Dienst ICT Uitvoering
Ministerie van Economische Zaken

Project Startarchitectuur (PSA) - Duurzame Tijdverantwoording (DTV)

Versie 1.0

Datum 14 juli 2014
Status Definitief

Colofon

Projectnaam	NVWA - Project Duurzame Tijdverantwoording
Locatie	T:\DICTU\dictu\Projecten\04 Divisie Inspecties\106959 - NVWA JB-Duurzame tijdverantwoording\03 PSA - Ontwerp - Review\20140714 PSA DTV 10.doc
Contactpersoon	Eric Penseel Senior ICT Architect T 070 378 5542 M 06 11591602 F 070 378 6186 e.j.s.penseel@dictu.nl DICTU | Divisie Inspecties - Team Inspecties Projecten Juliana van Stolberglaan 148 Postbus 20401 | 2500 EK Den Haag
Auteurs	Eric Penseel

Inhoud

Colofon—2
Documentbeheer—5
Managementsamenvatting—6

1 Inleiding—7
1.1 Identificatie—7
1.2 Leeswijzer—7
1.3 Doel van dit document—7
1.4 Referenties—8
1.5 Afkortingen en begrippen—8

2 Kaders—9
2.1 Ambitie en doelen DTV—9
2.2 Gewenste situatie—9
2.3 Architectuurkader—10
2.4 Architectuurkeuzen—10

3 Businessarchitectuur (BA)—11
3.1 Organisatie—11
3.1.1 Toezicht, handhaving en vervolging/opsporing—12
3.1.2 Betrokken partijen bij DTV—12
3.1.3 Eisen—12
3.2 Diensten en producten—12
3.2.1 Diensten—12
3.2.2 Producten—13
3.2.3 Eisen—14
3.3 Processen—14
3.3.1 Processen op hoofdlijnen—14
3.3.2 Te ondersteunen processtappen—15
3.3.3 Proces Tijdregistratie—15
3.3.4 Proces tijdverwerking—16
3.3.5 Eisen—17

4 Informatiearchitectuur (IA)—18
4.1 Gebruikers en applicaties—18
4.1.1 Gebruikers—18
4.1.2 Applicaties—18
4.1.3 Flexibiliteit en wendbaarheid—21
4.1.4 Eisen—21
4.2 Berichten en gegevens—22
4.2.1 Berichten—22
4.2.2 Dataservices—22
4.2.3 Overige koppelvlakken—23
4.2.4 Dynamisch berichtinhoud—23
4.2.5 Berichtdefinitie—23
4.2.6 Eisen—23
4.2.7 Gegevens—24
4.3 Informatie-uitwisseling—24
4.3.1 Financiële administratie—24
4.3.2 Personeelsadministratie—24

4.3.3 SPIN VTE, CLE en ORG (Productieproces)—24
4.3.4 Salarisadministratie—25
4.3.5 Component Tijdregistratie naar component Tijdverwerking—25
4.3.6 Versies—25
4.3.7 Eisen—25

5 Technische architectuur (TA)—26
5.1 Technische componenten—26
5.1.1 Tijdregistratie in SPIN-Tijdschrijven—26
5.1.2 Eisen technische componenten—27
5.1.3 Schaalbaarheid en robuustheid—30
5.1.4 Eisen (applicatie)componenten—31
5.1.5 Eisen webservices—31
5.1.6 Eisen database—32
5.2 Gegevensopslag—32
5.2.1 Eisen datastores—32
5.2.2 Eisen exporteren t.b.v rapporteren—32
5.2.3 Eisen onderhoudbaarheid—33
5.2.4 Eisen Integriteit—33
5.2.5 Eisen continuïteit—33
5.2.6 Eisen back-up—33
5.3 Netwerk—34

6 Beveiliging en privacy—35
6.1 Beveiligingsclassificatie—35
6.1.1 Eisen—36
6.2 Identity & Access Management (IAM)—37
6.2.1 Eisen identificatie en authenticatie—37
6.2.2 Eisen autorisatie—37
6.3 Toegang—37
6.3.1 Eisen—37
6.4 Monitoring, auditing en alerting—38
6.4.1 Eisen—38
6.5 Compartimentering—38
6.5.1 Eisen compartimentering—39
6.5.2 Eisen patchen en updates—40

7 Beheer—41
7.1 Formalisering afspraken—41
7.1.1 Eisen—41
7.2 Zelfbediening—41
7.2.1 Eisen—42
7.3 Lifecycle management—42
7.3.1 Eisen—42
7.4 Zelfbeheer en samenwerking in de beheerketen—42
7.4.1 Eisen—42
7.5 Service levels—42
7.6 Rapportages—43
7.6.1 Eisen—43
7.6.2 Eisen testen en accepteren—43

Documentbeheer

Versiehistorie

Versie	Datum	Status	Auteur
0.1	4-jun-14	Concept	Eric Penseel
0.2	11-jun-14	Concept	Eric Penseel – H-6 en 7 toegevoegd
1.0	14-jul-14	Definitief	Eric Penseel – aangepast na keuze voor alternatief 1

Distributie- en reviewhistorie

Naam	Functie/ afdeling	Versie							
Rob Brand	DICTU PM	0.1	0.2	1.0					
Reza Sharafat	NVWA PM	0.1	0.2	1.0					
Bart Coumans	NVWA			1.0					
Pieter Hubregtse	NVWA	0.1	0.2	1.0					
Sylvia Bergsma	NVWA			1.0					
Jan Boswijk	NVWA			1.0					
Ordina		0.1	0.2	1.0					

Versie goedkeuring

Versie	Datum	Naam	Functie/afdeling
0.1	4-jun-14		
0.2	11-jun-14		
1.0	14-jul-14		

Managementsamenvatting

Op dit moment maakt NVWA gebruik van meerdere voorzieningen voor het verantwoorden van tijd, zoals de applicaties FATIJDEC en SPIN. FATIJDEC ondersteunt naast tijdverantwoording ook de verwerking van declaraties en het factureren van bijv. retribueerbaar werk. SPIN is een systeem voor het vastleggen van inspectiewerkzaamheden en kent ook een eigen module Tijdverantwoording. Zowel SPIN als FATIJDEC ondersteunen de generieke werktijdenregeling van de NVWA niet volledig. Er is daarnaast ook geen eenduidig beeld rond verlof, vergoedingen etc.
Verder zijn deze systemen voor medewerkers niet gebruikersvriendelijk. Zo moeten gegevens in meerdere systemen worden vastgelegd. De directieraad van de NVWA heeft daarom besloten dat medewerkers de tijdverantwoording in de toekomst nog maar in één applicatie moeten doen.
Het doel van het project is het leveren van een (ICT-)voorziening voor een uniforme en duurzame invulling van het proces tijdverantwoording. Belangrijk afgeleid doel is dat de processen voor het registreren van tijd en voor het verwerken van tijd gesplitst worden.

De DTV-oplossing moet gebaseerd worden op de volgende uitgangspunten:

- *Efficiëntie en uniciteit/herbruikbaarheid*

De administratieve belasting voor medewerkers moet gereduceerd worden door middel van het voorkomen van dubbele registraties. De relatie met P-Direkt dient daarbij behouden te blijven. Informatie die is vastgelegd voor de uitvoering binnen het inspectiedomein dient hergebruikt te kunnen worden voor het proces van tijdverantwoording;

- *Kwaliteit*

Het proces van tijdverantwoording dient uniform te zijn en te voldoen aan de werktijdenregeling van de NVWA;

- *Sturing en validatie*

De sturingsmogelijkheden voor medewerkers en management en de controlemogelijkheden op volledigheid dienen verbeterd te worden. De gewenste verscherpte validatie is ook vanuit auditrapporten van de ADR gebleken;

- *Volledigheid*

De werktijdenregeling beschrijft vier verschillende werksituaties waarin werkzaamheden op ongebruikelijke tijden kunnen worden uitgevoerd. Alle medewerkers vallen onder deze regeling en kunnen geconfronteerd worden met één of meerdere van deze werksituaties, eventueel gecombineerd.

1 Inleiding

1.1 Identificatie

Dit document bevat de Project Start Architectuur (PSA) voor het project Duurzame Tijdverantwoording (DTV).

1.2 Leeswijzer

Voor een goed begrip van deze PSA is het aan te bevelen ook het Functioneel Ontwerp, de Informatieanalyse en de Contextanalyse Duurzame Tijdverantwoording te lezen [1][6] en [7].

- In *hoofdstuk 2* van deze PSA worden de doelen beschreven waaraan het project DTV moet bijdragen en wordt het gehanteerde architectuurkader kort beschreven;
- In *hoofdstuk 3* worden de kaders en richtlijnen ten aanzien van de businessarchitectuur beschreven;
- In *hoofdstuk 4* worden de kaders en richtlijnen ten aanzien van de informatiearchitectuur beschreven;
- In *hoofdstuk 5* worden de kaders en richtlijnen ten aanzien van de technische architectuur beschreven;
- In *hoofdstuk 6 en 7* worden de kaders en richtlijnen ten aanzien van beveiliging en privacy en beheer beschreven.

Opmerkingen:
- In dit document wordt met de afkorting DTV het gehele systeem bedoeld (alle (hoofd)functionaliteiten);
- De voorbeelden in dit document zijn ter verduidelijking en niet limitatief;
- In dit document zijn geen architectuurprincipes opgenomen. Vanwege de leesbaarheid zijn alleen de architectuureisen opgenomen, deze zijn richtingbepalend voor de realisatie. De architectuureisen zijn een concrete uitwerking van de architectuurprincipes;
- Elke eis is voorzien van een unieke identificatie (tussen rechte haken [ ]), die aangeeft welke partij verantwoordelijk is voor de eis. Dit kunnen één of meerdere partijen zijn. De volgende indicaties worden gebruikt:

AB	= Applicatiebeheer	FB NVWA	= Functioneel beheer NVWA
IB	= Informatiebeveiliging	L	= Leverancier/DICTU
E	= Eigenaar (NVWA)	SM	= Servicemanagement
KB	= Kwaliteitsborging	TB	= Technisch beheer

1.3 Doel van dit document

Het doel van een project startarchitectuur (PSA) bij het Ministerie van Economische Zaken is het project eenduidige, concrete, relevante en praktisch realiseerbare kaders mee te geven, zodat zeker gesteld wordt dat het projectresultaat past binnen het grotere geheel van de organisatie.

1.4 Referenties

Dit document is aanvullend op de volgende documenten.

#	Referentie	Document
1	Contextanalyse Duurzame Tijdverantwoording	Versie 0.3 – 2 mei 2014 - Pieter Hubregtse (NVWA)
2	Business Case Duurzame Tijdverantwoording	Versie 0.9 – Paul Oling (NVWA)
3	Memo Projectvoorstel Duurzaam Tijdschrijven	12 maart 2014 – Jan Boswijk (NVWA)
4	Integratiearchitectuur EL&I	Henk Romein en Bert Dingemans, 20-11-2012
5	Service Level Agreement voor DICTU Dienstverlening	Relatiemanagement DICTU
6	Informatieanalyse Duurzame Tijdverantwoording	Versie 0.5 – 26 juni 2014 – Pieter Hubregtse (NVWA)
7	Functioneel Ontwerp Duurzame Tijdverantwoording	Versie 0.1 – 4 juli 2014 – Bart Coumans (NVWA)

1.5 Afkortingen en begrippen

DTV	Duurzame Tijdverantwoording
FATIJDEC	Factureren, Tijdschrijven, Declareren
SPIN-VTE	SPIN-Verificatie
SPIN-ORG	SPIN-Opsporing/Interventie
SPIN-CLE	SPIN-Controle
M-SPIN	Mobile-SPIN
OBIEE	Oracle Business Intelligence Enterprise Edition
eBS	eBusiness Suite

2 Kaders

Dit hoofdstuk gaat in op de ambities en doelen van het project DTV en de gewenste situatie die met DTV moet worden bereikt. Vervolgens wordt het gehanteerde architectuurkader kort beschreven.

2.1 Ambitie en doelen DTV

Op dit moment maakt NVWA gebruik van meerdere voorzieningen voor het verantwoorden van tijd, zoals de applicaties FATIJDEC en SPIN. FATIJDEC ondersteunt naast tijdverantwoording ook de verwerking van declaraties en het factureren van bijv. retribueerbaar werk. SPIN is een systeem voor het vastleggen van inspectiewerkzaamheden en kent ook een eigen module Tijdverantwoording. Zowel SPIN als FATIJDEC ondersteunen de generieke werktijdenregeling van de NVWA niet volledig. Er is daarnaast ook geen eenduidig beeld rond verlof, vergoedingen etc.
Verder zijn deze systemen voor medewerkers niet gebruikersvriendelijk. Zo moeten gegevens in meerdere systemen worden vastgelegd. De directieraad van de NVWA heeft daarom besloten dat medewerkers de tijdverantwoording in de toekomst nog maar in één applicatie moeten doen.
Het doel van het project is het leveren van een (ICT-)voorziening voor een uniforme en duurzame invulling van het proces tijdverantwoording. Belangrijk afgeleid doel is dat de processen voor het registreren van tijd en voor het verwerken van tijd gesplitst worden [2].

2.2 Gewenste situatie

De DTV-oplossing moet gebaseerd worden op de volgende uitgangspunten [1]:

- *Efficiëntie en uniciteit/herbruikbaarheid*

De administratieve belasting voor medewerkers moet gereduceerd worden door middel van het voorkomen van dubbele registraties. De relatie met P-Direkt dient daarbij behouden te blijven. Informatie die is vastgelegd voor de uitvoering binnen het inspectiedomein dient hergebruikt te kunnen worden voor het proces van tijdverantwoording;

- *Kwaliteit*

Het proces van tijdverantwoording dient uniform te zijn en te voldoen aan de werktijdenregeling van de NVWA;

- *Sturing en validatie*

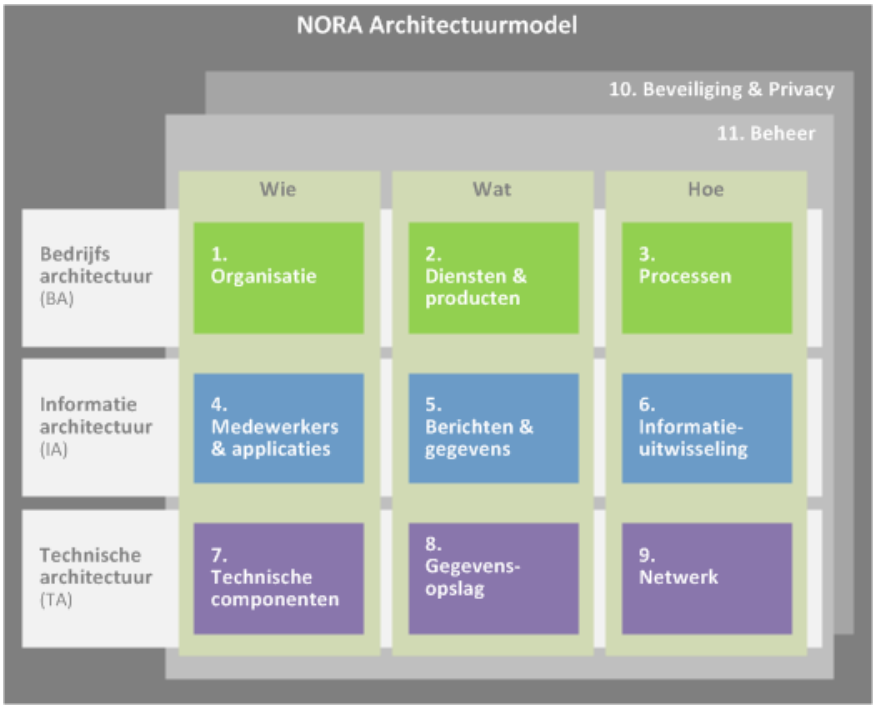
De sturingsmogelijkheden voor medewerkers en management en de controlemogelijkheden op volledigheid dienen verbeterd te worden. De gewenste verscherpte validatie is ook vanuit auditrapporten van de ADR gebleken;

- *Volledigheid*

De werktijdenregeling beschrijft vier verschillende werksituaties waarin werkzaamheden op ongebruikelijke tijden kunnen worden uitgevoerd [1]. Alle medewerkers vallen onder deze regeling en kunnen geconfronteerd worden met één of meerdere van deze werksituaties, eventueel gecombineerd.

