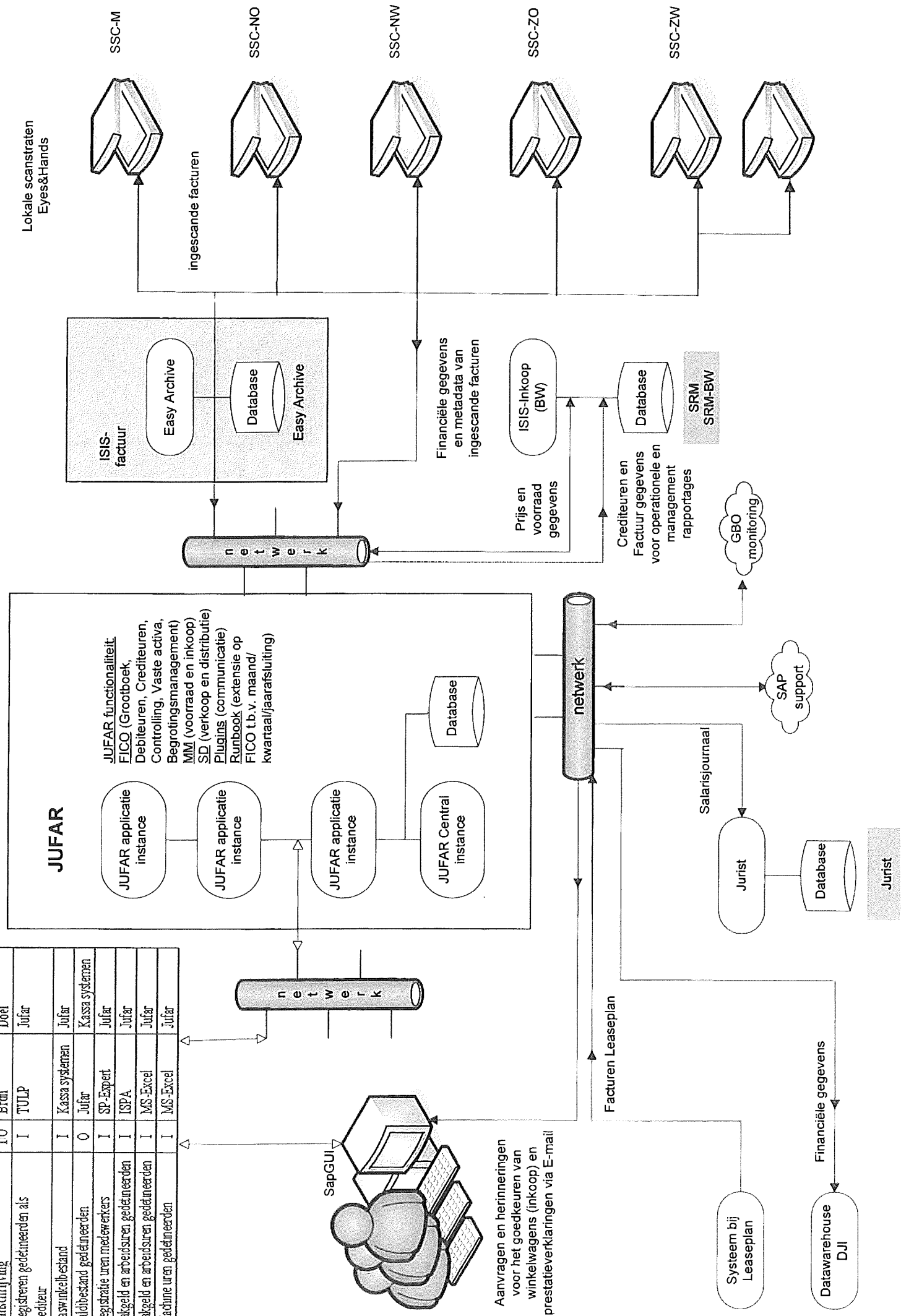




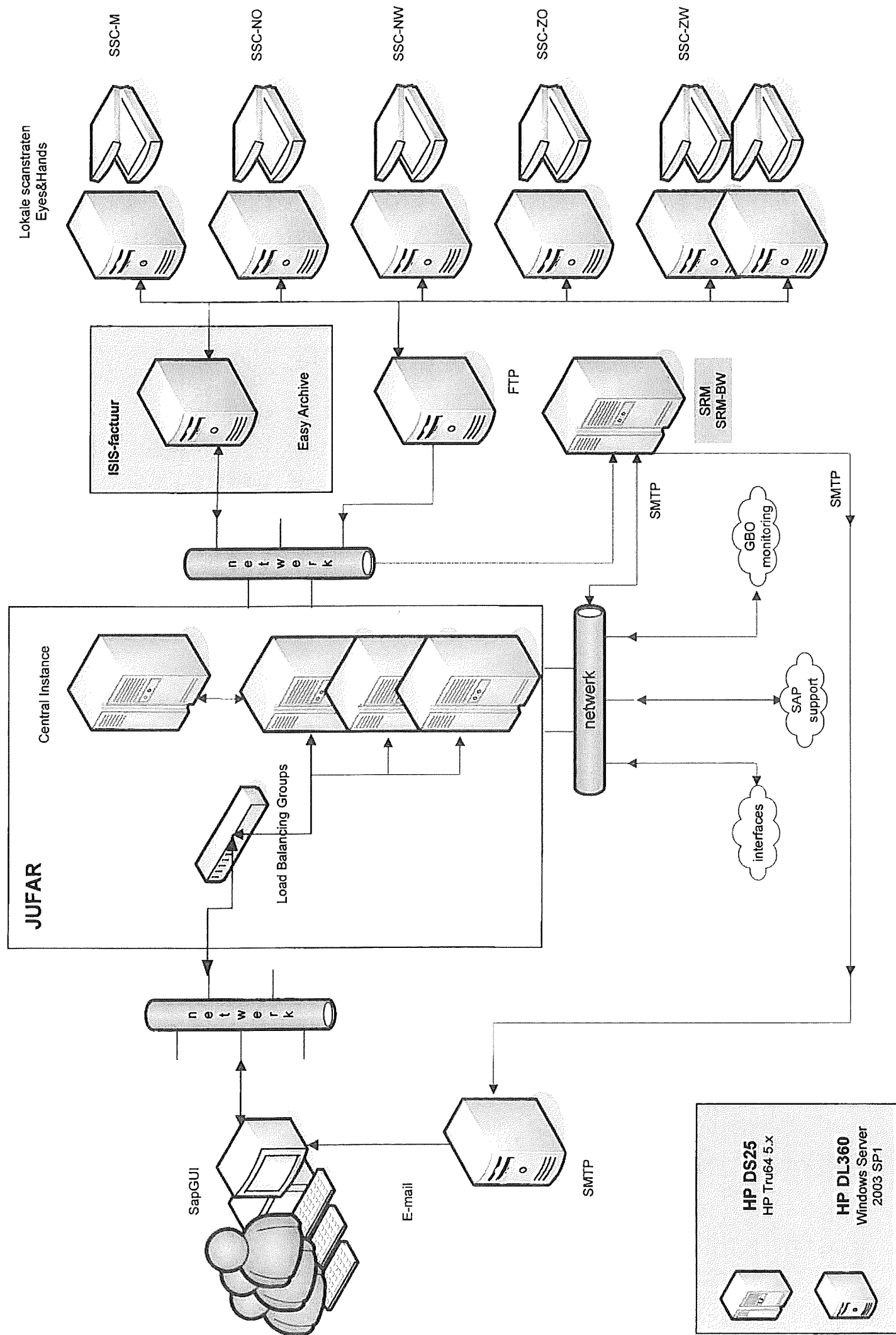
ISPA maakt gebruik van een Fox-pro database.
Gebruikers maken verbinding via Citrix

Omschrijving	I/O	Bron	Doel
Registreren gedetineerden als credituur	I	TULP	Jufar
Kaswinkelsbestand	I	Kassa systemen	Jufar
Saldo'sbestand gedetineerden	O	Jufar	Kassa systemen
Registratie uren medewerkers	I	SP-Expert	Jufar
Zakgeld en arbeidsluren gedetineerden	I	ISPA	Jufar
Zakgeld en arbeidsluren gedetineerden	I	MS-Excel	Jufar
Machine uren gedetineerden	I	MS-Excel	Jufar