2.3 Architectuurkader

Uitgangspunt voor de keuzen in deze PSA is het 9+2-vlaks architectuurraamwerk van NORA. De uitwerking in deze PSA volgt dit raamwerk.



Figuur 1. NORA 9+2 vlaks architectuurraamwerk

2.4 Architectuurkeuzen

De volgende architectuurkeuzen zijn gemaakt voor het project DTV:

- EZ/DICTU kiest voor applicaties/applicatiecomponenten met een beperkte omvang en complexiteit zodat het ontwikkelen, beheren en onderhouden ervan overzichtelijker en eenvoudiger wordt;
- EZ/DICTU kiest voor flexibiliteit binnen deze applicaties door de werking ervan te kunnen aanpassen op basis van configuratie en bij voorkeur niet door het aanpassen van de software. Op die manier kan zo flexibel mogelijk met huidige en toekomstige wensen om worden gegaan;
- EZ/DICTU kiest voor het zoveel mogelijk gebruik maken van herbruikbare componenten. DTV maakt dus enerzijds gebruik van beschikbare herbruikbare componenten en zorgt anderzijds voor het toevoegen van nieuwe herbruikbare componenten. Concreet: de DTV-oplossing moet herbruikbaar zijn in een omgeving die vanuit het programma Blik op 2017 wordt opgebouwd (bijv. een omgeving met een zaaksysteem).

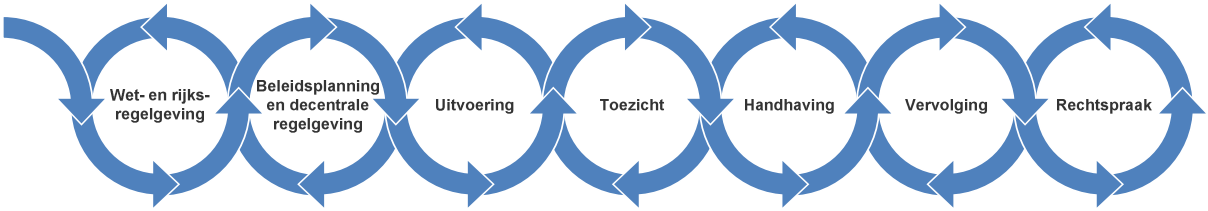
3 Businessarchitectuur (BA)

In dit hoofdstuk wordt de businessarchitectuur beschreven voor zover die van belang is voor de positie en de rol van DTV. Het is een beschrijving in brede zin, dat wil zeggen onafhankelijk van de te kiezen oplossing. In de businessarchitectuur wordt antwoord gegeven op de vragen:

- Wie zijn betrokken?
- Wat zijn de diensten en producten?
- Hoe verlopen de processen?

3.1 Organisatie

Binnen een beleidsdomein worden zeven taken onderscheiden: wet- en (rijks)regelgeving, beleidsplanning en decentrale regelgeving, uitvoering, toezicht, handhaving, vervolging en rechtspraak. In de volgende afbeelding zijn deze taken en hun samenhang weergegeven.



Figuur 2. De 7 taken en hun samenhang

Toelichting op de weergegeven taken:

- *Wet- en rijksregelgeving*: het voorstellen van en besluiten over wijziging van bestaande en invoering van nieuwe wetten, algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen;
- *Beleidsplanning en decentrale regelgeving*: het voorstellen van en besluiten over wijziging van bestaande en nieuwe visies, plannen, programma's en regelgeving, zoals verordeningen van provincies, gemeenten en waterschappen;
- *Uitvoering*: het opvolgen van wet- en regelgeving en beleidsplanning voorafgaand aan en bij het uitvoeren van activiteiten door burgers[1], bedrijven[2] en overheden[3];
- *Toezicht*: het verzamelen van informatie over de vraag of een handeling of zaak voldoet aan de gestelde eisen;
- *Handhaving*: de keten van activiteiten gericht op het (alsnog) laten voldoen van een handeling of zaak aan de gestelde eisen;
- *Vervolging/opsporing*: het instellen van strafrechtelijk onderzoek en het voor de rechter brengen van de resultaten van onderzoek;
- *Rechtspraak*: het geven van een oordeel over een rechtszaak.

1. Personen woonachtig in Nederland of in het buitenland.
2. Ondernemingen gevestigd in Nederland of in het buitenland; ook stichtingen, verenigingen en overheidsorganisaties (die voor eigen activiteiten aanvragen en meldingen indienen).
3. Overheidsorganisaties die betrokken zijn bij het besluiten over ingediende aanvragen en meldingen.

3.1.1 Toezicht, handhaving en vervolging/opsporing

De werkzaamheden van de NVWA hebben betrekking op de taken toezicht, handhaving en (de initiatie van) vervolging/opsporing. De tijdverantwoording in de DTV-oplossing heeft dus ook betrekking op deze taken.

3.1.2 Betrokken partijen bij DTV

3.1.2.1 Medewerkers NVWA

Voor de medewerkers is het van belang één omgeving te hebben waarin straks de tijdverantwoording kan worden gedaan. Op basis van een uniform proces van tijdverantwoording, conform de generieke werktijdenregeling en door middel van een eenmalige invoer van benodigde gegevens. Tevens dient de oplossing de mogelijkheid te bieden een controle uit te kunnen voeren op de volledigheid van de gegevens.

3.1.2.2 Management NVWA

De oplossing dient het management van de NVWA van voldoende sturingsmogelijkheden te kunnen voorzien. Ook voor het management is de controle op volledigheid een onderdeel van het tijdverantwoordingsproces.

3.1.2.3 Auditdienst Rijk (ADR)

De oplossing dient de ADR te kunnen voorzien van de juiste auditgegevens. Zo moet het bijvoorbeeld mogelijk zijn te toetsen op doelmatigheid en rechtmatigheid.

3.1.3 Eisen

De volgende architectuureisen gelden op het gebied van de organisatie.

ID	Eis
BA01.1.01 [E][L]	NVWA houdt rekening met de digitale volwassenheid van de organisatie die gebruik moet maken van DTV en zorgt er samen met DICTU voor dat er meerdere opties zijn om gebruik te maken van DTV (lees: via meerdere kanalen)
BA01.1.02 [E]	NVWA toetst of de configuratie van de oplossing consistent is met de generieke werktijdenregeling van de NVWA en voldoet aan de afspraken binnen de NVWA-organisatie v.w.b. vergoedingen, declaraties, verlofafspraken etc.
BA01.1.03 [E]	Hierop aansluitend; NVWA is verantwoordelijk voor het in gebruik nemen van een juiste en intern vastgestelde werktijdenregeling

3.2 Diensten en producten

3.2.1 Diensten

Om de uitvoering van de tijdverantwoording door de NVWA te kunnen ondersteunen worden de volgende diensten geleverd binnen het project DTV [1]:

1. De DTV-oplossing maakt het mogelijk een complete dagfilm van de tijdsbesteding op te stellen en deze te kunnen valideren;
2. Autorisaties moeten worden bijgehouden van de rubrieken waarop verantwoord mag worden;

3. De dagfilm moet worden verwerkt zodat de juiste op- en toeslagen worden toegekend;
4. Bij de verwerking van tijd worden regels toegepast op basis van de specifieke arbeidsvoorwaarden van een medewerker;
5. Urenpools worden bijgehouden voor bijvoorbeeld vakantiedagen etc.;
6. De juiste gegevens worden gedistribueerd naar de salarisadministratie, zodat de toegekende op- en toeslagen ook daadwerkelijk worden uitbetaald.

De volgende diensten vallen buiten de scope van het project DTV:

1. De registratie van de tijdsbesteding van taken in het productie/uitvoeringsproces. De in de productie/uitvoering geregistreerde tijd wordt wel (her)gebruikt om een timesheet al gedeeltelijk in te vullen;
2. Declaraties, zoals reis- en verblijfkosten;
3. Opstellen van een salarisstrook;
4. Opstellen van managementrapportages op basis van de uurbesteding;
5. Verwerken van uren tot facturen in het kader van 'reversed billing'. Deze uren worden wel beschikbaar gesteld aan de financiële administratie (applicatie Oracle eBS), maar het ophalen en verwerken van de gegevens valt buiten scope;
6. De registratie van de organisatiestructuur (afdelingen en medewerkers) vindt binnen de personeelsadministratie plaats (applicatie P-direkt);
7. Het toepassen van de eindafrekening in het kader van de overgangsregeling voor inconveniënten gebeurt handmatig aan het eind van het jaar.

3.2.2 Producten

3.2.2.1 Een applicatie/applicatiecomponent voor de registratie van tijd

De eerste applicatiecomponent wordt ingezet voor het registreren van tijd. Deze applicatie moet o.a. de volgende functionele wensen kunnen invullen: het ontvangen van productie-uren, het opstellen en valideren van timesheets, het aanvragen en intrekken van autorisaties en het aanvullen van het dagrooster.

3.2.2.2 Een applicatie/applicatiecomponent voor de verwerking van tijd

Deze applicatiecomponent wordt ingezet voor de verwerking van tijd. Het betreft dan functionele wensen als: het bepalen van het tijdvak en rooster, het verwerken van een timesheet en het klaarzetten van de gegevens voor distributie aan de salarisadministratie.

3.2.2.3 Distributiemechanisme/koppelvlak voor de verstrekking van gegevens aan de salarisadministratie

Dit product kan integraal onderdeel zijn van de applicatie(component) Tijdverwerking, maar wordt hier toch apart genoemd. Aan het einde van een payroll-periode moeten de uren per payroll-groep worden geleverd aan P-direkt voor verdere verwerking in de salarisadministratie.

Het is van belang dat gegevens die het juiste functioneren van deze drie producten ondersteunen, beheerd moeten kunnen worden in de DTV-oplossing. Dan denken we

bijvoorbeeld aan de overzichten van feestdagen, referentielijsten, tijdvakken, urenpools en werktijdpakketten.

3.2.3 *Eisen*

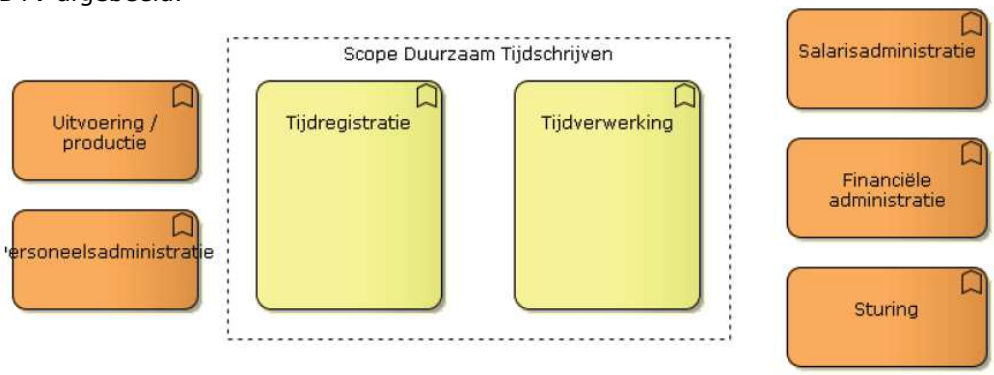
De volgende eisen gelden voor diensten en producten.

ID	Eis
BA02.1.01 [E][L]	DTV levert de diensten 'opstellen en valideren dagfilm', 'bijhouden en intrekken autorisaties', 'verwerken dagfilm', 'toepassen (bedrijfs)regels', 'bijhouden urenpools' en 'distributie naar de salarisadministratie'
BA02.1.02 [E][L]	DTV levert de producten 'applicatiecomponent tijdregistratie', 'applicatiecomponent tijdverwerking' en 'koppelvlak salarisadministratie'
BA02.1.03 [E][L]	Het product 'koppelvlak salarisadministratie' moet gegevens overdragen aan de salarisadministratie (applicatie P-Direkt)

3.3 Processen

3.3.1 *Processen op hoofdlijnen*

In onderstaande figuur staan de belangrijkste procesonderdelen voor het project DTV afgebeeld.



Figuur 3. Procesmodel op hoofdlijnen

Toelichting op de weergegeven procesonderdelen [1]:

- Uitvoering/productie: de uitvoering van taken door een (inspectie)medewerker;
- Personeelsadministratie: daarin worden de gegevens over de medewerkers bijgehouden. Het gaat hier om persoonsgegevens (naam, adres etc.) en arbeidsvoorwaarden (salarisschaal, aantal vakantie/compensatie-uren en modaliteit);
- Tijdregistratie: het verantwoorden van de tijdsbesteding door een medewerker en het valideren door de leidinggevende;
- Tijdverwerking: het verwerken van de gevalideerde en geaccordeerde timesheets. Daarbij worden specifieke tijdvakken bepaald en (bedrijfs)regels toegepast op basis van de arbeidsvoorwaarden van een medewerker;
- Salarisadministratie: het opstellen van de salarisstrook en het uitbetalen van het salaris;
- Financiële administratie: verwerken in de financiële administratie in het kader van 'reversed billing';

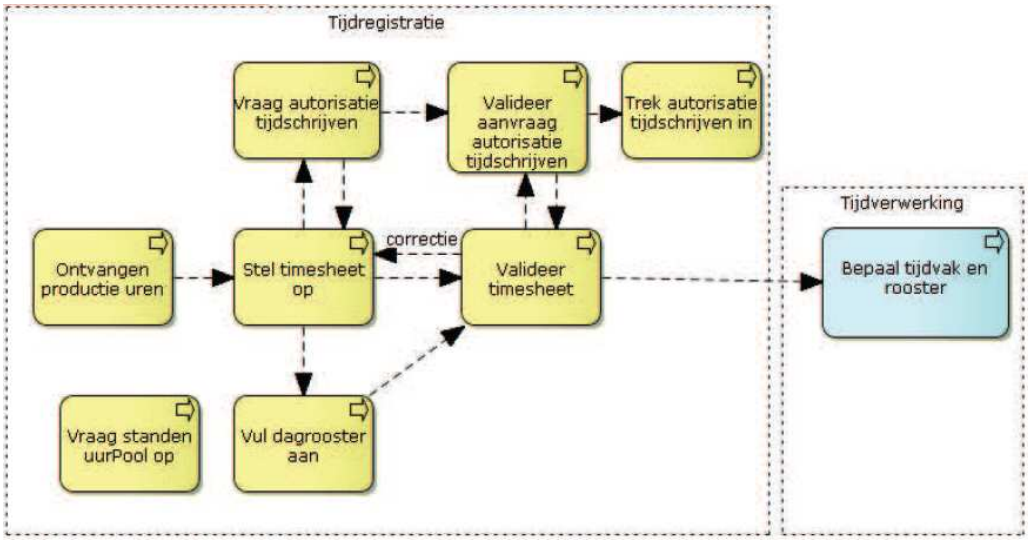
- Sturing: mogelijkheden voor het management en de medewerkers om te sturen op de tijdverantwoording.

3.3.2 *Te ondersteunen processtappen*

Het project DTV zal zich in de kern richten op twee hierboven beschreven procesonderdelen, te weten:
- Tijdregistratie;
- Tijdverwerking.

3.3.3 *Proces Tijdregistratie*

In het (hoofd)proces Tijdregistratie is een aantal processtappen onderkend. Deze staan in onderstaande figuur afgebeeld.



Figuur 4. Processtappen tijdregistratie

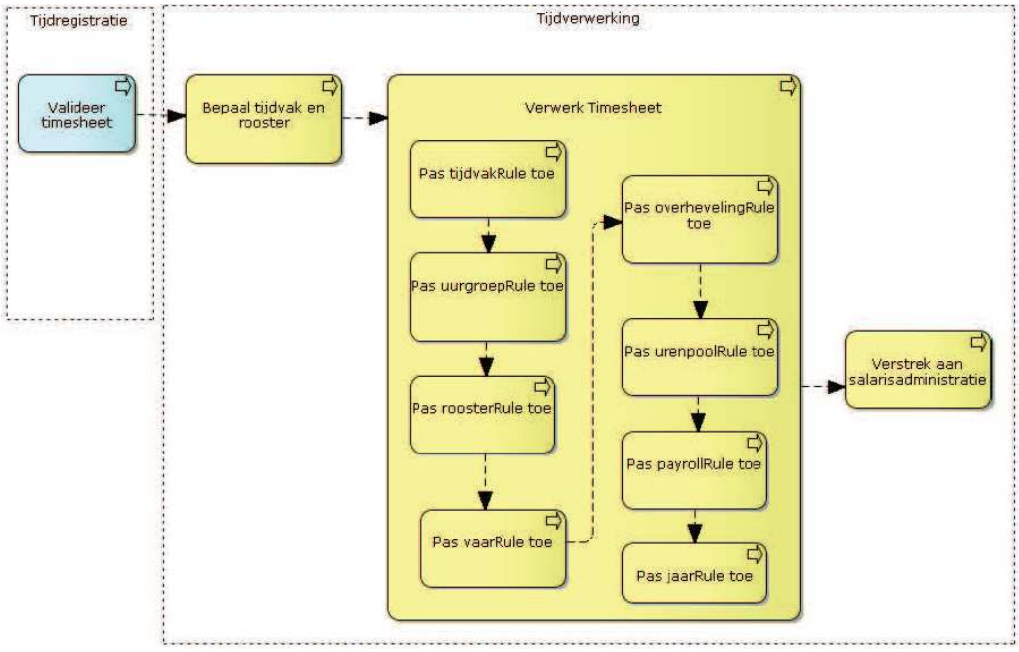
Toelichting op de weergegeven stappen [1]:

- Ontvangen productie-uren: tijdens het productieproces worden begin- en eindtijden van taken geregistreerd. Deze tijden zijn over het algemeen verbonden met de afhandeling van een zaak, zoals een inspectie. Deze tijden worden gebruikt voor de facturering naar de klant en het vullen van de timesheets;
- Opstellen timesheet: een medewerker moet per dag tijd verantwoorden. Voor bepaalde medewerkers is een deel van de tijd al verantwoord in het productie/uitvoeringsproces (bijv. tijdens inspecties) en vooringevuld in de timesheet;
- Aanvragen autorisatie: er is een directe relatie tussen het opstellen van een timesheet en de autorisatie. Een medewerker kan alleen registreren op bijv. een activiteit, project of kostenplaats als hij/zij geautoriseerd is;
- Valideer autorisatie: de aanvraag van een autorisatie wordt gevalideerd door de leidinggevende en goed- of afgekeurd;
- Intrekken autorisatie: een leidinggevende kan een gegeven autorisatie beëindigen;
- Valideren timesheet: de leidinggevende krijgt iedere week de afgesloten timesheets aangeboden en valideert deze. Bij afkeuring wordt deze ter correctie

opnieuw aangeboden aan de medewerker. De gevalideerde en goedgekeurde sheets worden aangeboden aan het (hoofd)proces tijdverwerking;
- Standen urenpool: de medewerker kan de standen van de urenpools opvragen, zoals het resterende aantal vakantiedagen (dit zijn gegevens die vanuit de applicatie P-direkt komen);
- Aanvullen dagrooster: een medewerker heeft een standaard werkrooster dat gekoppeld is aan zijn/haar werktijdenprofiel. Het werkrooster bepaalt welke (bedrijfs)regels worden toegepast binnen het proces tijdverwerking. Indien een medewerker volgens een afwijkend rooster heeft gewerkt, moet dit worden geregistreerd in het dagrooster.

3.3.4 Proces tijdverwerking

In het (hoofd)proces Tijdverwerking is een aantal processtappen onderkend. Deze staan in onderstaande figuur afgebeeld.



Figuur 5. Processtappen tijdverwerking

Toelichting op de weergegeven stappen [1]:

- Bepalen tijdvak en rooster: iedere regel in een aangeleverde (gevalideerde en goedkeurde) timesheet wordt gesplitst naar een tijdvak en een rooster. Als een regel verdeeld is over meerdere uurtijdvakken, wordt deze gesplitst per uurtijdvak. Als meerdere roostersoorten van toepassing zijn, wordt ook nog gesplitst naar roostersoort. Uiteindelijk leidt dit tot één of meerdere tijdvakresultaten;
- Verwerken van de timesheet: op de uiteindelijke tijdvakresultaten worden meerdere (bedrijfs)regels toegepast (uitgebreide beschrijvingen staan in [1] en [6]):
    - Jaar Rule;
    - Overheveling Rule;
    - Payroll Rule;
    - Rooster Rule;
    - Tijdvak Rule;

    - Urenpool Rule;
    - Uurgroep Rule;
    - Vaar Rule.
- Verstrekken aan de salarisadministratie: de uren worden per payroll-groep aan P-direkt geleverd.

3.3.5 Eisen

De volgende eisen gelden voor processen.

ID	Eis
BA03.1.01 [E]	De DTV-oplossing ondersteunt NVWA-medewerkers bij de (hoofd)processen 'tijdregistratie' en 'tijdverwerking'
BA03.1.02 [E]	Elke tijdverantwoording moet te relateren zijn aan een combinatie van 'activiteit', 'project' en 'kostenplaats'

4 Informatiearchitectuur (IA)

In dit hoofdstuk wordt de informatiearchitectuur beschreven. Deze is bepalend voor de te kiezen technische oplossingen. Het is een beschrijving in brede zin, dat wil zeggen onafhankelijk van de te kiezen technische oplossingen. In de informatie-architectuur wordt antwoord gegeven op de vragen:

- Wie zijn de uitvoerders?
- Wat zijn de gegevens en berichten?
- Hoe verloopt de informatie-uitwisseling?

4.1 Gebruikers en applicaties

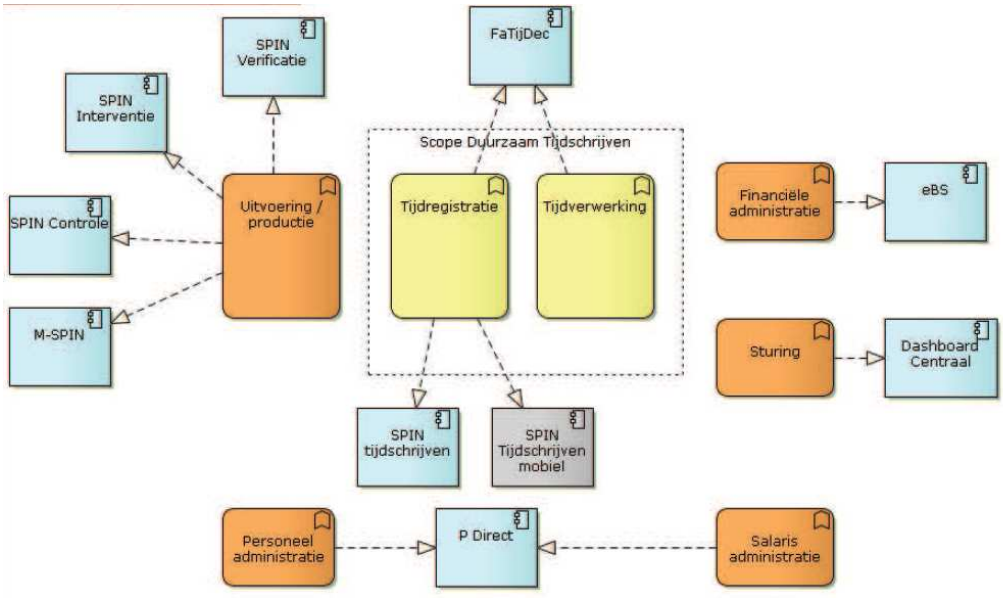
4.1.1 Gebruikers

In principe hebben we het over drie categorieën gebruikers:

- NVWA-medewerkers die de tijdregistratie moeten uitvoeren;
- Managers/leidinggevenden die de timesheets en autorisaties goedkeuren/afwijzen, maar ook sturingsinformatie verkrijgen vanuit de DTV-oplossing;
- De Auditdienst Rijk (ADR) die op basis van gegevens in de DTV-oplossing haar audits kan uitvoeren.

4.1.2 Applicaties

Om de huidige tijdverantwoording op basis van de applicaties SPIN en FATIJDEC te verbeteren moeten er twee generieke applicatiecomponenten komen, te weten één voor de tijdregistratie en één voor de tijdverwerking.
In de volgende afbeelding zijn de huidige/bestaande applicaties/applicatiemodules en hun businessfuncties weergegeven. Deze businessfuncties sluiten aan op de in het vorige hoofdstuk aangegeven procescomponenten.



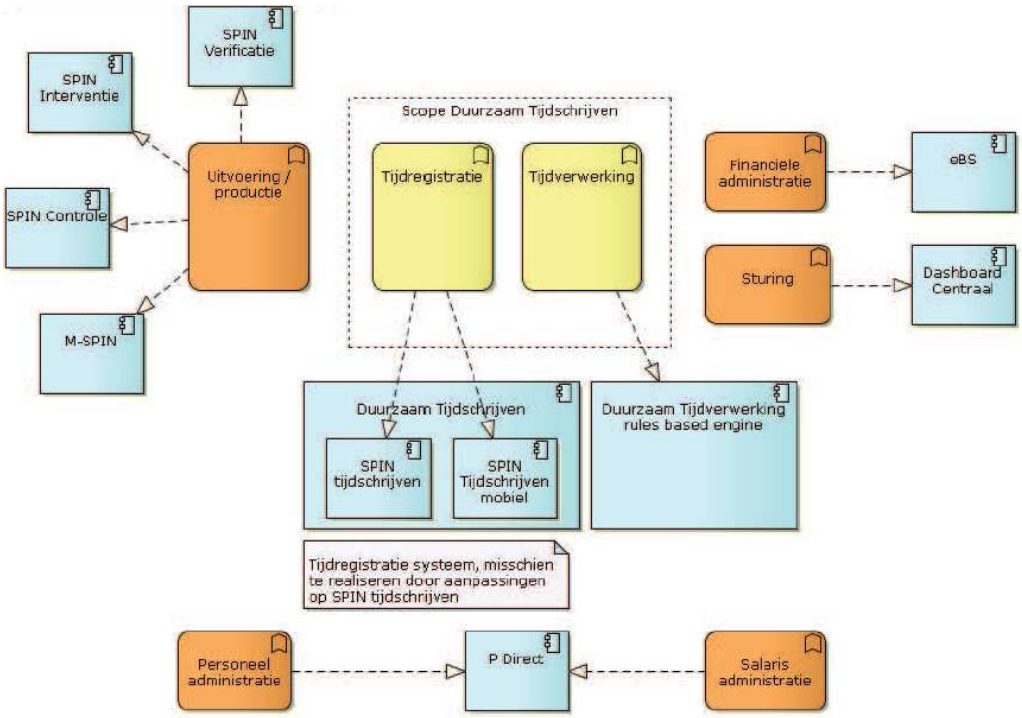
Figuur 5. IST-applicatieoverzicht en hun businessfuncties

Businessfuncties

- De tijdregistratie vindt deels plaats in FATIJDEC en deels in (Mobile-)SPIN. FATIJDEC is op dit moment ook de gegevensleverancier van P-Direkt, v.w.b. uren en toeslagpercentages;
- De verwerking van tijd vindt plaats in FATIJDEC;
- De salaris- en personeelsadministratie vindt plaats in P-Direkt. P-Direkt levert gegevens over medewerkers en de inrichting van de organisatie. De applicatie ontvangt gegevens van FATIJDEC v.w.b. uren en toeslagpercentages;
- Het productieproces (zoals inspecties) vindt plaats in de SPIN-modules Verificatie (VTE), Controle (CLE) en Opsporing/Interventie (ORG) en ook in de mobiele versie van SPIN, M-SPIN;
- Sturingsinformatie komt beschikbaar via de Oracle Business Intelligence Enterprise Edition (OBIEE), ook wel Dashboard Centraal genoemd;
- De financiële administratie van de NVWA en dus ook het proces van 'reversed billing' vindt plaats in Oracle eBS.

4.1.2.1 SOLL-situatie

In de SOLL-situatie zullen de businessfuncties tijdregistratie en tijdverwerking worden afgehandeld in een tweetal gescheiden applicatiecomponenten.



Figuur 6. SOLL-applicatieoverzicht en hun businessfuncties

Businessfuncties

Verschil met de IST-situatie zit vooral in het wegvallen van FATIJDEC als applicatie voor tijdregistratie en tijdverwerking.

- De tijdregistratie zal plaatsvinden in de huidige module Tijdschrijven in de applicatie (Mobile-)SPIN. Dit betekent een aanpassing van deze module om deze geschikt te maken voor de (generieke) werktijdenregeling van de NVWA;

- De tijdverwerking zal in een nieuwe applicatiecomponent worden opgenomen. Deze component zal ook een 'engine' moeten bevatten die overweg kan met de verschillende bedrijfsregels die van toepassing zijn op het hoofdproces tijdverwerking;
- De overige bedrijfsfuncties blijven gehandhaafd.