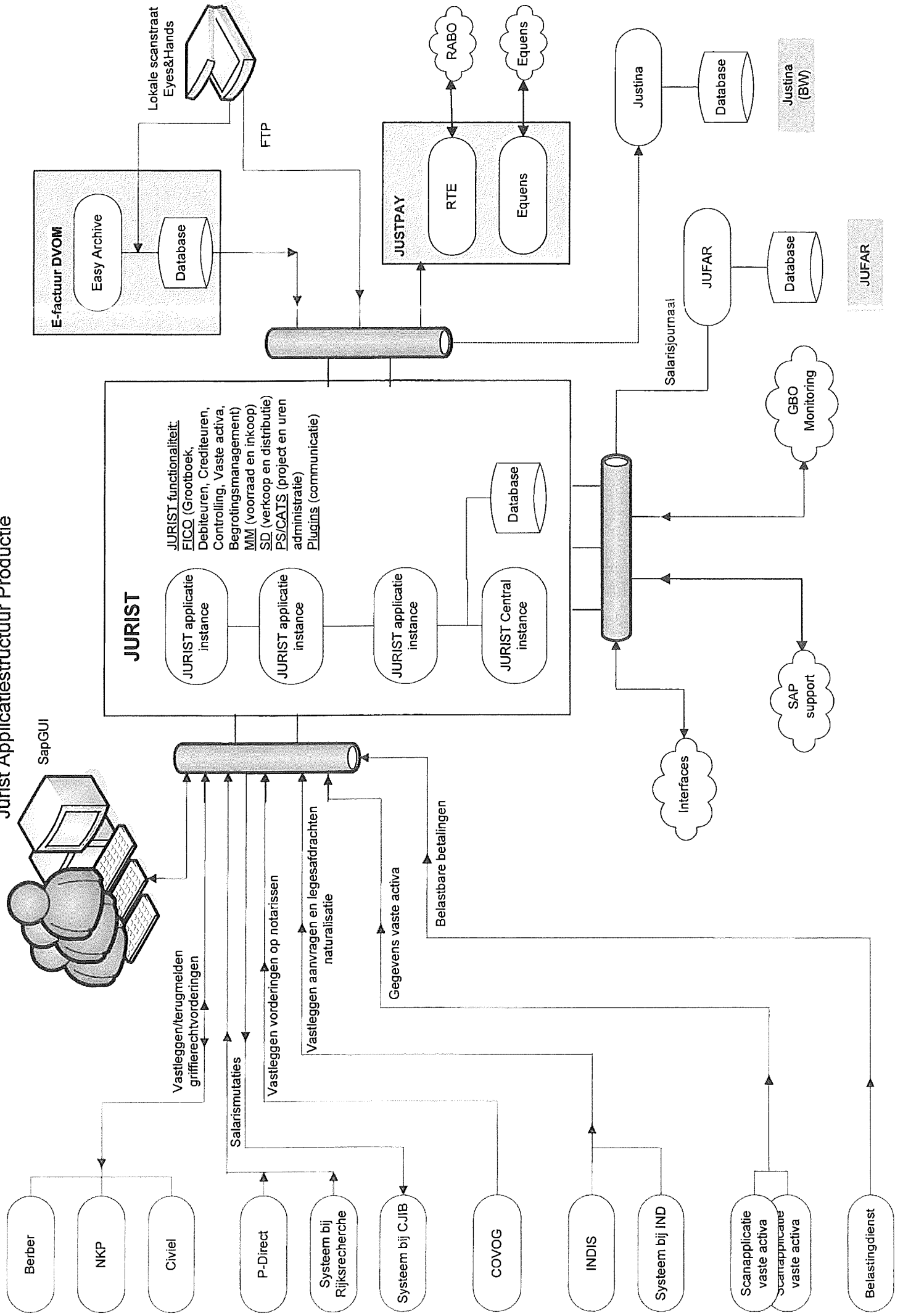
Jufar Applicatiestructuur Productie



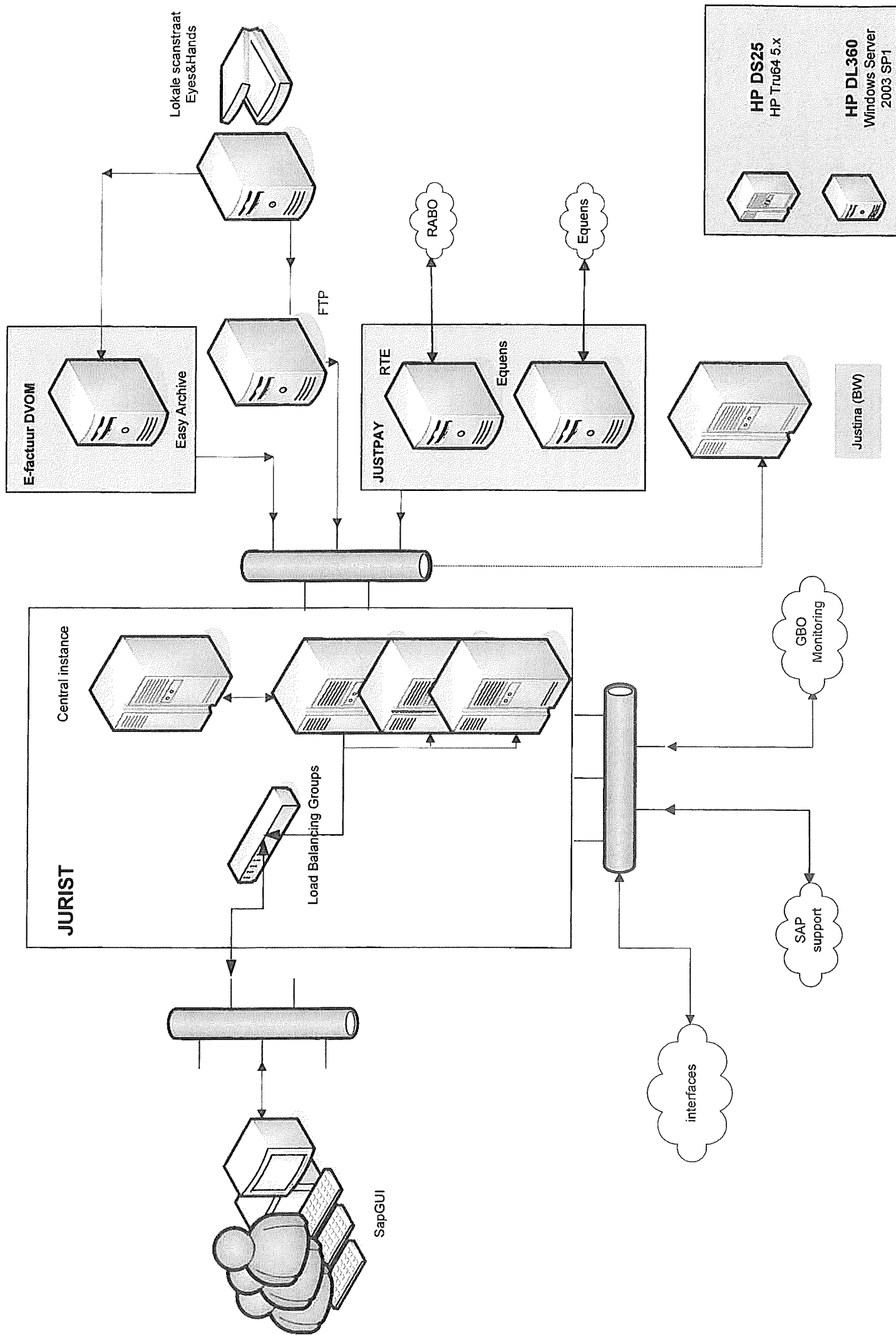
Jufar Infrastructuur Productie



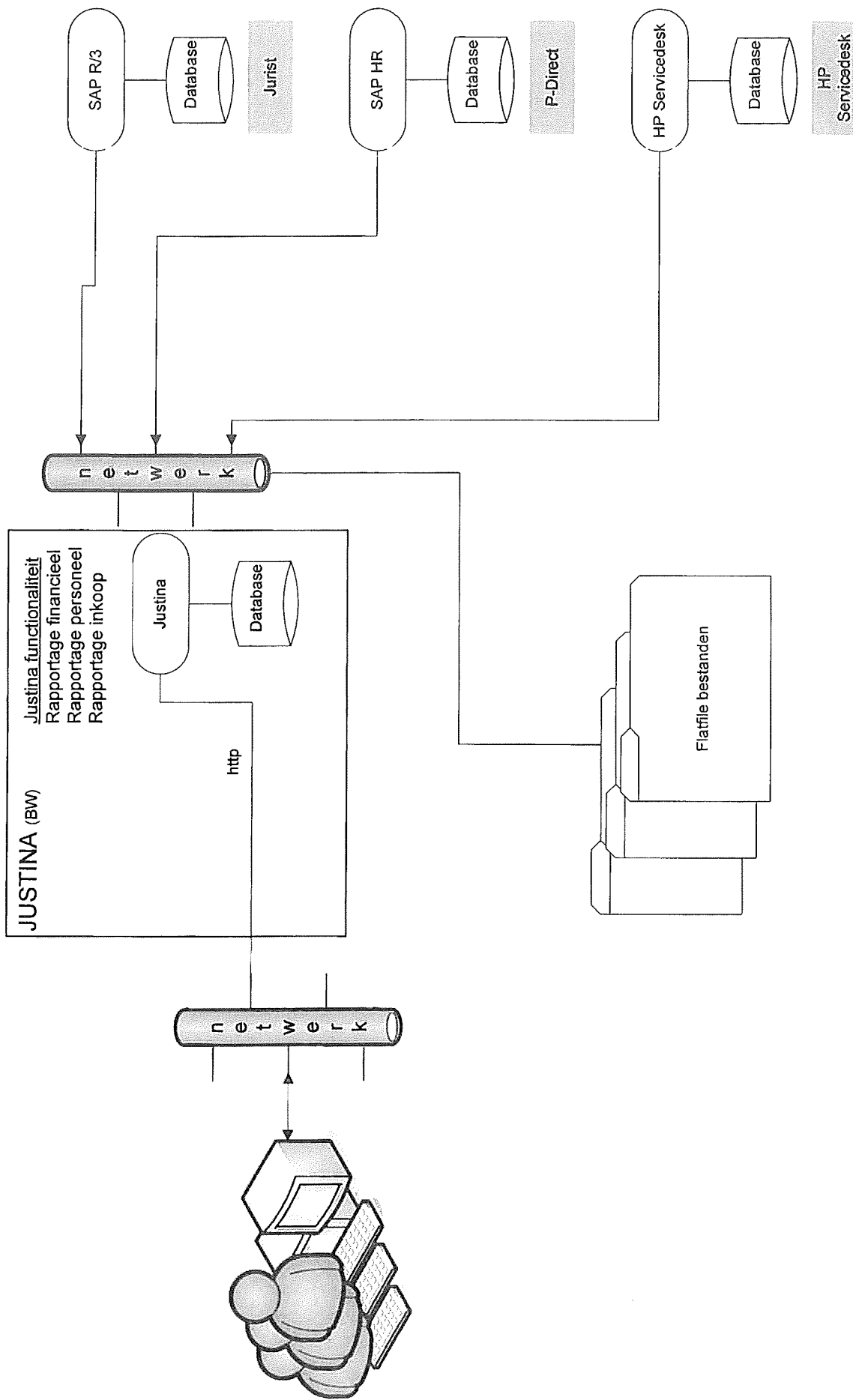
Jurist Applicatiestructuur Productie



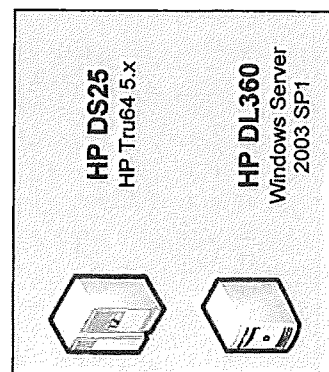
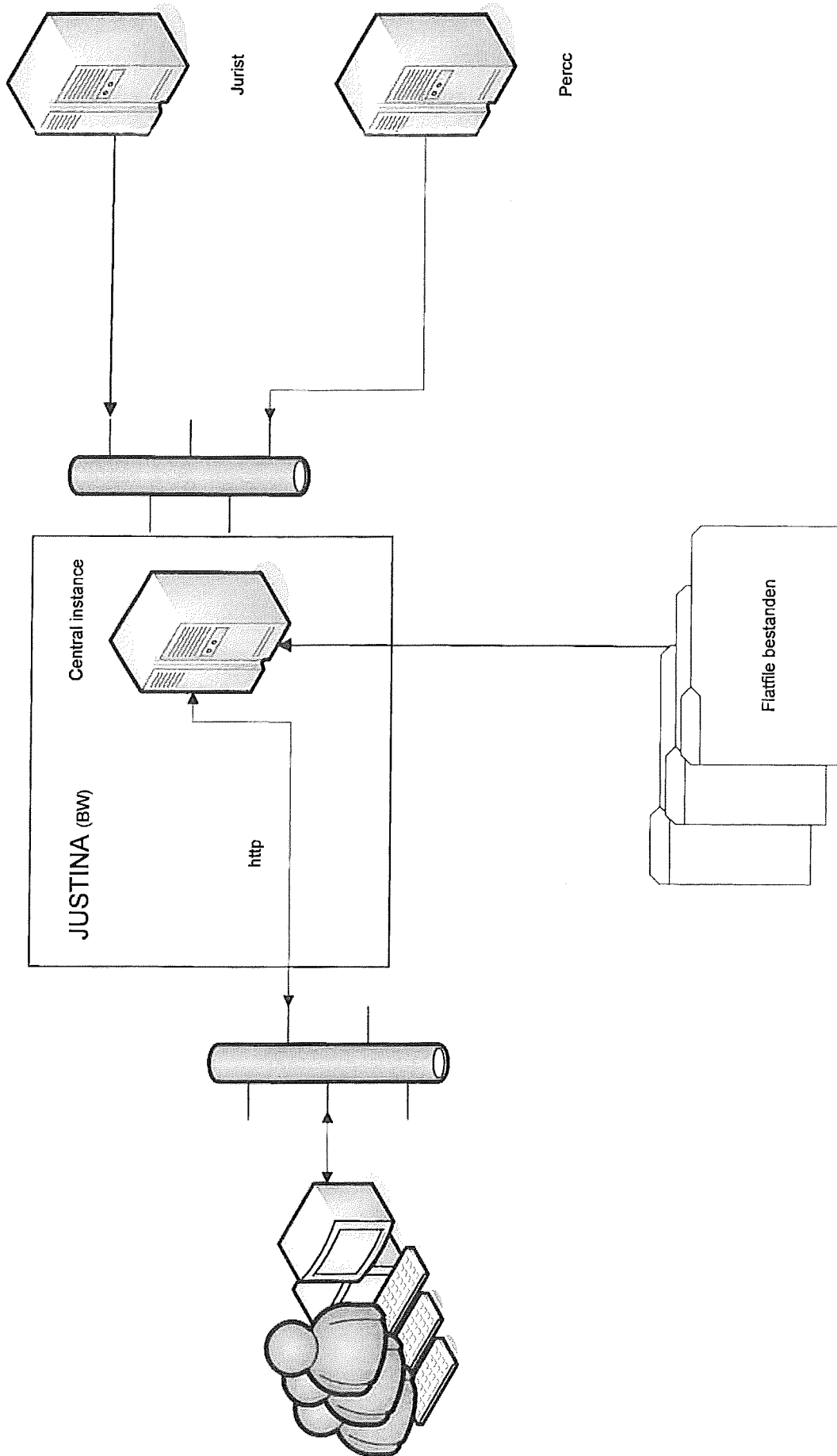
Jurist Infrastructuur Productie