4.1.2.2 Servicegerichte architectuur

De DTV-oplossing en de (herbruikbare) applicatiecomponenten waar deze oplossing gebruik van gaat maken worden bij voorkeur opgezet op basis van servicegerichte architectuurprincipes.
Dit betreft onder andere (data)services voor de uitwisseling van gegevens en daarmee dus ook de definitie van berichten(boeken) voor de koppelvlakken met aanleverende en afnemende systemen.
Echter, uitgaande van bovenstaande oplossing op basis van tijdregistratie in SPIN, zal een servicegerichte architectuur niet volledig haalbaar zijn. De interfaces tussen de (productie)modules van SPIN (VTE, ORG en CLE) en de SPIN-module voor tijdschrijven zijn niet gebaseerd op (web)services. Gezien het programma Blik op 2017 is het advies hier nu geen wijzigingen in aan te brengen. De nieuwe applicatiecomponent voor de verwerking van tijd zal een servicegerichte architectuur wel moeten volgen.

4.1.2.3 (Functionele) applicatiecomponenten en businessfuncties

De DTV-oplossing gaat bestaan uit specifieke en herbruikbare functionaliteiten. Specifiek in de zin dat de hiervoor beschreven businessfuncties specifiek zijn voor de processen tijdregistratie en tijdverwerking. Maar herbruikbaar in de zin dat de benoemde (functionele) applicatiecomponenten herbruikbaar moeten zijn, mogelijk in een nieuw applicatielandschap vanuit het programma Blik op 2017.
De componenten worden daarom ook wel herbruikbare bouwstenen genoemd, nodig voor het realiseren van twee applicaties/applicatiecomponenten.

Deze applicatiecomponenten dienen ontsloten te worden via een drietal interactiekanalen:
- Web/Internet (HTML);
- Mobiel (HTML);
- Apps (Mobiel en tablets).

Een interactiekanaal is een manier waarop gebruikers kunnen werken met de DTV-applicaties. Ongeacht via wel kanaal een gebruiker werkt met de DTV-oplossing, het resultaat zal hetzelfde moeten zijn.
Vanuit de gedachte van een servicegerichte architectuur betekent dit dus dat het niet is toegestaan om businesslogica in de presentatielaag van de DTV-oplossing op te nemen. De DTV-applicaties maken dus gebruik van dezelfde DTV-services als systemen die mogelijk in de toekomst gaan koppelen.

In hoofdstuk 5 (Technische architectuur (TA)) wordt de doorvertaling gemaakt van deze (functionele) applicatiecomponenten naar technische componenten. In het technische componentenmodel is aangegeven welke componenten (reeds) beschikbaar zijn (lees: herbruikbaar) en welke componenten als onderdeel van het project DTV opgeleverd dienen te worden (lees: herbruikbaar vanuit het project DTV).
DICTU maakt de beweging naar herbruikbare (functionele) componenten die EZ-, maar ook inspectiebreed inzetbaar moeten zijn. Dit betekent dat het project DTV

enerzijds beschikbare herbruikbare componenten moet kunnen hergebruiken en anderzijds nieuwe componenten als herbruikbare componenten op wil leveren, die weer ingezet kunnen worden voor andere applicaties (voor andere opdrachtgevers).

Een businessfunctie maakt gebruik van één of meer (functionele) componenten (bouwblokken). De businessfuncties zijn zoals gezegd gespecialiseerd/specifiek voor een bepaalde taak of functie en afgestemd op het proces waarin ze toegepast worden. Voor herbruikbare componenten hanteert DICTU het principe: 'hergebruiken voor kopen voor bouwen'. Waar componenten nog niet beschikbaar zijn, wordt zowel binnen als buiten de EZ-organisatie gekeken naar mogelijk te hergebruiken componenten. Eventuele nieuwe benodigde functionaliteit kan worden opgenomen in een bestaande component. Als dat niet mogelijk of wenselijk is, moet de extra functionaliteit dus met een nieuwe herbruikbare component gerealiseerd worden.

4.1.3 Flexibiliteit en wendbaarheid

Flexibiliteit en wendbaarheid bij de inrichting van de DTV-oplossing, met andere woorden de mogelijkheid de oplossing snel aan te kunnen passen aan gewijzigde en nieuwe situaties, zijn bepalend voor het succes van DTV.
Om deze flexibiliteit te kunnen bereiken wordt een aantal belangrijke mechanismen ingezet:

- De al eerder genoemde toepassing van een servicegerichte architectuur;
- De werking van de applicaties worden aangepast op basis van configuratie en niet op basis van het aanpassen van de software;
- Het toepassen van een rule engine om (flexibel) overweg te kunnen met de tijdvakresultaten uit de timesheets.

Door gebruik te maken van deze mechanismen is de werking van het systeem eenvoudig aan te passen.

4.1.4 Eisen

Applicaties/applicatiecomponenten
De volgende eisen gelden voor de applicaties/applicatiecomponenten.

ID	Eis
IA01.1.01 [L]	Elke applicatie(component) is geheel zelfstandig, moet onafhankelijk van andere applicaties kunnen werken en kent een eigen ontwikkel- en beheercyclus
IA01.1.02 [L]	Elke applicatie heeft een eigen gebruikersinterface waarmee functionaliteit wordt aangeboden aan de eindgebruikers
IA01.1.03 [L]	Elke applicatie controleert of alle verplichte informatie ingevuld en geldig is, voordat deze wordt aangeboden aan een volgende component. Dit zorgt voor een optimale gebruikerservaring en voorkomt het overbodig heen en weer sturen van informatie tussen de gebruikte componenten
IA01.1.04 [L]	Elke applicatie heeft een eigen beheerinterface waarin de beheerder alles kan doen en instellen wat voor de werking van de applicatie nodig is
IA01.1.05 [L]	Elke applicatie moet in zijn geheel kunnen worden overgedragen aan een andere eigenaar, kunnen worden overgezet naar een andere/nieuwe omgeving of kunnen worden vervangen zonder dat de werking van de functionaliteit voor afnemende applicaties daardoor wijzigt
IA01.1.06 [L]	De koppelvlakken die de applicatie gebruikt (product- en leverancierneutraal) kunnen ook worden aangeboden aan andere systemen. Hiermee is de functionaliteit van de applicatie beschikbaar voor andere applicaties

Servicegerichte architectuur
De volgende eisen gelden voor (web)services.

ID	Eis
IA01.2.01 [L]	Services kennen een eigen ontwikkel- en beheercyclus. Ze worden zelfstandig ontwikkeld en kunnen onafhankelijk van elkaar en de applicaties uitgerold en getest worden
IA01.2.02 [L]	(Functionele) applicatiecomponenten hebben voor het beheer eigen webservices waarmee beheerfunctionaliteit wordt ontsloten
IA01.2.03 [L]	(Functionele) applicatiecomponenten communiceren met elkaar op basis van webservices

Businessfuncties
De volgende eisen gelden voor de businessfuncties (deze eisen liggen in lijn met die voor applicaties/applicatiecomponenten).

ID	Eis
IA01.3.01 [L]	Elke businessfunctie is geheel zelfstandig, moet onafhankelijk van andere businessfuncties kunnen werken en kent een eigen ontwikkel- en beheercyclus. Businessfuncties kunnen onafhankelijk van elkaar en de applicaties uitgerold en getest worden
IA01.3.02 [L]	Echter, een businessfunctie binnen een applicatie moet functioneren als één samenhangend geheel
IA01.3.03 [L]	Een businessfunctie moet in zijn geheel kunnen worden overgedragen aan een andere eigenaar, naar een andere omgeving kunnen worden overgezet of kunnen worden vervangen zonder dat de werking van de businessfunctie voor afnemende applicaties daardoor wijzigt

4.2 Berichten en gegevens

4.2.1 Berichten

Geautomatiseerde informatie-uitwisseling gebeurt via webservices. Systemen kunnen elkaar elektronische berichten toesturen, deze lezen en beantwoorden.

4.2.2 Dataservices

Een belangrijke functie in de DTV-oplossing is het uitwisselen van gegevens tussen verschillende applicaties/applicatiecomponenten (en bijbehorende bedrijfsfuncties). Het gaat daarbij om gestructureerde gegevens. Voorbeelden van deze uitwisseling zijn:

- Uitwisseling van uurcomponenten vanuit de applicatie Tijdverwerking aan de applicatie eBS (financiële administratie);
- Uitwisseling van organisatie- en medewerkergegevens vanuit P-Direkt (personeelsadministratie) aan de componenten Tijdregistratie- en verwerking;
- Uitwisseling van uren uit het productieproces in SPIN met de component Tijdregistratie.

Hiervoor is al aangegeven dat bij de uitwisseling met P-direkt (bestandsoverdracht) en bij het (her)gebruiken van de module SPIN-Tijdschrijven het gebruik van webservices, zoals het zich nu laat inzien, niet mogelijk is en dat de huidige koppelvlakken gehandhaafd blijven.

Voor de overige koppelvlakken is het aan te bevelen voor de dataservices een centraal kernbericht te definiëren dat generiek inzetbaar is.

4.2.3 Overige koppelvlakken

Naast het genoemde (generieke) kernbericht kent de DTV-oplossing dus de volgende koppelvlakken:

- Bestaande bestandsoverdracht aan P-Direkt t.b.v. de salarisadministratie (batchproces);
- Batchproces om de timesheet-regels vanuit de component Tijdregistratie te splitsen naar de uiteindelijke tijdvakresultaten in de component Tijdverwerking;

4.2.4 Dynamisch berichtinhoud

Bij berichten wordt vaak onderscheid gemaakt tussen een statisch deel en een dynamisch deel. Een wijziging in het statisch deel van een bericht vereist een nieuwe versie van het koppelvlak. Het dynamisch deel kan wijzigen zonder dat een nieuwe versie van het koppelvlak nodig is.

Een wijziging in bijv. de werktijdenregeling of in de verschillende werksituaties kan leiden tot een wijziging in het kernbericht. Dit betekent dat de inhoud van berichten aanpasbaar moet zijn zonder dat de software van de applicatie aangepast hoeft te worden.
Dit leidt dan altijd tot het publiceren van een nieuwe versie van de relevante berichtdefinities (koppelvlak). Dit koppelvlak is van toepassing op zowel aanbiedende als afnemende systemen/applicaties. De DTV-oplossing moet met deze dynamiek om kunnen gaan. Een wijziging in een bericht heeft ook impact op systemen van leverende partijen.

4.2.5 Berichtdefinitie

Het moet mogelijk zijn om nieuwe berichttypen te definiëren en bestaande berichten te wijzigen zonder dat de software hoeft te worden aangepast. Met deze functionaliteit wordt de berichtopbouw gedefinieerd op basis van berichtonderdelen, Met andere woorden, wordt gedefinieerd uit welke berichtonderdelen een bericht bestaat.

4.2.6 Eisen

Berichten

ID	Eis
IA02.1.01 [L]	De berichten die verstuurd en ontvangen worden, worden per applicatie beschreven in een berichtencatalogus. Dit is een functionele beschrijving. Daarnaast zijn de WSDL's en XSD's beschikbaar
IA02.1.02 [L]	De termen in het centrale kernbericht zijn gegeneraliseerd zodat deze breder bruikbaar zijn
IA02.1.03 [L]	Met berichtdefinities kunnen nieuwe berichttypes worden gedefinieerd en bestaande beheerd
IA02.1.04 [L]	Het wijzigen van bijv. de werktijdenregeling of werksituaties leidt altijd tot het publiceren van een nieuwe versie van een koppelvlak
IA02.1.05 [L]	Het dynamisch deel van berichten kan wijzigen zonder dat een nieuwe versie van het koppelvlak nodig is. De DTV-oplossing moet met deze dynamiek van berichten om kunnen gaan. Ook aanleverende en ontvangende systemen moeten

	met deze dynamiek van berichten om kunnen gaan
IA02.1.06 [L]	Een berichtdefinitie bepaalt uit welke berichtonderdelen een bericht bestaat en wat aan welk berichtonderdeel gekoppeld is
IA02.1.07 [L]	De inhoud van berichten moet aangepast kunnen worden zonder dat de software hoeft te worden aangepast

4.2.7 Gegevens

4.2.7.1 Eisen

ID	Eis
IA02.2.01 [L]	De definities en modellering van de gegevens volgen het gegevensmodel uit de context- [1] en informatieanalyse [6]. Dit gegevensmodel beschrijft de business in termen van de objecttypen waarvan de kenmerken en eigenschappen (gegevens) relevant zijn
IA02.2.02 [L]	De definities en modellering van de gegevens worden per applicatiecomponent beschreven in een gegevenscatalogus. Een gegevenscatalogus is een document die door de business gelezen en begrepen kan worden

4.3 Informatie-uitwisseling

De informatie-uitwisseling betreft de koppelvlakken tussen de applicaties/applicatiecomponenten binnen de DTV-oplossing.

4.3.1 Financiële administratie

Dit betreft een (data)service vanuit de applicatiecomponent Tijdverwerking naar de applicatie eBS.

Toelichting op de weergegeven koppeling:
- Deze wordt gebruikt om 'reversed billing' uit te voeren.

4.3.2 Personeelsadministratie

Dit betreft het koppelvlak tussen de applicatie P-Direkt en de applicatiecomponenten Tijdregistratie en Tijdverwerking (op basis van bestandsoverdracht).

Toelichting op de weergegeven koppeling:
- Deze wordt gebruikt om organisatie- en medewerkersgegevens aan het proces van tijdverantwoording te leveren.

4.3.3 SPIN VTE, CLE en ORG (Productieproces)

Dit betreft een service tussen de SPIN-modules Verificatie, Controle en Opsporing en de component Tijdregistratie. Deze component is de hergebruikte en gewijzigde module SPIN-Tijdschrijven, dus zal het koppelvlak geen webservice zijn, maar een databasekoppeling.

Toelichting op de weergegeven koppeling:
- Deze wordt gebruikt om productie/uitvoeringsuren aan het proces Tijdregistratie te leveren en die uren in deze component te ontvangen.

4.3.4 Salarisadministratie

Dit betreft een batchproces/bestandsoverdracht tussen de applicatiecomponent Tijdverwerking en de applicatie P-Direkt.

Toelichting op de weergegeven koppeling:
- Deze wordt gebruikt om informatie over uren en toeslagpercentages vanuit het proces Tijdverwerking aan de salarisadministratie te leveren.

4.3.5 Component Tijdregistratie naar component Tijdverwerking

Dit betreft een koppelvlak tussen de applicatiecomponent Tijdregistratie en de applicatiecomponent Tijdverwerking. Ook hier geldt weer dat, vanwege het feit dat de component Tijdregistratie de hergebruikte en gewijzigde module SPIN-Tijdschrijven is, deze koppeling (mogelijk) geen webservice kan zijn, maar een databasekoppeling.

Toelichting op de weergegeven koppeling:
- Deze wordt gebruikt om de gevalideerde en goedgekeurde timesheets vanuit het proces Tijdregistratie aan het proces Tijdverwerking te leveren.