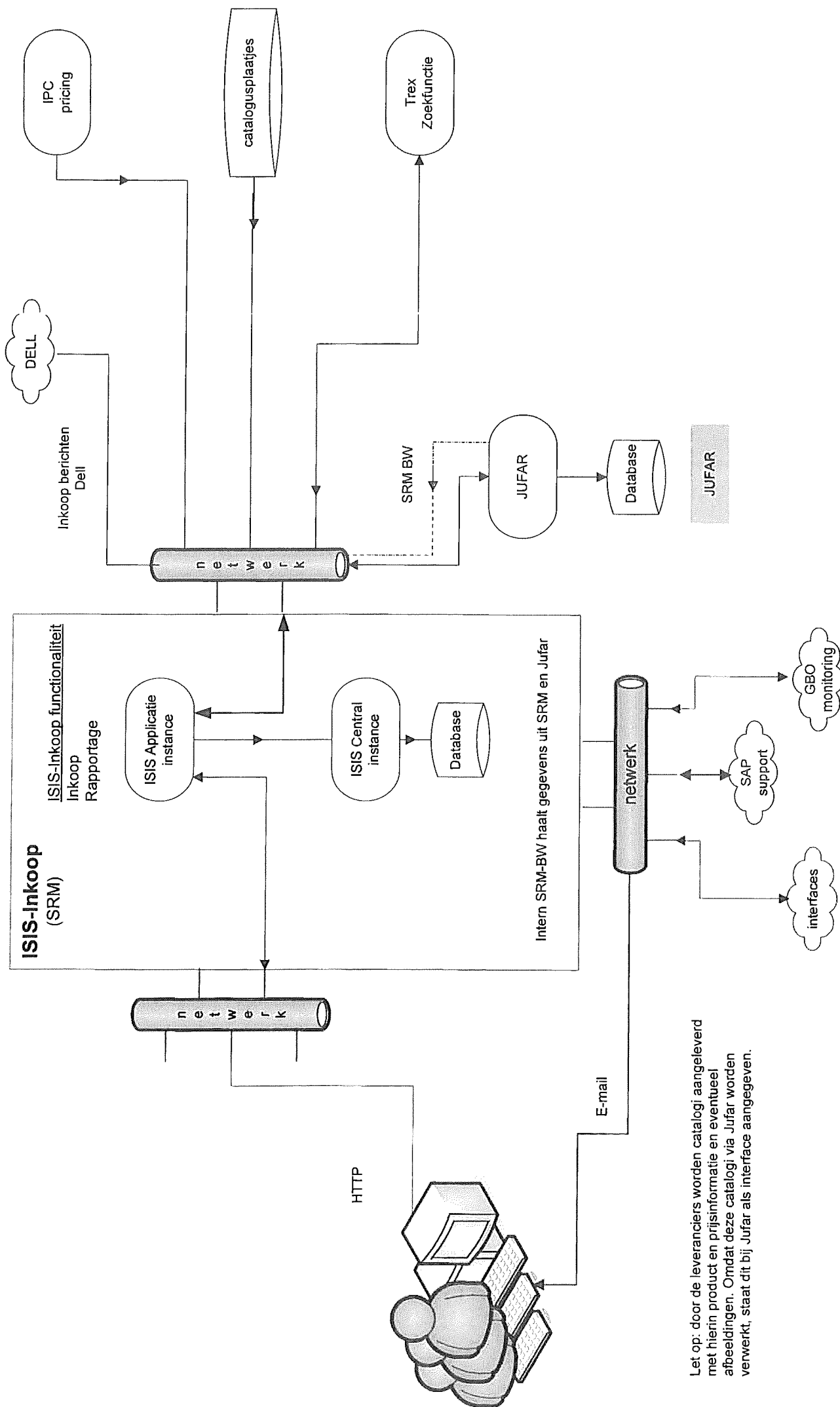
Justina Applicatiestructuur Productie



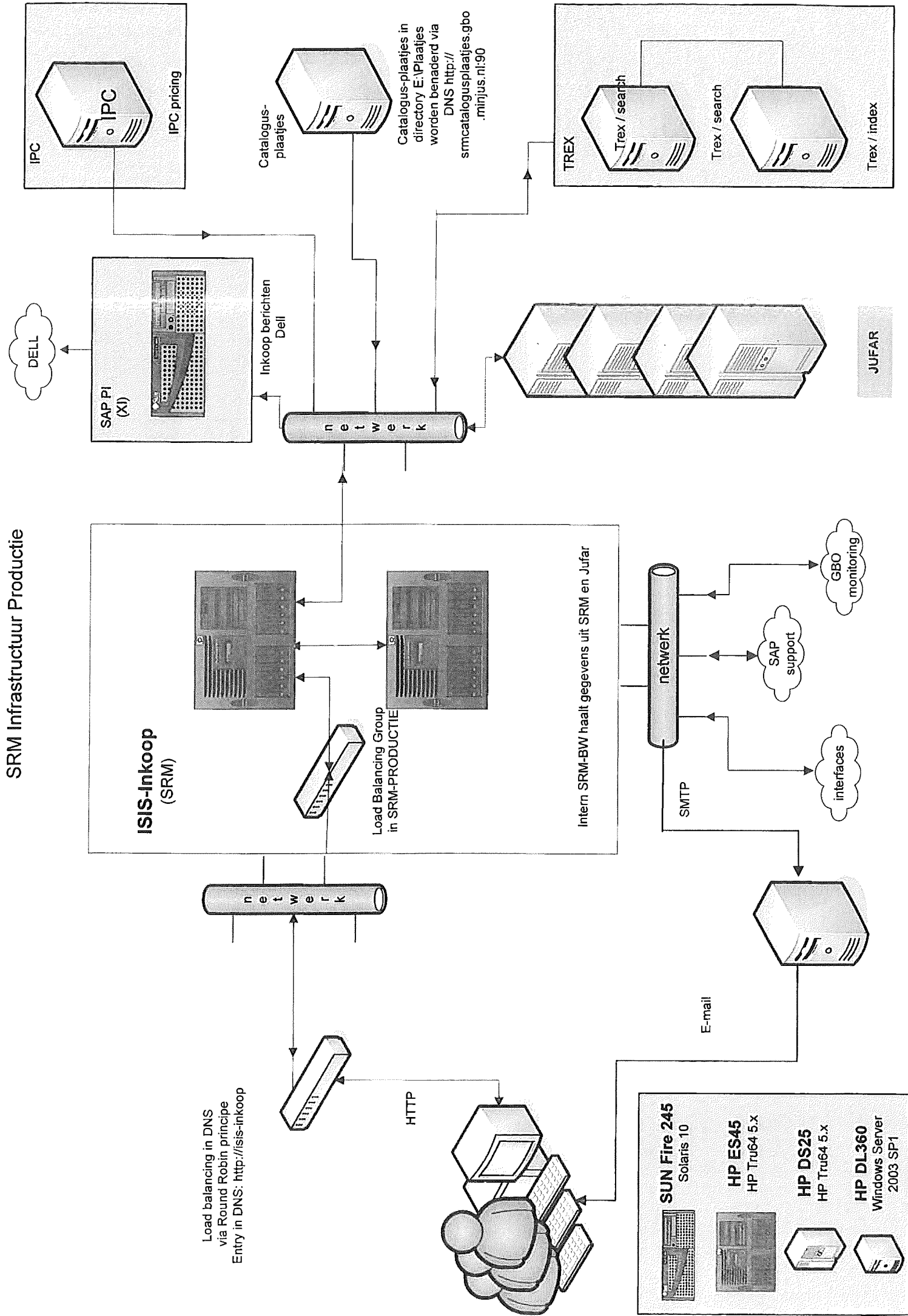
Justina Infrastructuur Productie



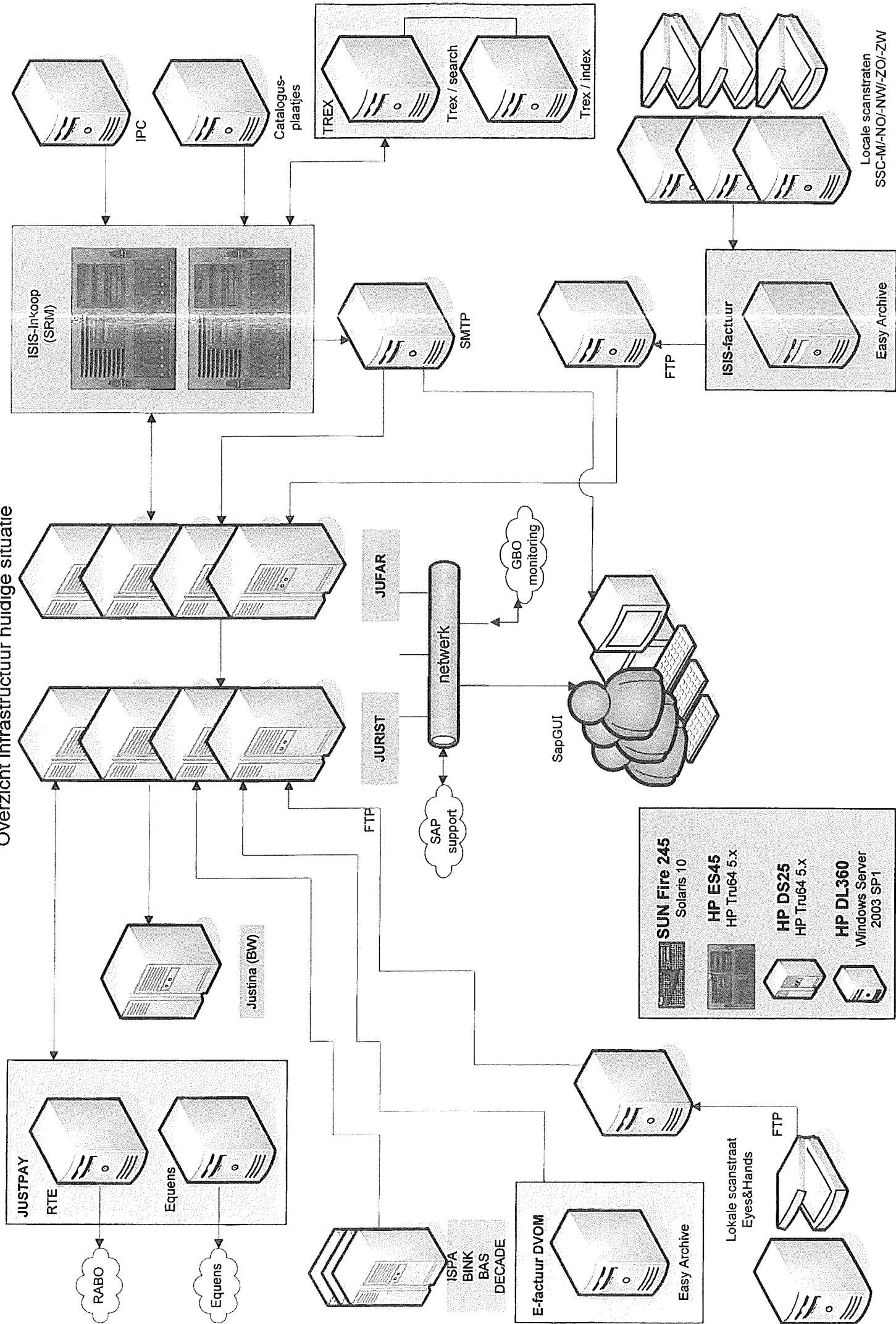
SRM Applicatiestructuur Productie



SRM Infrastructuur Productie



Overzicht infrastructuur huidige situatie



Dienst Justitiële Inrichtingen

Project WERKT!

**Functionaliteiten beschrijving
Informatie Systeem Penitentiaire Arbeid (ISPA)**

Inhoudsopgave

Inleiding.....		4.
Gebruikersscenario's.....		5.
2.1 Gebruikers.....		5.
02.2 Overzicht scenario's		5.
2.3 Bedrijf-bedrijfsnummer-prestatiesoort aanmaken	S2.0.01	7.
2.4 Locatie-capaciteit-divisie aanmaken	S2.1.02	8.
2.5 Werkzaal cap.personeel cap.gedetineerden aanmaken	S2.1.03	9.
2.6 Magazijn aanmaken	S2.1.04	10.
2.7 Machine aanmaken	S2.1.05	11.
2.8 Functie aanmaken	S2.1.06	12.
2.9 Werkrooster aanmaken	S2.1.07	13.
3.0 Perioden aanmaken	S2.1.08	14.
3.1 Bijzondere perioden aanmaken	S2.1.09	15.
3.2 Capaciteitsblokken aanmaken	S2.1.10	16.
3.3 Personeelslid aanmaken	S2.1.11	17.
3.4 Rechten toekennen	S2.1.12	18.
3.5 Reorganiseren systeem	S2.1.13	19.
3.6 Pakketinstellingen	S2.1.14	20.
3.7 Systeeminstellingen	S2.1.15	21.
3.8 Ordergegevens verwijderen	S2.1.16	22.
3.9 Uursoorten aanmaken	S2.1.17	23.
4.0 Prestatiesoort aanmaken	S2.1.18	24.
4.1 Eenheden aanmaken	S2.1.19	25.
4.2 Klachtensoorten aanmaken	S2.1.20	26.
4.3 Oplossingssoorten aanmaken	S2.1.21	27.
4.4 Prognose managementstool	S2.1.22	28.
4.5 Bedrijfssluiting aanmaken	S2.1.23	29.
4.6 Relatiegegevens aanmaken (debiteuren)	S2.2.04	30.
4.7 Artikel aanmaken	S2.2.05	31.
4.8 Voorcalculatie (Acquisiteur)	S1.1.01	32.
4.9 Voorcalculatie (Locale arbeid)	S4.1.01	33.