4.3.6 Versies

Bij informatie-uitwisseling wordt gebruik gemaakt van gestandaardiseerde koppel-vlakken. Een koppelvlak definieert hoe de gegevens worden uitgewisseld. Bij het wijzigen van een koppelvlak moet het mogelijk zijn om een voorgaande versie voor een beperkte periode te blijven gebruiken. Hierdoor wordt het beschikbaar komen van een koppelvlak ontkoppeld van het gebruik ervan. Dit voorkomt wederzijdse afhankelijkheden bij het introduceren van nieuwe koppelvlakken.

4.3.7 Eisen

ID	Eis
IA03.1.01 [L]	Bij het ontwikkelen van de DTV-oplossing worden het standaardenregister EZ en de overheidsstandaarden aangehouden zoals vastgesteld door het Forum Standaardisatie (http://www.forumstandaardisatie.nl)
IA03.1.02 [L]	Als er geen relevante standaard is vastgesteld in het standaardenregister EZ of door het Forum Standaardisatie dan wordt een standaard in overleg met en na goedkeuring van de DICTU-architecten gekozen. Hierbij wordt, in de aangegeven volgorde, gekeken naar overheids-, open- en de facto standaarden
IA03.1.03 [L]	Voor de informatie-uitwisseling tussen systemen wordt bij voorkeur gebruik gemaakt van de servicebustechnologie van DICTU (3 tier-architectuur)
IA03.1.04 [L]	Kennis over de koppelvlakversie is ontkoppeld van de applicatie(component)
IA03.1.05 [L]	De in 4.3.1 t/m 4.3.5 genoemde koppelingen zijn onderdeel van de oplossing en dienen gerealiseerd te worden

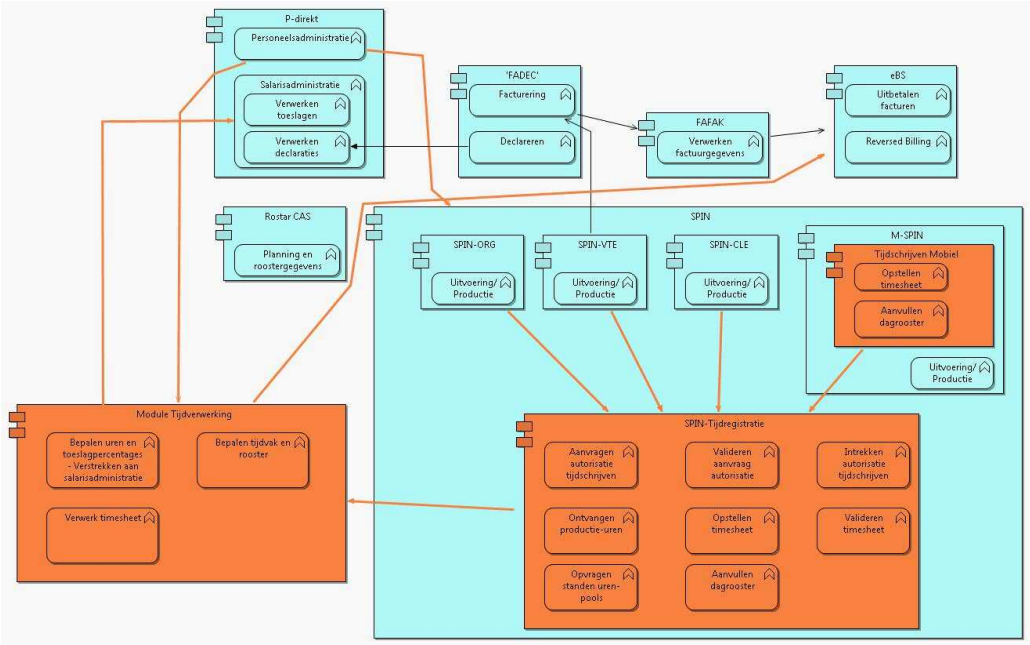
5 Technische architectuur (TA)

In dit hoofdstuk worden de kaders en richtlijnen ten aanzien van de technische architectuur beschreven. Dit is bepalend voor de te kiezen oplossing of de te beschrijven alternatieven. De technische architectuur omvat bijv. de volgende aspecten:

- Wie/wat leveren/levert de functionaliteit?
- Wat is nodig voor opslag?
- Hoe verloopt de communicatie?

5.1 Technische componenten

De afbeelding hieronder geeft een overzicht van de technische componenten die nodig zijn voor het realiseren van de DTV-oplossing (in oranje). Dit overzicht is een doorvertaling van de (functionele) applicatiecomponenten zoals beschreven in de hoofdstukken 3 en 4. De platen met de functionele componenten en de platen met de technische componenten hanteren dezelfde opbouw en categorisering, waardoor de componenten aan elkaar te relateren zijn. Een functioneel component kan bestaan uit meerdere technische componenten. Onderstaande plaat staat groter afgebeeld aan het einde van deze PSA.



Figuur 7. Overzicht technische componenten en koppelvlakken

5.1.1 Tijdregistratie in SPIN-Tijdschrijven

Er is gekozen voor een alternatief waarin het proces Tijdregistratie wordt uitgevoerd in de bestaande module SPIN-Tijdschrijven. Deze module inclusief de koppelvlakken voldoen zoals eerder aangegeven niet goed aan de huidige (generieke) werktijdenregeling en zullen moeten worden aangepast. FA(TIJ)DEC wordt dan niet meer gebruikt voor de tijdverantwoording en zal alleen nog worden ingezet voor facturatie en declaratie.

De technische componenten in dit alternatief zijn onder te verdelen in de volgende categorieën:

- Componenten die al beschikbaar zijn, zoals de module SPIN-Tijdschrijven, inclusief de daarbij al in gebruik zijnde koppelvlakken;
- Componenten die door het project DTV nieuw geleverd gaan worden:
    - De module Tijdverwerking;
    - Een aantal nieuwe koppelvlakken voor de informatie-uitwisseling, zoals beschreven in H-4.3.

Herbruikbare componenten kunnen daarbij afkomstig zijn van andere partijen.

Voordelen van deze oplossing:

- Hergebruik van de bestaande module SPIN-Tijdschrijven voor het proces van tijdregistratie, inclusief de koppelvlakken tussen de productiemodules en SPIN-Tijdschrijven;
- Kennis van de SPIN-applicatie is aanwezig binnen de EZ-organisatie.

Nadelen van deze oplossing:

- De huidige module SPIN-Tijdschrijven is niet direct bruikbaar, maar vergt aanpassingen en uitbreidingen. Zo moeten er meerdere schermfuncties worden gebouwd: voor het opstellen van de timesheet (deze moet ook beschikbaar zijn in de mobiele variant (app)), voor het aanvragen van een autorisatie, voor het valideren van een autorisatie, voor het intrekken van een autorisatie, voor het valideren van de timesheet, voor het opvragen van urenpools en voor het vullen van het (dag)rooster (ook deze in een mobiele variant));
- Voor een aantal koppelvlakken wordt de servicegerichte architectuur losgelaten;
- Vanuit het oogpunt van het programma Blik op 2017 is de module SPIN-Tijdschrijven niet (goed) herbruikbaar als losse applicatiecomponent in bijvoorbeeld de context van een nieuw zaaksysteem.

5.1.2 Eisen technische componenten

5.1.2.1 Eisen webinterface en interactiekanalen

ID	Eis
TA01.1.01 [L]	Alle user interfaces ondersteunen minimaal de interactiekanalen Webbrowser en Mobiel/app
TA01.1.02 [L]	De specifieke eisen voor de herbuikbare componenten worden in de specificatiefase uitgewerkt. Algemene richtlijnen ten aanzien van herbruikbare componenten, zoals in dit document benoemd, zijn hierbij leidend
TA01.1.03 [L]	De webinterface van de DTV-oplossing en de herbruikbare componenten kunnen met een standaard webbrowser bediend worden zonder het installeren van add-ons ofwel plugins
TA01.1.04 [L]	Alle standaard webbrowsers en versies die een marktaandeel van meer dan 5% hebben moeten ondersteund worden
TA01.1.05 [L]	De webinterface moet ook correct werken op elke mobiele OS-versie (Android, iOS en Windows Phone) met een marktaandeel van meer dan 5%
TA01.1.06 [L]	De DTV-oplossing, voor zowel gebruikers als beheerders, is in het Nederlands

5.1.2.2 Eisen responsiveness

Een webpagina dient zo snel mogelijk opgebouwd te worden. Om dit te bereiken is de webpagina direct zichtbaar en bruikbaar en wordt dynamische content in de achtergrond opgehaald en toegevoegd.

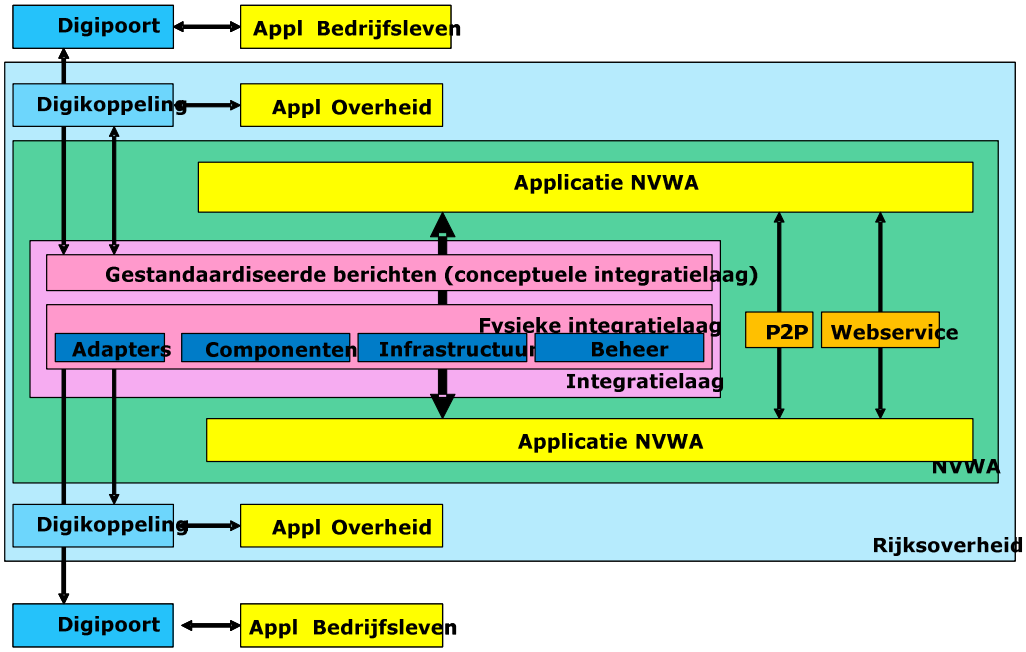
ID	Eis
TA01.2.01 [L]	Om een optimale gebruikerservaring te bereiken wordt bij voorkeur gewerkt met asynchrone achtergrond-calls.
TA01.2.02 [L]	De gebruikersinterface is geschikt voor verschillende type devices (touch, no touch, desktop, mobile, tablet)

5.1.2.3 Eisen datacenter

ID	Eis
TA01.3.01 [TB]	Voor de DTV-oplossing wordt gebruik gemaakt van het DICTU-(Rijks)datacenter
TA01.3.02 [TB]	De applicatiecomponenten/DTV-oplossing worden centraal geplaatst

5.1.2.4 Eisen Servicebustechnologie/integratiearchitectuur

De DTV-oplossing maakt v.w.b. de ontsluiting van services en koppelvlakken (uiteraard afhankelijk van de mogelijkheden binnen de gekozen oplossing) gebruik van servicebustechnologie (Oracle ESB). Dit platform draait in een DICTU-(Rijks)datacenter. Dit platform levert gestandaardiseerde middlewareproducten en componenten waar software en services gebruik van maken.



Figuur 8. Model integratiearchitectuur

In bovenstaand model [4] van de integratiearchitectuur zijn in het 'NVWA-deel' de mogelijke integratievormen bij interne applicaties afgebeeld. Steeds verder naar

buiten zien we in de figuur de informatiesystemen van de Rijksoverheid en het bedrijfsleven.
Uiteraard vindt integratie bij voorkeur plaats via generieke voorzieningen binnen de integratielaag, maar we zullen er bij de DTV-oplossing niet aan ontkomen dat zich in het applicatielandschap nog Point-to-Point-koppelingen, directe koppelingen tussen applicaties op basis van webservices of zelfs nog bestandsuitwisseling (inclusief FTP/SFTP) bevinden. Dit is hier het geval bij projectspecifieke zaken, bij bestaande legacy-systemen of ketenpartnerbeperkingen (lees: P-Direkt). Dit zijn, zoals eerder in dit hoofdstuk aangegeven, geen toekomstvaste oplossingen.

De gewenste integratielaag is opgebouwd uit een conceptuele integratielaag, met definities van gestandaardiseerde berichten, en een technische implementatie/fysieke integratielaag bestaande uit een beheerde omgeving van componenten en infrastructuur. Deze worden technisch ontsloten met een aantal implementatiewijzen zoals Business Process Engineering Language (BPEL), Enterprise Service Bus (ESB) en andere componenten.
De integratie met andere overheden en het bedrijfsleven vindt bij voorkeur plaats via Rijksbrede voorzieningen als Digikoppeling en Digipoort.

In deze figuur verloopt de communicatie bijvoorbeeld als volgt:
1. Een applicatie/informatiesysteem van een leverancier genereert een bericht en verzendt deze naar de Digipoort-voorziening. Dit kan bijvoorbeeld een elektronische factuur zijn;
2. Het bericht met de elektronische factuur wordt ontvangen door Digipoort. Digipoort bepaalt aan de hand van het bericht wie de geadresseerde overheidspartij is, in dit geval de NVWA, en routeert het bericht.
3. Het bericht wordt via een Digikoppeling verzonden naar de integratielaag van NVWA;
4. Het bericht met de elektronische factuur is gebaseerd op een open standaard en wordt daar via een generiek koppelvlak ontvangen;
5. De infrastructurele componenten in de integratielaag routeren het bericht naar een applicatiespecifiek koppelvlak;
6. Dit applicatiespecifieke koppelvlak, in dit geval van een financieel systeem, ontvangt het bericht en verwerkt het binnen de eigen gegevensverzameling.

In het geval van DTV zal alleen communicatie plaatsvinden tussen applicatiecomponenten binnen het NVWA-domein en wordt geen gebruik gemaakt van Digipoort/Digikoppeling.

Communicatie tussen componenten, ongeacht of het een maatwerk of standaard component betreft, is altijd op basis van een leverancier- en technologieneutraal koppelvlak. Deze services draaien altijd op het ESB-platform.

ID	Eis
TA01.4.01 [L]	Maatwerk- en standaard componenten maken gebruik van het ESB-platform

5.1.2.5 Eisen applicatiecomponenten

ID	Eis
TA01.5.01 [L]	Voor de keuze van (applicatie)componenten geldt: hergebruiken voor kopen voor bouwen. Bij hergebruik geldt dat er expliciet, zowel binnen als buiten de EZ-organisatie, wordt gekeken of er een geschikte component beschikbaar is. De keuze dient voor elk component te worden goedgekeurd door de DICTU-

	architecten
TA01.5.02 [L]	Indien een component wordt gerealiseerd met standaard software, dan moet deze software ook gebruikt worden zoals geleverd, zonder aanpassingen aan de code. Aanpassingen aan de code zijn wel toegestaan als gegarandeerd wordt dat deze worden opgenomen in de eerstvolgende officiële release
TA01.5.03 [L]	De configuratie van een component moet zonder aanpassingen kunnen werken na installatie van een nieuwe versie. Dit geldt voor zowel open source als voor standaard componenten
TA01.5.04 [L]	De (herbruikbare) componenten zijn als zelfstandige component te gebruiken en zonder verdere aanpassingen in te zetten voor andere systemen

5.1.2.6 Eisen open source

ID	Eis
TA01.6.01 [L]	Bij voorkeur wordt gebruik gemaakt van open source producten
TA01.6.02 [L]	Bij het ontwikkelen en selecteren van standaard software is men gehouden aan het standaardenregister EZ en de standaarden op de website van het Forum Standaardisatie (http://www.forumstandaardisatie.nl)

5.1.3 Schaalbaarheid en robuustheid

De systemen en componenten binnen de DTV-oplossing moeten schaalbaar zijn (op- en afschakelen) om met de onvoorspelbaarheid van het gebruik van de voorziening om te kunnen gaan.
Om de voorspelbaarheid van de performance van de DTV-oplossing te garanderen is het vereist dat de applicatiecomponenten onafhankelijk van elkaar schaalbaar en ook robuust zijn. Dit wordt bereikt door elk onderdeel als een zelfstandige eenheid ofwel service/dienst te laten functioneren en expliciet rekening te houden met de mogelijkheid dat componenten tijdelijk niet beschikbaar kunnen zijn.

Bij het uitwerken van een schaalbare architectuur moet rekening gehouden worden met de volgende variabelen:

- Schaalbaarheid: Het gaat hier om het aantal gelijktijdige gebruikers, sessies, transacties of operaties dat een systeem als geheel kan uitvoeren;
- Prestaties: Optimaal gebruik maken van beschikbare middelen (resources);
- Reactietijd: Tijd die nodig is om een operatie in de DTV-omgeving uit te voeren;
- Beschikbaarheid: Bepaalt of een applicatie of een deel van een applicatie beschikbaar is;
- Downtime impact: De impact van het niet-beschikbaar zijn van een server, (web)service, component of applicatie. Ook van belang daarbij is het aantal gebruikers of systemen dat hier nadeel van ondervindt en de consequenties ervan;
- Kosten: Welke kosten zijn acceptabel om een schaalbare architectuur te realiseren in verhouding tot de impact van het niet beschikbaar zijn of niet goed presteren van een systeem;
- Beheerbaarheid: Zijn fouten eenvoudig te herleiden en op te lossen door beheer.

Schaalbaarheid
Bij het begrip schaalbaarheid zijn verschillende opties mogelijk:

- Verticaal schalen: Daarbij wordt capaciteit uitgebreid door het toevoegen van geheugen en/of CPU's in een server. Dit wordt geregeld door middel van virtualisatie(software). Het uitbreiden van geheugen en CPU's op een server kent uiteraard grenzen;
- Horizontaal schalen: Daarbij wordt verwerkingscapaciteit uitgebreid door extra servers toe te voegen en een (applicatie)component over verschillende servers te verdelen. Een load balancer zorgt er dan voor dat de aanvragen voor een component over verschillende servers verdeeld worden. Door services en componenten over meerdere servers te verdelen neemt de capaciteit, robuustheid en beschikbaarheid toe;
- Partitioneren: Dan wordt er gekozen voor fysieke scheiding door verschillende componenten op aparte servers te plaatsen. Dan wordt bijvoorbeeld de componenten front-end, backend en database op verschillende servers geplaatst. Hierdoor is het mogelijk een server optimaal te tunen voor de component die er gebruik van maakt.

Schalen kan effectiever en efficiënter toegepast worden als de (applicatie)componenten ontworpen zijn met schaalbaarheid als uitgangspunt. Capaciteit moet dynamisch schaalbaar zijn (op- en afgeschaald kunnen worden) op basis van het werkelijke gebruik.

5.1.4 Eisen (applicatie)componenten

De DTV-oplossing bestaat uit een aantal applicatiecomponenten en deze kunnen uitvallen. De architectuur houdt expliciet rekening met het uitvallen van componenten en kan hiermee omgaan.

ID	Eis
TA01.7.01 [TB]	De componenten binnen de DTV-oplossing maken gebruik van virtualisatie
TA01.7.02 [L]	De DTV-componenten zijn onafhankelijk van elkaar schaalbaar
TA01.7.03 [L]	De DTV-oplossing houdt expliciet rekening met de mogelijkheid dat componenten tijdelijk niet beschikbaar kunnen zijn en kan hiermee omgaan. Dit is het uitgangspunt, maar kan niet altijd afgedwongen worden. Als een component kritisch is voor het proces, dan zal het niet beschikbaar zijn daarvan het proces stoppen. Als dit het geval is moet het proces, nadat de component weer hersteld is, verder gaan vanaf het punt waar het gevorderd was
TA01.7.04 [L]	Componenten zijn onafhankelijk van elkaar en kunnen uitgevoerd worden zonder kennis te hebben van andere componenten
TA01.7.05 [L][TB]	Een component kan over meerdere servers verdeeld worden
TA01.7.06 [L][TB]	Een component kan over meerdere virtuele machines op een enkele server verdeeld worden
TA01.7.07 [L][AB]	Componenten passen caching toe om te voorkomen dat dezelfde gegevens continu opgehaald worden. De caching-periode is door beheer instelbaar

5.1.5 Eisen webservices

ID	Eis
TA.01.8.01 [L]	Asynchrone communicatie wordt toegepast bij alle berichten die niet direct verwerkt hoeven te worden

TA.01.8.02 [L]	Samengestelde services hebben een compensatiemechanisme. Bij een samengestelde service wordt een aantal services gebruikt om de benodigde applicatielogica te realiseren. Bij een compensatiemechanisme kan een service een eerder aangebrachte wijziging zelf terugdraaien

5.1.6 Eisen database

Bij gegevensopslag moet onderscheid gemaakt worden tussen opslag voor mutatie- en opslag voor raadpleegdoeleinden. Hierdoor wordt het mogelijk om de dataopslag te optimaliseren voor de betreffende toepassing o.a. door het partitioneren van gegevens en door middel van geoptimaliseerde indexstructuren. Hiermee kan voorkomen worden dat verschillende soorten gegevensgebruik elkaar beïnvloeden. Het raadplegen van een grote selectie mag bijvoorbeeld geen merkbare gevolgen hebben voor het muteren van gegevens.

ID	Eis
TA.01.9.01 [L]	Er wordt onderscheid gemaakt tussen opslag voor mutatie en opslag voor raadplegen
TA.01.9.02 [L]	Het is mogelijk om datasets verticaal te partitioneren
TA.01.9.03 [L]	De in de gegevenscatalogus per applicatie(component) vastgelegde gegevens-definities en -formaten worden consistent binnen het hele systeem doorgevoerd

5.2 Gegevensopslag

Binnen de DTV-oplossing worden grote hoeveelheden data ontvangen en verwerkt. Gegevensopslag is hierdoor een belangrijk onderdeel en is verantwoordelijk voor het op de juiste manier opslaan en ophalen van gegevens. Het zorgt ook voor plausibiliteits- en consistentiecontroles.

5.2.1 Eisen datastores

Ingevoerde gegevens of berichten zijn gestructureerde gegevens. Er is bij de DTV-oplossing geen sprake van bijv. het gebruik van documenten (ongestructureerde gegevens).

ID	Eis
TA02.1.01 [L]	Gestructureerde gegevens worden in een database opgeslagen
TA02.1.02 [L]	Voor relationele databases wordt gebruik gemaakt van één van de databaseopties: PostgreSQL, SQL-Server of Oracle. Voor de NVWA heeft Oracle de voorkeur
TA02.1.03 [TB]	Databaseservers maken gebruik van een eigen databasestorage op een SAN, waarbij replicatie plaatsvindt (master/slaves). Replicatie kan op applicatieniveau of op databaseniveau opgelost worden op basis van synchrone of asynchrone replicatie
TA02.1.04 [L]	Bij een relationele datastore dient technische en functionele referentiële integriteit tussen records afgedwongen te worden

5.2.2 Eisen exporteren t.b.v rapporteren

BI-tooling biedt de meest efficiënte en onderhoudbare oplossing voor exporteren van gegevens voor rapportages. ETL-tools zijn bewezen oplossingen voor bulk-gegevensuitwisseling.

ID	Eis
TA02.2.01 [L]	Voor het exporteren van gegevens voor rapportages wordt gebruik gemaakt van BI-tooling (Oracle BI of SAS)

5.2.3 Eisen onderhoudbaarheid

ID	Eis
TA02.3.01 [L]	Data moet voldoen aan de Nederlandse standaarden voor getallen en datums
TA02.3.02 [L]	Sleutels ofwel ID's zijn betekenisloos

5.2.4 Eisen Integriteit

Gegevens moeten aantoonbaar origineel en onveranderd zijn.

ID	Eis
TA02.4.01 [L]	De database is alleen toegankelijk voor de bron(applicatie)component, de component die verantwoordelijk is voor het bewerken en opvragen van de gegevens. Het is niet toegestaan om gegevens direct, al of niet handmatig, in de database te manipuleren. Het muteren en opvragen van gegevens wordt altijd via de broncomponent uitgevoerd
TA02.4.02 [L]	Van gegevens wordt de mutatiehistorie bijgehouden. Van elke record is bekend wanneer deze toegevoegd, gewijzigd en verwijderd is en door wie
TA02.4.03 [L]	Gegevens die niet meer gewijzigd mogen worden dienen omgezet te worden naar een archiefwaardig bestandsformaat (zoals XML en PDF) en gearchiveerd te worden. Metadata wordt in het genereren meegenomen (zoals wie, wat en wanneer)
TA02.4.04 [L][AB]	Gegevens worden niet verwijderd maar gemarkeerd als verwijderd. De DTV-oplossing biedt opschoonfunctionaliteit om gegevens na een bepaalde periode permanent uit de database te kunnen verwijderen met behoud van consistentie. De criteria hiervoor zijn door beheer instelbaar. Voor gearchiveerde gegevens gelden bij het opschonen de archiefeisen

5.2.5 Eisen continuïteit

Gegevens mogen niet verloren gaan.

ID	Eis
TA02.5.01 [L]	Bij (her)installatie van (een deel van) het systeem of een applicatiecomponent mogen geen gegevens verloren gaan

5.2.6 Eisen back-up

ID	Eis
TA02.6.01 [TB][AB]	Er wordt gebruik gemaakt van de standaard back-up functionaliteit en -processen van DICTU

5.3 Netwerk

De netwerkinfrastructuur van DICTU is onderverdeeld in verschillende zones (compartimenten) bestaande uit een onvertrouwd deel (OV), Demilitarized Zone (DMZ)/semivertrouwd deel (SV) en (zeer) vertrouwde delen ((Z)V).

Bij communicatie van en naar andere overheidsorganisaties wordt gebruik gemaakt van het Diginetwerk. Diginetwerk is een besloten overheidsnetwerk (VPN) dat verschillende fysieke overheidsnetwerken verbindt, zoals GEMnet, SURFnet, Haagse Ring, Suwinet, etc. De communicatie over Diginetwerk is niet afgeschermd. Om te zorgen dat de communicatie afgeschermd is moet het transport tussen domeinen beveiligd worden.
Bij communicatie tussen een webbrowser in de zone onvertrouwd (bijv. openbaar Internet) en de DTV-oplossing wordt eenzijdige SSL toegepast. Bij berichtenverkeer met bedrijven of andere overheden wordt normaal gesproken tweezijdige SSL toegepast. Dit laatste is niet het geval bij de DTV-oplossing.

5.3.1.1 Eisen koppelvlak

ID	Eis
TA03.1.01 [TB]	De DTV-oplossing maakt gebruik van een centraal/standaard koppelvlak voor het openbare Internet
TA03.1.02 [TB]	Directe toegang tot applicaties en databases is op netwerkniveau afgeschermd

5.3.1.2 Eisen compartimentering

ID	Eis
TA03.2.01 [TB]	De DTV-oplossing dient te voldoen aan de compartimenteringseisen zoals beschreven in paragraaf 6.5 Compartimentering

6 Beveiliging en privacy

In dit hoofdstuk wordt ingegaan op beveiliging en privacy als pijlers voor een betrouwbare dienstverlening. Betrouwbaarheid is in dit verband het inbouwen van mechanismen die bescherming van informatie tot doel hebben.

6.1 Beveiligingsclassificatie

Voor alle DICTU-omgevingen geldt dat voldaan dient te worden aan het BIR (Baseline Informatiebeveiliging Rijksoverheid). De vertaling hiervan in kaders en richtlijnen van de informatiebeveiligingsarchitectuur moet zorgen voor een effectieve, efficiënte, kwalitatieve en betrouwbare beveiliging van gegevens. Hiervoor worden twee wegen bewandeld:
1. Overeenstemming met onderstaande normenkaders, wet- en regelgeving;
2. Een integrale benadering van informatiebeveiliging waarbij IB vanaf het begin van het project geïntegreerd wordt in de architecturen en ontwerpen.

Kaderstellend voor de informatiebeveiliging voor het project DTV zijn naast het genoemde BIR de volgende zaken:
- ISO27001 en ISO27002 (zijn ook overgenomen in het bovengenoemde BIR);
- WBP (Wet Bescherming Persoonsgegevens);

(http:// http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/vraag-en-antwoord/wat-regelt-de-wet-bescherming-persoonsgegevens-wbp.html)
- Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIR-BI);

(http://nl.wikipedia.org/wiki/Voorschrift_Informatiebeveiliging_Rijksdienst)
- AKI – Algemeen Kader Informatiebeveiliging;
- Richtlijn Webservices van het Nationaal Cyber Security Centrum (NCSC);
- Nederlandse Overheid Referentiearchitectuur (NORA) (3.0)-dossier Informatiebeveiliging.

(http://www.e-overheid.nl/images/stories/nieuws_2010/arch_aanpaknoradossier_informatiebeveiliging.pdf)

Voor de beveiligingsclassificatie wordt gebruik gemaakt van de zogenaamde BIV-classificatie:
- Beschikbaarheid: Hoe vaak en wanneer een component toegankelijk is en kan worden gebruikt;
- Integriteit: Het in overeenstemming zijn van informatie met het afgebeelde deel van de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). Het gaat hier om de integriteit van gegevens waarop en waarmee een component werkt;
- Vertrouwelijkheid: Het beperken van de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie tot een gedefinieerde groep van gerechtigden.

In het VIR-BI wordt daarnaast voor 4 categorieën van informatie extra eisen gesteld. Het betreft de volgende beveiligingsniveaus:

1. Departementaal Vertrouwelijk;
2. Staatsgeheim Confidentieel;
3. Staatsgeheim Geheim;
4. Staatsgeheim Zeer geheim.

Het VIR-BI legt per beveiligingsniveau beveiligingseisen op aan de beheerder van vertrouwelijke informatie.