5.0 Voorcalculatie (Regio Bedrijfs-Bureau Arbeid)	S3.1.01	34.
5.1 Orderadministratie	S2.2.01	35.
5.2 Blokkeren – deblokken werkorder	S3.2.02	36.
5.3 Werkorder inplannen op de werkzaal	S3.2.03	37.
5.4 Beginsaldi personeel invoeren	S3.3.01	38.
5.5 Niet gestarte opdrachten (overzicht)	S7.3.01	39.
5.6 Opdrachten die de deadline gaan overschrijden (overzicht)	S7.3.02	40.
5.7 Overschreden deadline (overzicht)	S7.3.03	41.
5.8 Klachten registreren	S3.5.01	42.
5.9 Werkorders inplannen op werkplekken	S4.3.01	43.
6.0 Werkorder splitsen over de werkzalen	S4.3.03	44.
6.1 Werkpatroon en prestatiesoort toekennen	S4.4.01	45.
6.2 Wachttijdst gedetineerden	S4.4.02	46.
6.3 Gedetineerden plaatsen op de werkzaal	S4.4.03	47.
6.4 Tulpbestand inlezen/verversen	S4.4.04	48.
6.5 Afdelingsgegevens aanmaken	S4.4.05	nvt
6.6 Wijziging celnummers	S4.4.06	nvt
6.7 Verlof toekennen dat door het systeem geweigerd is	S4.7.02	nvt
6.8 Correcties op het verlofgoed	S4.7.03	nvt
6.9 Bijzonder verlof toekennen	S4.7.04	nvt.
7.0 Ziek melden personeel (registratie)	S4.7.05	nvt
7.1 werkproces aanmaken	S4.8.04	49.
7.2 Afgesloten werkorders opvragen	S6.1.01	...
7.3 Opbrengsten per werkzaal	S6.1.02	50.
7.4 Omzet per locatie	S6.1.03	51.
7.5 Creëren van een BIM-file	S6.2.01	52.
7.6 Controle van een BIM-file	S6.3.01	53.
7.7 Overzichten van BIM-files	S6.3.02	53.
7.8 Oplossingen registreren van klachten	S6.4.01	54.
7.9 Afmelden van klachten	S6.4.02	55.
8.0 Verlof overzichten	S6.5.01	nvt
8.1 Personele capaciteit	S6.5.02	nvt
8.2 Ziekteverzuim personeel	S6.5.03	nvt.
8.3 Openstaande werkopdrachten	S6.7.01	56.
8.4 Opdrachtstatus opdrachtgever	S6.7.02	57.
8.5 Ingeplande werkorders op werkzaal	S4.3.02	58.
8.6 Starten van de werkopdracht	S4.8.01	59.