Voor de DTV-oplossing, die gebaseerd is op een SLA Basis 24, leidt dit tot de beveiligingsclassificaties volgens onderstaand overzicht:

- **Beschikbaarheid (en oplostijden):** De beschikbaarheidseis voor de gehele omgeving wordt als maximaal 'Basis 24' geclassificeerd.
  De beschikbaarheid voor de DTV-oplossing, op basis van een Service Level Agreement Basis 24, betekent [5]:
  - Een openstelling van de dienst 7 x 24 uur en 98% beschikbaarheid;
  - Het lijkt op het eerste gezicht dat een openstelling van de helpdesk gedurende werkdagen (08:00-18:00) voldoet;
  - Oplossingstijd max. 2 dagen.
- **Integriteit:** de integriteit van de informatie die getransporteerd wordt in de DTV-omgeving als 'Geborgd' geclassificeerd.
- **Vertrouwelijkheid**: de vertrouwelijkheid van informatie binnen de DTV-oplossing wordt als maximaal 'Departementaal Vertrouwelijk' geclassificeerd.
- **WBP:** informatie die door middel van de applicatie(componenten) wordt verwerkt/ beschikbaar gesteld wordt, wordt gezien als maximaal 'risicoklasse 1 (basis)'.

In tabelvorm komen we daarmee op het volgende overzicht:

Niveau IB	Beschikbaarheid	Integriteit	Vertrouwelijkheid	WBP
	Basis24+	**Onweerlegbaar**	**STG Confidentieel**	**3, hoog risico**
	Basis24	**Geborgd**	**DV**	**2. verhoogd risico**
	Basis		**Intern**	**1. basis**
		Standaard	**Openbaar**	**0. openbaar**

6.1.1 Eisen

ID	Eis
BV01.1.01 [L]	Gegevens zijn voorzien van een beveiligingsclassificatie op basis van de VIR-BI en de Wet bescherming persoonsgegevens (WBP). De persoonsgegevens in DTV zijn geclassificeerd binnen risicoklasse 1 van de WBP. Informatie wordt daarom versleuteld getransporteerd en is alleen toegankelijk voor geautoriseerde gebruikers
BV01.1.02 [L]	Gevoelige gegevens worden versleuteld als ze worden getransporteerd over het netwerk. Bij communicatie tussen een webbrowser en de DTV-oplossing wordt eenzijdige SSL toegepast. Bij berichtenverkeer met bedrijven en overheden wordt tweezijdige SSL toegepast
BV01.1.03 [CA]	De zender en ontvanger van gegevens authenticeren elkaar voordat gevoelige gegevens worden uitgewisseld
BV01.1.04 [L]	Gebruikersnamen, wachtwoorden of beveiligingssleutels worden versleuteld opgeslagen en uitgewisseld
BV01.1.05 [L]	Bij het gebruik van productiedata in een testsysteem mogen personen en organisaties niet herleidbaar zijn

6.2 Identity & Access Management (IAM)

Beveiliging is een belangrijk aspect. Vanuit onderhoudbaarheid en consistentie wordt dit op één plek en éénmalig gedefinieerd. Beveiliging mag niet afhankelijk zijn van de discipline van ontwikkelaars. Applicaties en beveiliging zijn daarom ontkoppeld.

6.2.1 Eisen identificatie en authenticatie

In het geval van DTV is er geen berichtenverkeer met bedrijven of andere overheden en wordt bij het gebruik van een webbrowser vanuit een onbeveiligde Internetzone eenzijdige SSL toegepast. De server moet zich door middel van een PKIoverheid (PKI-O) certificaat identificeren. Autorisatie wordt gedaan door te controleren of de combinatie OIN uit het PKI-O-certificaat en het eindpunt geautoriseerd is.

ID	Eis
BV02.1.01 [TB][IB]	Voor identificatie en authenticatie bij berichtuitwisseling wordt gebruik gemaakt van PKIoverheid-certificaten
BV02.1.02 [TB][IB]	Bij authenticatie wordt gebruik gemaakt van Single Sign On (SSO)
BV02.1.03 [TB][IB]	Er is een herbruikbare beveiligingscomponent t.b.v. authenticatie en autorisatie. Alle toegang tot applicaties verloopt via deze beveiligingscomponent. Applicaties voeren zelf geen authenticatie en autorisatie uit maar delegeren dit naar de beveiligingscomponent. De standaard IAM-oplossing is Oracle AM

6.2.2 Eisen autorisatie

Ontkoppeling van applicatie en beveiliging zorgt ervoor dat autorisatie eenduidig en op de juiste manier wordt afgedwongen ongeacht de ingang, het interactiekanaal of (architectuur)laag.

ID	Eis
BV02.2.01 [L]	Toegang tot vertrouwelijke gegevens is geautoriseerd. Beveiligingsfunctionaliteit is niet hard gecodeerd in programmacode. Er wordt gebruik gemaakt van een identity omgeving/server voor het vastleggen van autorisatie policies en het afdwingen hiervan
BV02.2.02 [L]	Autorisaties worden bijvoorbeeld op basis van RBAC opgevraagd van de identity omgeving

6.3 Toegang

6.3.1 Eisen

ID	Eis
BV03.1.01 [L]	(Applicatie)componenten voeren altijd een authenticatie- en autorisatiecheck uit van gebruikers, systemen of componenten die toegang willen krijgen tot functionaliteiten of gegevens
BV03.1.02 [L]	Autorisaties worden geregeld op basis van rollen en niet op basis van personen. Een gebruiker heeft één of meerdere rollen
BV03.1.03 [L]	De DTV-oplossing moet voldoen aan de eisen uit de Baseline Informatiebeveiliging Rijksoverheid (BIR)

6.4 Monitoring, auditing en alerting

Monitoring omvat het vastleggen van gebeurtenissen en bijbehorende informatie van acties die authenticatie en autorisatie vereisen. Bijvoorbeeld wie wanneer heeft ingelogd en het operationeel monitoren en waarschuwen op basis van indicatoren. Monitoring is zowel van belang voor de operationele veiligheid als voor het voldoen aan wet- en regelgeving en de controle daarvan achteraf, bijvoorbeeld via audits.

Om fouten op te sporen en om achteraf te kunnen zien of er ongeoorloofd gebruik van de informatie heeft plaatsgevonden wordt auditinformatie bijgehouden. Hiermee is na te gaan wie, wanneer, wat heeft gedaan.

6.4.1 Eisen

Vanuit integriteits- en beveiligingsperspectief is het niet gewenst dat berichten buiten de bron worden gemanipuleerd. Dan kan namelijk de herleidbaarheid van handelingen en de betrouwbaarheid van de communicatie niet worden gegarandeerd. Het introduceert het risico dat bijv. beheerders het berichtenverkeer manipuleren. Daarnaast worden gegevens gecommuniceerd die niet (meer) consistent zijn met de bron.

Hetzelfde geldt voor gegevens. Als deze buiten de bron worden gemanipuleerd, kan de herleidbaarheid van handelingen, en de betrouwbaarheid en consistentie van de gegevens niet worden gegarandeerd.

ID	Eis
BV04.1.01 [L]	Alle handelingen van systemen, (applicatie)componenten en gebruikers zijn traceerbaar en reproduceerbaar
BV04.1.02 [L]	Berichten worden niet handmatig aangemaakt, gewijzigd of verwijderd buiten de bron. Applicatiecomponenten moeten functionaliteit bieden om berichten indien nodig opnieuw aan te kunnen bieden
BV04.1.03 [FB/AB/TB]	Gegevens in databases worden niet handmatig aangemaakt, gewijzigd of verwijderd buiten de bron
BV04.1.04 [L]	Alle gebeurtenissen in het netwerk, op het DTV-platform en binnen applicaties, die authenticatie en autorisatie vergen, worden vastgelegd in een auditlog. Uitgevoerde handelingen zijn herleidbaar tot op initiërend organisatie-, persoons- of systeemniveau
BV04.1.05 [TB]	Voor de auditlog wordt bij voorkeur gebruik gemaakt van een auditing component die niet door reguliere beheerders te wijzigen is. Zodoende is de integriteit van de auditinformatie gewaarborgd
BV04.1.06 [TB]	Auditinformatie wordt na een bepaalde periode automatisch verwijderd. De duur van deze periode is instelbaar

6.5 Compartimentering

Er wordt, zoals in H-5 al is aangegeven, netwerkcompartimentering toegepast. Tussen de verschillende compartimenten wordt alleen de noodzakelijke communicatie toegestaan. Het compromitteren van een server of een applicatie(component) heeft hierdoor geen directe gevolgen voor componenten in andere compartimenten.

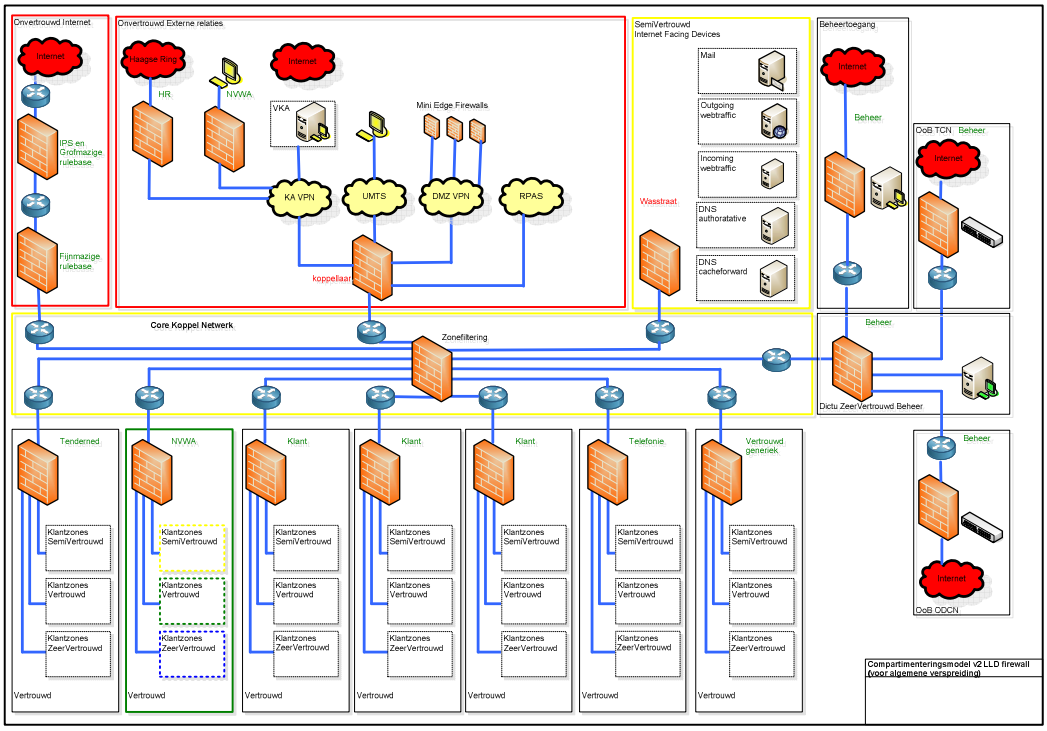
Door de gelaagde opbouw van applicaties (bijv. een front-end, koppelingen/koppelvlakken, een backend (ontsloten via webservices), én gegevens) is compartimentering mogelijk. Het beveiligingsniveau neemt per laag toe door de

communicatie tussen de lagen te beperken tot alleen de aangrenzende laag. De interactielaag/front-end communiceert met de servicelaag (koppelingen/koppelvlakken), de servicelaag met de applicatielaag/backend (ontsloten via webservices) en de backend met de gegevenslaag.

Binnen het DICTU-compartimenteringsmodel worden daarvoor de volgende compartimenten onderscheiden:

- Onvertrouwde rode zone: interactielaag/front-end;
- Semi-vertrouwde gele zone (SV/DMZ): koppelvlakken en (vaak afhankelijk van het soort applicatiecomponent) ook de backends;
- Vertrouwde groene zone: gegevenslaag/backend-gegevens/databases;
- Zeer vertrouwde blauwe zone: beheercomponenten die gebruik maken van de databases in de groene zone.

Als een front-end via internet toegankelijk is, dan staat deze altijd in de rode zone. In onderstaande plaat staat het (geanonimiseerde) compartimenteringsmodel met de verschillende zones afgebeeld. Daarin is het klantcompartiment van de NVWA afgebeeld met een eigen gele, groene en blauwe zone.
Deze plaat staat groter afgebeeld in de bijlage.



Figuur 9. Compartimenteringsmodel met NVWA-klantzone

6.5.1 *Eisen compartimentering*

ID	Eis
BV06.1.01 [L]	De DTV-oplossing kent een gelaagde opbouw en ondersteunt hiermee de voorgeschreven compartimentering

6.5.2 Eisen patchen en updates

Een goed functionerend updatemechanisme is van groot belang om voldoende beschermd te zijn tegen bekende beveiligingsproblemen in software. Naast een technische implementatie van een dergelijk mechanisme is het ook van belang een goede procedure in te richten waarin beschreven staat hoe om te gaan met updates: hoe snel de organisatie een kritieke patch implementeert, welke procedure de patch moet doorlopen en wie de verantwoordelijkheid draagt.

ID	Eis
BV06.1.01 [AB/TB]	Beheer is verantwoordelijk voor het monitoren van security waarschuwingen en patches op de beheerde software, componenten en libraries
BV06.1.02 [AB/TB]	Een security patch dient binnen 30 dagen na beschikbaar komen door beheer te zijn getest en beschikbaar te worden gesteld als nieuwe release
BV06.1.03 [L]	Applicaties/applicatiecomponenten moeten voldoen aan de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC)

7 Beheer

In dit hoofdstuk wordt ingegaan op beheer als een van de pijlers van een betrouwbare serviceverlening.

Voor DICTU is beheer een zeer belangrijk aspect bij het realiseren van systemen en applicaties. Er dient veel aandacht besteed te worden aan het realiseren van een beheerbare en beheersbare DTV-oplossing.

7.1 Formalisering afspraken

De DTV-oplossing maakt gebruik van een aantal componenten. Afhankelijkheden worden daarbij beperkt door bij de communicatie met deze componenten gebruik te maken van gestandaardiseerd product- en technologieneutrale koppelvlakken. Hierdoor kunnen componenten onafhankelijk van afnemers doorontwikkelen door bijvoorbeeld een nieuw koppelvlak aan te bieden. Afnemers moeten dan binnen een af te spreken periode migreren naar dit nieuwe koppelvlak.
Om het geheel beheersbaar en beheerbaar te houden, dient voor alle betrokken partijen helder te zijn hoe het beheer van de DTV-componenten belegd is en wie waarvoor verantwoordelijk is.