8.7	Gereed melden van producten	S4.8.02	60.
8.8	Verwijderen van producten	S4.8.03	61.
8.9	Opdracht gereed melden	S4.8.04	62.
9.0	Verlonen op werkzaal	S4.5.01	63.
9.1	Registreren van machine uren	S4.6.01	64.
9.2	<i>Verlof aanvraag</i>	<i>S4.7.01</i>	<i>nvt.</i>
9.3	Palletsoorten ontvangst registratie	S5.1.01	65.
9.4	Gereed product boeken in het magazijn	S5.2.01	66.
9.5	Uitlevering gereed product	S5.3.01	67.
9.6	Retour ontvangen gereed product	S5.1.02	68.
9.7	Retour boeken gereed product naar de werkzaal	S5.4.01	69.
9.8	Overzicht soort ontvangen – uitgeleverde pallets	S5.1.03 S5.4.02	70.
9.9	Uitwisselen gereed product tussen de magazijnen	S5.1.04 S5.4.03	71.
10.0	Overzicht gereed product in het magazijn	S5.0.01	72.
10.1	Management informatie	S8.1.01	73.
10.2	Uren op werk – dummyorder	S8.4.01	74.
10.3	Nacalculatie op werkorder	S8.5.01	75.

3. Gegevensmodel ---- (nog nader uit te werken)
 Operationele eisen en ontwerpbeperkingen ----(nog nader uit te werken)
 Uitwerking gegevensmodel ---- (nog nader uit te werken)

NB. Aan het einde van de proeftuin zal de functionaliteit en de gebruiksvriendelijkheid nader bepaald worden.
 In dit model is de CRM module nog niet meegenomen (ontwerp/test stadium)

1. Inleiding

1.

Aanleiding

Landelijke Penitentiaire Arbeid bestaat uit verschillende arbeidsvormen, zoals vakarbeid, diversen arbeid tewerkstelling buiten de Inrichting, interne banen o.a. facilitair, keukenhulp, catering, tuin, terrein, en gebouwen onderhoud. Met deze vormen van arbeid wordt getracht de inrichtingskosten te verminderen. Landelijk worden verschillende ondersteunde systemen gebruikt om deze arbeidsvormen, faciliteiten en activiteiten te registreren, in de vorm van gedetineerden verlonen, calculeren, opbrengst - kostenberekening, werk – personeel - gedetineerdenplanning, logistieke transacties en management informatie. Mede hierdoor worden de jaarcijfers per inrichten verschillend geïnterpreteerd. Verschillende ondersteunde systemen maakt ook, dat op landelijk niveau niet meetbaar is wat de werkelijke resultaten zijn in alle facetten. Verschillende ondersteunde systemen buiten het Landelijke SAP om, zijn ontwikkeld om sturing en greep te krijgen op de arbeidsbewegingen. Om op landelijk niveau bedrijfsvoering uniform uit te oefenen is standaardisatie van de verschillende ondersteunde systemen wenselijk.

Doel

Dit document beschrijft de eisen die het Landelijke Bureau Bedrijfsvoering stelt aan het te realiseren Informatie Systeem Penitentiaire Arbeid. (ISPA)

Doelgroep

Dit document is bestemd voor leveranciers die een voorstel willen doen om het in dit document gespecificeerde systeem te realiseren.

Leeswijzer

Afkorting:

Gebruikersgroepen:

LS	=	Landelijke Sales
RS	=	Regio Sales
RM	=	Regiomanager
RBBA	=	Regio bedrijfsbureau Arbeid
LA	=	Locale Arbeid
LL	=	Locale Logistiek
CAA	=	Centrale Arbeids-Administratie
LA	=	Locatie Interne Afdelingen
RC	=	SCC-FEZ Rekening Courant

2. Gebruikersscenario's

2.

2.1 Gebruikers

Het systeem kent de volgende gebruikersgroepen:

- Sales – **LS** (landelijke Sales, Hoofd commercie)
- Regio Sales – **RS** (Acquisiteurs)
- Regiomanager - **RM**
- Regio Bedrijfsbureau Arbeid – **RBBA** (Hoofd Bedrijfsbureau, Bedrijfsbureau medewerkers)
- Locale Arbeid – **LA** (Locatiehoofd, Productiecoördinator, Medewerker arbeid)
- Locale Logistiek – **LL** (Hoofd logistiek, Logistieke medewerkers)
- SSC-Centrale Arbeidsadministratie **CAA** (hoofd CAA, Gebruikers CAA, Kerngebruikers CAA/ISPA)
- Locale Interne afdeling - **IA** (Afdelingshoofd, PIW-ers)
- SCC-FEZ Rekening Courant (BIM-file verwerking)

2.2 Overzicht Scenario's

Gebruikersgroepen	Scenario	Frequentie
CAA (kernegebr.)	Bedrijf-bedrijfsnummer-prestatiesoort aanmaken	S2.0.01 Eenmalig
CAA (kernegebr.)	Locatie-capaciteit-divisie aanmaken	S2.1.02 Eenmalig
CAA (kernegebr.)	Werkzaal cap.personeel cap.gedetineerden aanmaken	S2.1.03 Eenmalig
CAA (kernegebr.)	Magazijn aanmaken	S2.1.04 Eenmalig
CAA (kernegebr.)	Machine aanmaken	S2.1.05 Jaarlijks
CAA (kernegebr.)	Functie aanmaken	S2.1.06 Jaarlijks
CAA (kernegebr.)	Werkrooster aanmaken	S2.1.07 Jaarlijks
CAA (kernegebr.)	Perioden aanmaken	S2.1.08 Jaarlijks
CAA (kernegebr.)	Bijzondere perioden aanmaken	S2.1.09 Jaarlijks
CAA (kernegebr.)	Capaciteitsblokken aanmaken	S2.1.10 Jaarlijks
CAA (kernegebr.)	Personeelslid aanmaken	S2.1.11 Maandelijks
CAA (kernegebr.)	Rechten toekennen	S2.1.12 Maandelijks
CAA (kernegebr.)	Reorganiseren systeem	S2.1.13 Wekelijks
CAA (kernegebr.)	Pakketinstellingen	S2.1.14 Eenmalig
CAA (kernegebr.)	Systeeminstellingen	S2.1.15 Eenmalig
CAA (kernegebr.)	Ordergegevens verwijderen	S2.1.16 Eenmalig
CAA (kernegebr.)	Uursoorten aanmaken	S2.1.17 Jaarlijks
CAA (kernegebr.)	Prestatiesoort aanmaken	S2.1.18 Jaarlijks
CAA (kernegebr.)	Eenheden aanmaken	S2.1.19 Jaarlijks
CAA (kernegebr.)	Klachtensoorten aanmaken	S2.1.20 Eenmalig
CAA (kernegebr.)	Oplossingssoorten aanmaken	S2.1.21 Eenmalig
CAA (kernegebr.)	Prognose managementstool	S2.1.22 Maandelijks
CAA (kernegebr.)	Bedrijfssluiting aanmaken	S2.1.23 Jaarlijks
CAA	Relatiegegevens aanmaken (debiteuren)	S2.2.04 Dagelijks
CAA	Artikel aanmaken	S2.2.05 Dagelijks
RS	Voorcalculatie (acquisiteur)	S1.1.01 Dagelijks
LA (loc.verandw.)	Voorcalculatie (Locale arbeid)	S4.1.01 Dagelijks
RBB	Voorcalculatie (Regio bureau)	S3.1.01 Dagelijks
CAA	Orderadministratie	S2.2.01 Dagelijks
RBB	Blokkeren – deblokkeren werkorder	S3.2.02 Wekelijks
RBB	Werkorder inplannen op de werkzaal	S3.2.03 Dagelijks
CAA	Beginsaldi personeel invoeren	S3.3.01 Jaarlijks
RBBA/LA/CAA	Niet gestarte opdrachten (overzicht)	S7.3.01 Dagelijks
RBBA/LA/CAA	Opdrachten die de deadline gaan overschrijden (overzicht)	S7.3.02 Dagelijks
RBBA/LA/CAA	Overschreden deadline (overzicht)	S7.3.03 Dagelijks
RBBA/LA	Klachten registreren	S3.5.01 Dagelijks
LA (loc.verandw.)	Machines inplannen	S4.2.01 Dagelijks
LA (loc.verandw.)	Werkorders inplannen op werkplekken	S4.3.01 Dagelijks
LA (loc.verandw.)	Werkorder splitsen over de werkzaal	S4.3.03 Wekelijks
LA (loc.verandw.)	Werkpatroon en prestatiesoort toekennen	S4.4.01 Dagelijks
LA (loc.verandw.)	Wachttijd gedetineerden	S4.4.02 Dagelijks
LA (loc.verandw.)	Gedetineerden plaatsen op de werkzaal	S4.4.03 Dagelijks
LA (loc.verandw.)	Tulpbestand inlezen/verversen	S4.4.04 Dagelijks
LA (loc.verandw.)	Afdelingsgegevens aanmaken (nvt)	S4.4.05 nvt
LA (loc.verandw.)	Wijziging celnummers (nvt)	S4.4.06 nvt
LA (loc.verandw.)	Verlof toekennen dat door het systeem geweigerd is	S4.7.02 nvt
LA (loc.verandw.)	Correcties op het verlofgoed	S4.7.03 nvt
LA (loc.verandw.)	Bijzonder verlof toekennen	S4.7.04 nvt
LA (loc.verandw.)	Ziek melden personeel (registratie)	S4.7.05 nvt
LA (loc.verandw.)	Werkproces aanmaken	S4.8.04 Dagelijks
LA /RBBA/CAA	Afgesloten werkorders opvragen	S6.1.01 Wekelijks

LA/RBBA/CAA	Opbrengsten per werkzaal	S6.1.02	Dagelijks
LA /RBBA/CAA	Omzet per locatie	S6.1.03	Dagelijks
LA (loc.verandw.)	Creëren van een BIM-file	S6.2.01	Dagelijks
LA (loc.verandw.)	Controle van een BIM-file	S6.3.01	Dagelijks
LA (loc.verandw.)	Overzichten van BIM-files	S6.3.02	Dagelijks
LA (loc.verandw.)	oplossingen registreren van klachten	S6.4.01	Wekelijks
LA/RBB/CAA	Afmelden van klachten	S6.4.02	Wekelijks
LA (loc.verandw.)	<i>Verlof overzichten</i>	S6.5.01	nvt
LA (loc.verandw.)	<i>Personele capaciteit</i>	S6.5.02	nvt
LA (loc.verandw.)	<i>Ziekteverzuim personeel</i>	S6.5.03	nvt
LA /RBB/CAA	Openstaande werkopdrachten	S6.7.01	Dagelijks
LA (loc.verandw.)	Opdrachtstatus opdrachtgever	S6.7.02	Dagelijks
LA/RBB/CAA	Ingeplande werkorders op werkzaal	S4.3.02	Dagelijks
LA	Starten van de werkopdracht	S4.8.01	Dagelijks
LA	Gereed melden van producten	S4.8.02	Dagelijks
LA	Verwijderen van gereed product (foutief geboekt)	S4.8.03	Maandelijks
LA	Opdracht gereed melden	S4.8.04	Dagelijks
LA	Verlonen op werkzaal	S4.5.01	Dagelijks
LA	Registreren van machine uren	S4.6.01	Dagelijks
LA	<i>Verlof aanvraag</i>	S4.7.01	nvt
LL	Palletsoorten ontvangst registratie	S5.1.01	Dagelijks
LL	Gereed product boeken in het magazijn	S5.2.01	Dagelijks
LL	Uitlevering gereed product	S5.3.01	Dagelijks
LL	Retour ontvangen gereed product	S5.1.02	Maandelijks
LL	Retour boeken gereed product naar de werkzaal	S5.4.01	Maandelijks
LL	Overzicht soort ontvangen – uitgeleverde pallets	S5.1.03 S5.4.02	Dagelijks
LL	Uitwisselen gereed product tussen de magazijnen	S5.1.04 S5.4.03	Maandelijks
LL/RBBA/LA/CAA	overzicht gereed product in het magazijn	S5.0.01	Dagelijks
CAA	Management informatie	S8.1.01	Bij opvragen
CAA	Uren op werk - dummyorder	S8.4.01	Bij opvragen
CAA	Nacalculatie op werkorder	S8.5.01	Bij opvragen

NB.

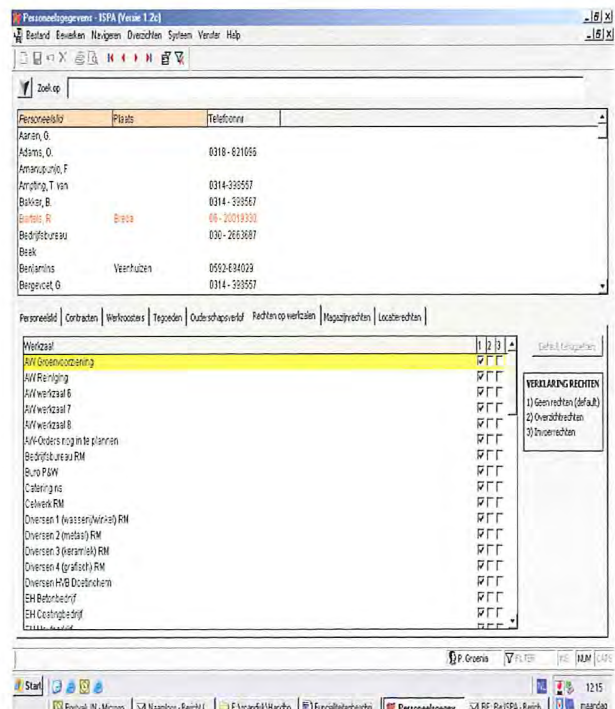
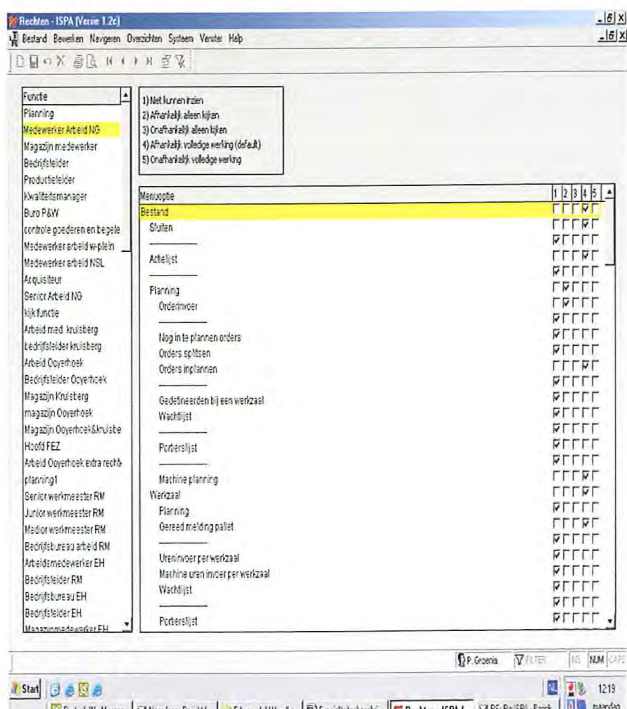
Ieder scenario is op functieniveau af te geschermen door het instellen van de rechten, in de vorm van:

1. Niet kunnen inzien
2. Afhankelijk alleen kijken
3. Onafhankelijk alleen kijken
4. Afhankelijk volledige werking
5. Onafhankelijk volledige werking

In ISPA zijn meerdere locaties, werkzalen en magazijnen toegankelijk.