7.1.1 Eisen

ID	Eis
BH01.1.01 [SM]	Het beheer van de DTV-oplossing is duidelijk belegd en geborgd in een DAP en in SLA's
BH01.1.02 [SM]	De SLA en de Quality of Service (QoS) van de componenten en services zijn gedefinieerd en geborgd
BH01.1.03 [L]	De componenten binnen de oplossing kennen een eigen ontwikkel- en releasecyclus en een eigen, goed gedefinieerd, leverancier- en technologie-neutraal koppelvlak
BH01.1.04 [SM/FB/AB/TB]	Voorgaande versies van een koppelvlak worden gedurende een af te spreken periode ondersteund, na het beschikbaar komen van een nieuwe versie van het koppelvlak. Afnemers van services van zo'n (herbruikbare) component bepalen zelf het moment waarop ze binnen deze periode migreren naar een nieuwe versie
BH01.1.05 [L]	De DTV-oplossing en haar (applicatie)componenten zijn overdraagbaar. Een andere partij moet met minimale inspanning een component over kunnen nemen

7.2 Zelfbediening

Om de beheerlast te beperken en te zorgen dat de NVWA-organisatie, gebruiker van de DTV-oplossing, snel en adequaat wijzigingen kan doorvoeren in de omgeving, wordt gestreefd naar maximale zelfbediening. Daarmee is de NVWA zelf 'in control' en worden de afhankelijkheden beperkt.

7.2.1 Eisen

ID	Eis
BH02.1.01 [L]	De NVWA heeft eigen beheeraccounts waarmee zij bepaalde organisatiespecifieke zaken zelf kunnen inrichten, zoals toekennen van rollen aan gebruikers, koppelen van services, wachtwoorden resetten etc.

7.3 Lifecycle management

7.3.1 Eisen

ID	Eis
BH03.1.01 [SM]	Voor elke omgeving (OTAP) dient een goed gedefinieerd acceptatieproces te bestaan. Daarin is o.a. beschreven welke documenten aanwezig moeten zijn, waar documenten aan moeten voldoen, wie akkoord geeft om door te gaan naar de volgende omgeving etc.
BH03.1.02 [SM]	Om het ontwikkel- en releaseproces te ondersteunen en te allen tijde over betrouwbare en beheersbare systemen te beschikken, wordt het OTAP-principe toegepast
BH03.1.03 [SM]	OTAP-omgevingen zijn gescheiden. Een release of change doorloopt altijd alle omgevingen voordat deze in productie gaat. Verantwoordelijkheid voor acceptatie en goedkeuring voor de overgang naar de volgende omgeving is per omgeving gescheiden
BH03.1.04 [L]	Software en configuratie zijn gescheiden. De applicatiecomponenten zijn parametriseerbaar en bevatten geen hard gecodeerde verwijzingen

7.4 Zelfbeheer en samenwerking in de beheerketen

Beheerders krijgen notificaties bij verstoringen van componenten of bij overschrijding van drempelwaarden van responsetijden.

7.4.1 Eisen

ID	Eis
BH04.1.01 [SM/FB/AB/TB]	Componenten loggen naar een centrale logging-component. Deze component biedt een (bij voorkeur) webgebaseerde UI die toegang geeft tot de logging-data en maakt deze doorzoekbaar. Logging-data stelt beheerders in staat om zelfstandig de oorzaak van problemen te herleiden
BH04.1.02 [SM/FB/AB/TB]	Van een component is bekend op welke aspecten de monitoring dient plaats te vinden, zodat de monitoringtool hierop ingericht kan worden
BH04.1.03 [SM/FB/AB/TB]	Beheerders worden genotificeerd bij verstoringen van componenten of bij overschrijding van drempelwaarden van responsetijden.

7.5 Service levels

In H-6 is al aangegeven dat de DTV-oplossing voldoet aan een SLA-niveau Basis 24. De precieze componenten van dit serviceniveau staan beschreven in de Generieke SLA DICTU [5].

7.6 Rapportages

Er wordt over de kwaliteit van de dienstverlening gerapporteerd. Dit betekent dat er gemonitord en gerapporteerd wordt over hoe de verschillende DTV-onderdelen presteren.

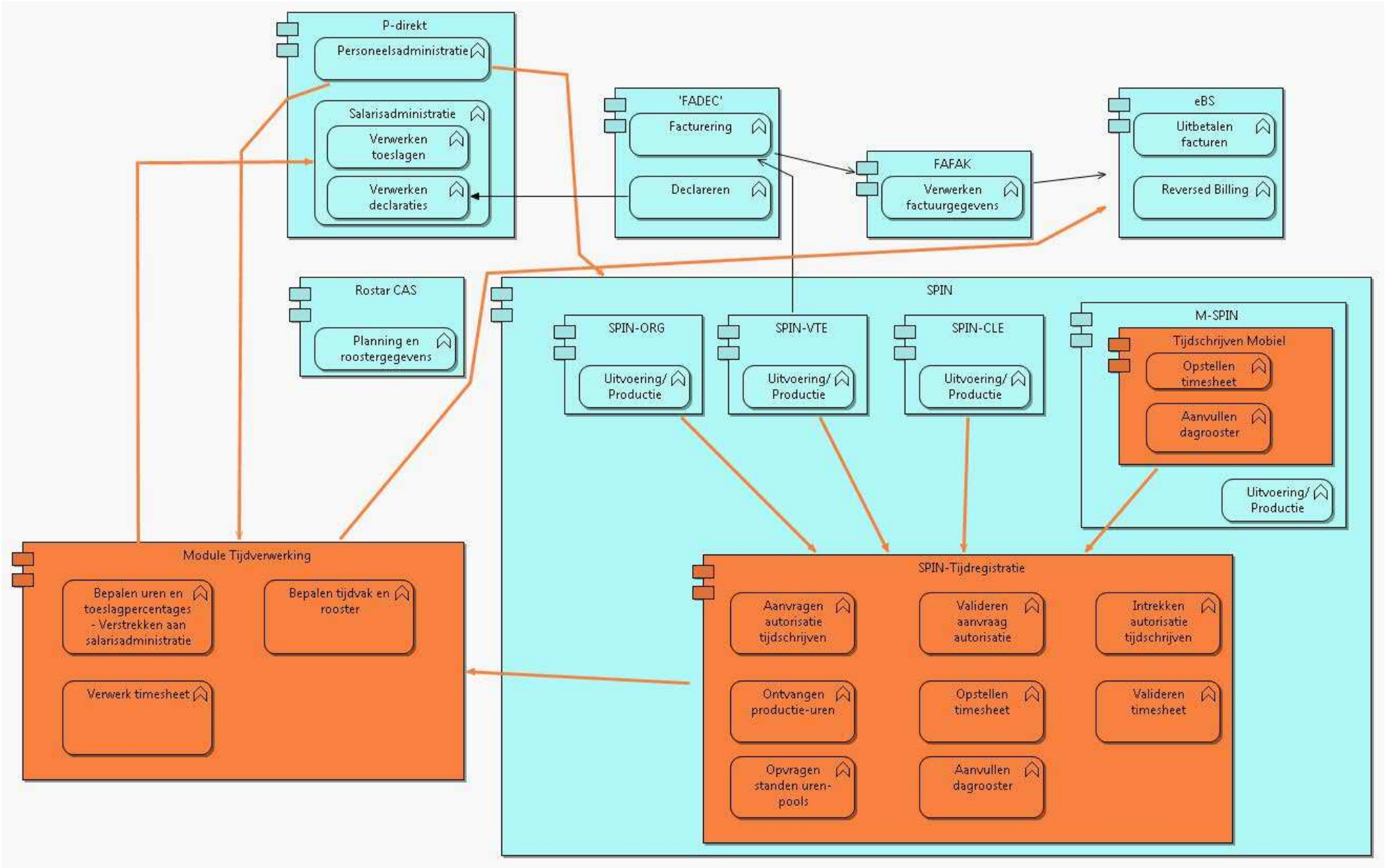
7.6.1 Eisen

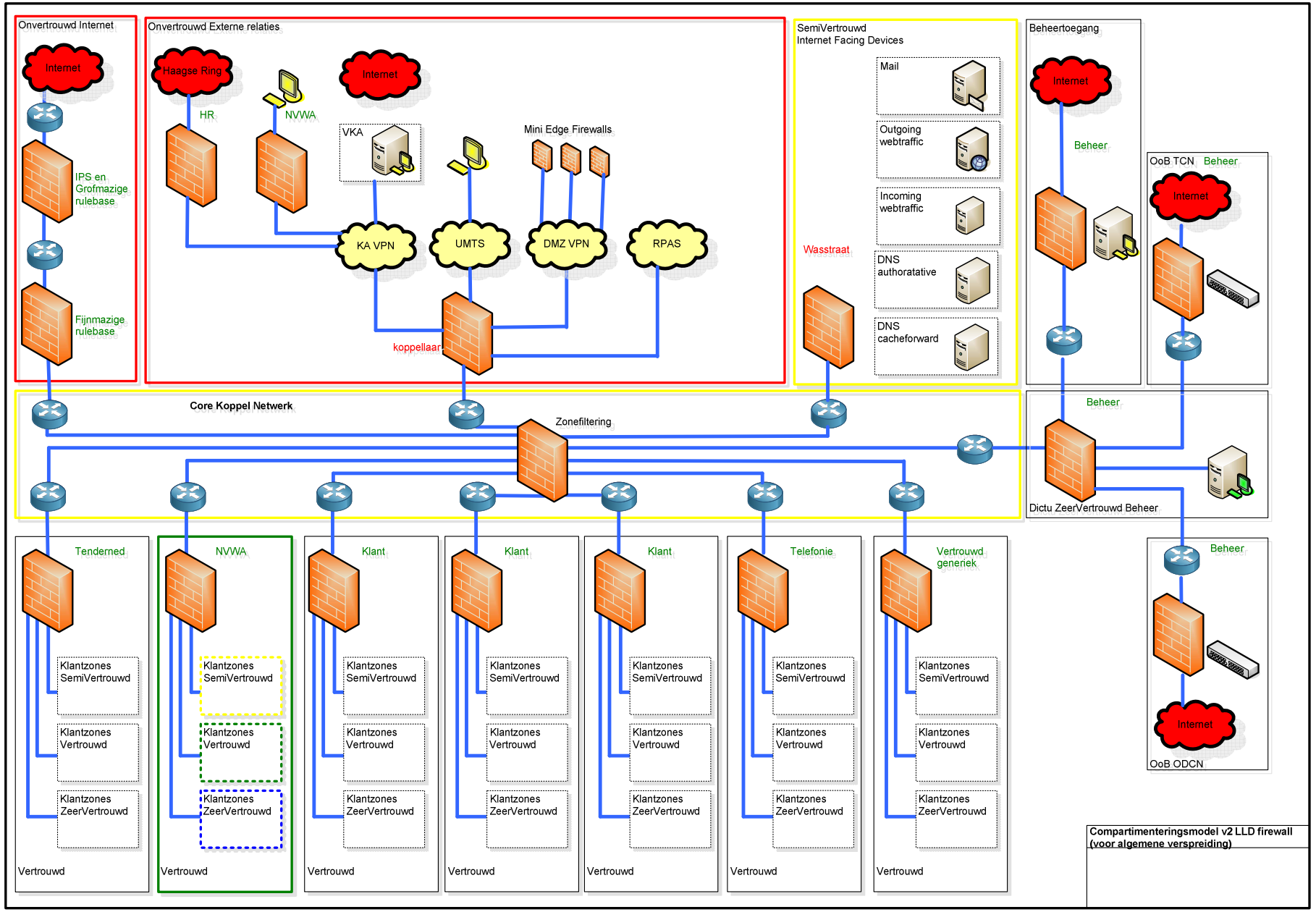
ID	Eis
BH05.1.01 [SM]	Voor het rapporteren wordt aangesloten op de monitorings- en rapportage-functionaliteit van DICTU
BH05.1.02 [SM]	Er wordt conform de in de SLA en DAP afgesproken termijnen gerapporteerd over het genoemde service level
BH05.1.03 [SM]	Er wordt gerapporteerd over de beschikbare capaciteit en de belasting hiervan
BH05.1.04 [TB]	Er wordt gerapporteerd over incidenten

7.6.2 Eisen testen en accepteren

Het testen en accepteren van wijzigingen wordt releasematig aangepakt volgens een gestructureerde methodiek. Een load- en stresstest toont aan dat applicatiecomponenten voldoen aan de afgesproken prestatie-eisen en dat zij schaalbaar en robuust zijn.

ID	Eis
BH06.1.01 [KB]	Elke release van een applicatiecomponent wordt opgeleverd met testscripts om de UI en de webservices functioneel te kunnen testen. Deze tests worden gebruikt om een regressietest uit te voeren
BH06.1.02 [KB]	Elke release van een applicatiecomponent wordt opgeleverd inclusief source code. Alleen als de source code door de controles komt wordt een release geaccepteerd
BH06.1.03 [KB]	Afhankelijk van de grootte of impact van een release behoort een load- en stresstest tot het acceptatieproces om van de acceptatie- naar de productieomgeving te kunnen gaan
BH06.1.04 [KB]	Elke release van een applicatiecomponent wordt opgeleverd met alle documenten die nodig zijn om de release in beheer te kunnen nemen en te zorgen dat deze overdraagbaar/opnieuw implementeerbaar is


P-direkt
Personeelsadministratie
Salarisadministratie
Verwerken toeslagen
Verwerken declaraties
'FADEC'
Facturering
Declareren
FAFAK
Verwerken factuurgegevens
eBS
Uitbetalen facturen
Reversed Billing
Rostar CAS
Planning en roostergegevens
SPIN
SPIN-ORG
Uitvoering/ Productie
SPIN-VTE
Uitvoering/ Productie
SPIN-CLE
Uitvoering/ Productie
M-SPIN
Tijdschrijven Mobiel
Opstellen timesheet
Aanvullen dagrooster
Uitvoering/ Productie
Module Tijdverwerking
Bepalen uren en toeslagpercentages - Verstrekken aan salarisadministratie
Bepalen tijdvak en rooster
Verwerk timesheet
SPIN-Tijdregistratie
Aanvragen autorisatie tijdschrijven
Valideren aanvraag autorisatie
Intrekken autorisatie tijdschrijven
Ontvangen productie-uren
Opstellen timesheet
Valideren timesheet
Opvragen standen uren-pools
Aanvullen dagrooster


Onvertrouwd Internet
Internet
IPS en Grofmazige rulebase
Fijnmazige rulebase
Onvertrouwd Externe relaties
Haagse Ring
HR
NVWA
Internet
VKA
Mini Edge Firewalls
KA VPN
UMTS
DMZ VPN
RPAS
koppellaar
SemiVertrouwd
Internet Facing Devices
Mail
Outgoing webtraffic
Incoming webtraffic
DNS authoratative
DNS cacheforward
Wasstraat
Beheertoegang
Internet
Beheer
OoB TCN
Beheer
Internet
Core Koppel Netwerk
Zonefiltering
Beheer
Dictu ZeerVertrouwd Beheer
Beheer
Internet
OoB ODCN
Tenderned
NVWA
Klant
Klant
Klant
Telefonie
Vertrouwd generiek
Klantzones SemiVertrouwd
Klantzones Vertrouwd
Klantzones ZeerVertrouwd
Vertrouwd
Compartimenteringsmodel v2 LLD firewall (voor algemene verspreiding)