Iedere locatie, werkzaal en magazijn is op gebruikersniveau/op naam af te schermeren met rechten in de vorm van:

1. Geen rechten
2. Overzichtsrechten
3. Invoerrechten



Scenario	2.3 Bedrijf – Bedrijfsnummer – Prestatiesoort S2.0.01
Toelichting scenario	Dit scenario betreft het invoeren van de stamgegevens per bedrijf.
Relatie met scenario	S2.1.17 - S2.1.18 en alle ordergerelateerde scenario's
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens

Scenario stap	Invoervereisten	Variabele	Link
1	Het bedrijfsnummer	Bedrijfsnummer	
2	De naam van het bedrijf	Naam PI	
3	Selecteert - koppeling prestatiesoort		aangemaakt in S2.1.18

Frequentie handeling	Eenmalig (Nb. eenmalig, tenzij de inrichting anders wordt ingedeeld wat betreft de alle boven genoemde items of vaste gegevens.)
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	2.4 Locatie – Capaciteit Personeel – Divisie	S2.1.02
Toelichting scenario	Aanmaken van een locatie. De maximale personeelscapaciteit en de soorten divisies op deze locatie.	
Relatie met scenario	S2.1.03 - S2.1.04 - S2.1.11 - S2.1.22 - S.2.2.04 - S.1.1.01 - S.2.2.01 – S3.2.02 – S3.5.01 – S6.1.03 – S6.2.01 – S6.3.02 – S6.5.02 – S8.1.01	
Gebruikergroep	CAA (kernegebruiker)	
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.	

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van de locatie		
2	Het nummer van de kostenplaats		
3	Het inrichtingsnummer	nummer van de locatie	
4	Selecteer - koppeling bedrijfsnummer		aangemaakt in S2.0.01
5	De naam van het bedrijfsbureau		
6	Het telnr, faxnr en emailadres		
7	De directory in waar de BIM-file geplaatst wordt voor deze betreffende locatie. (de BIM-file is een transportfile voor het verlonen van gedetineerden in SAP)		
8	De maximale capaciteit personeel		
9	De namen van de divisies	(bv. hout, metaal, diverse enz. enz.)	
10	Het standaarduurtarief	(divisie/werkplektarief)	
11	De overhead kosten		

Frequentie handeling	Eenmalig (Nb. eenmalig, tenzij de inrichting anders wordt ingedeeld wat betreft de alle boven genoemde items of vaste gegevens.)
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	2.5 Werkzaal – Capaciteit Personeel –Capaciteit Gedetineerden S2.1.03
Toelichting scenario	Aanmaken van een werkzaal en koppelen aan de locatie. De maximale capaciteit van personeel en gedetineerden vastleggen voor deze werkzaal.
Relatie met scenario	S.2.1.05 – S1.2.06 – S2.1.11 – S2.1.12 – S3.2.03 – S4.3.01 - S4.3.03 – S4.4.02 – S4.4.03 – S6.1.01 – S6.1.02 – S4.3.02 – S4.8.01 – S4.8.02 – S4.5.01 - S.2.1.04
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van de werkzaal		
2	Selecteert – koppeling locatie		aangemaakt in S2.1.02
3	Het aantal productieve uren per dagdeel		
4	Vinkt aan, controle vier uur per dagdeel	maximaal verlonen p/ dagdeel	
5	De naam van het bedrijfsbureau		
6	Het nummer van de kostenplaats		
7	Het aantal maximale werkplekken		
9	Het aantal dagen in dat teruggemuteerd mag worden		
10	De minimale capaciteit aantal personeel		
	Het maximale aantal oproepbaar gedetineerden		

Frequentie handeling	Eenmalig (Nb. eenmalig, tenzij de inrichting anders wordt ingedeeld wat betreft de alle boven genoemde items of vaste gegevens.)
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	2.6 Magazijn aanmaken S2.1.04
Toelichting scenario	Het aanmaken van een magazijn, en deze koppelen aan de locatie en werkzalen
Relatie met scenario	S5.1.01 – S5.2.01 – S5.3.01 – S5.1.02 – S5.4.01 – S5.1.03 – S5.1.03 – S5.4.02 – S5.1.04 S5.4.03 – S5.0.01
Gebruikergroep	CAA (kerngebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van het magazijn		
2	Selecteert - koppeling locatie		aangemaakt in S2.1.02
3	Selecteert - koppeling werkzalen		aangemaakt in S2.1.03

Frequentie handeling	Eenmalig (Nb. eenmalig, tenzij de inrichting anders wordt ingedeeld wat betreft de alle boven genoemde items of vaste gegevens.)
Zichtbaar voor	CAA (kerngebruiker)
Beheerbaar door	CAA (kerngebruiker)

Scenario	2.7 Machine aanmaken S2.1.05
Toelichting scenario	Het aanmaken van een machine en koppelen aan de werkzaal. Aan deze machine een standaard uurtarief koppelen.
Relatie met scenario	S2.1.03 - S4.2.01 – S4.6.01 – S8.1.01
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van de machine		
2	Het serienummer		
3	Selecteert - koppeling werkzaal		aangemaakt in S2.1.03
4	De datum van ingebruikstelling		
5	De datum van buitengebruik		
6	Het uurtarief		
7	De datum vanaf geldigheid uurtarief		
8	De datum tot de geldigheid uurtarief		

Frequentie handeling	jaarlijks
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	2.8 Functie aanmaken S2.1.06
Toelichting scenario	Het aanmaken van de functies, dienen er voor om functionaliteiten beschikbaar te stellen en of af te kunnen schermen
Relatie met scenario	S2.1.11 – S2.1.12
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van de functie	aanmaken een lijst van functies - Rollen	

Frequentie handeling	jaarlijks (Nb. jaarlijks, tenzij de inrichting anders wordt ingedeeld wat betreft de alle boven genoemde items of vaste gegevens.)
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	2.9 Werkrooster aanmaken S2.1.07
Toelichting scenario	Meerdere werkrooster aanmaken die in een later scenario gekoppeld worden.
Relatie met scenario	S2.1.11 – S6.5.02 – S4.7.01
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van een werkrooster		
2	Selecteert – koppeling dag		aangemaakt in S2.1.10
3	De tijd vanaf		
4	De tijd tot		

Frequentie handeling	jaarlijks
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	3.0 Perioden aanmaken S2.1.08
Toelichting scenario	Het aanmaken van perioden waar het systeem mee kan rekenen. Iedere periode vertaalt de lengte van een maand.
Relatie met scenario	S2.1.23 – S2.1.22 – S2.1.23 – S3.2.03 - S8.1.01 – S8.5.01 - S3.2.03 – S7.3.01 – S7.3.02 S7.3.03 – S4.2.01 – S4.3.01 – S4.7.02 – S4.7.04 – S4.7.05 - S6.1.02 (En alle scenario's die een berekening doen met de lengte van de perioden)
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	Het periode nummer		
2	De datum vanaf		
3	De datum tot		

Frequentie handeling	jaarlijks
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)

Scenario	3.1 Bijzondere Perioden aanmaken S2.1.09
Toelichting scenario	Bijzondere perioden zijn die dagen waarop de arbeid of een deel van de arbeid gesloten is. Deze periode kan vooraf worden vastgelegd. Het systeem zal rekening houden met alles wat planbaar is. Deze blokken worden afgeschermd als zijnde niet aanwezig.
Relatie met scenario	Gegevens voor verder gebruik: (alle scenario's waar ISPA rekent met dagen, zoals personeelsplanning, werk-machineplanning, gedetineerdenplanning.)
Gebruikergroep	CAA (kernegebruiker)
Triggers	De software inrichten met vaste bedrijfsgegevens om de onderliggende componenten te kunnen koppelen. Deze vaste gegevens worden gebruikt om het systeem te kunnen voeden met stuurgegevens.

Scenario stap	Invoervereisten	Variabele	Link
1	De naam van de periode		
2	De datum vanaf		
3	De datum tot		

Frequentie handeling	jaarlijks
Zichtbaar voor	CAA (kernegebruiker)
Beheerbaar door	CAA (kernegebruiker)