



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Assurance-rapport en Verantwoording 2010

Digipoort (koppelvlakken SMTP, X.400, FTP en POP3)

Datum 30 juni 2011
Status Concept

Colofon

Projectnaam	Assurance-rapport en Verantwoording 2010
Versienummer	1 0
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 servicecentrum@logius.nl
Bijlage(n)	Lijst met afkortingen Beheersdoelstellingen
Auteurs	Verantwoording: Logius Assurance-rapport: Rijksauditedienst

Woord vooraf

Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), verantwoordelijk voor het beheer en de verdere ontwikkeling van een aantal overheidsbrede ICT-producten, bestaat vijf jaar! Met het enthousiasme van een jonge organisatie biedt Logius al vijf jaar professionele dienstverlening. Een groeiend aantal klanten binnen en buiten de Rijksoverheid maakt gebruik van deze producten. Deze klanten zijn voor hun bedrijfsvoering afhankelijk van de betrouwbaarheid van de producten van Logius. Dat Logius kwaliteit hoog in het vaandel heeft staan, laten we zien door jaarlijkse afgifte van een Assurance-rapport en Verantwoording over onze belangrijkste producten. Het Assurance-rapport en de Verantwoording over DigiD voor Burgers en Haagse Ring (onderdeel van Diginetwerk) zijn gepubliceerd op 17 mei jl.

Het Assurance-rapport en de Verantwoording die voor u liggen, hebben betrekking op de opzet, het bestaan en de werking van Digipoort met de koppelvlakken SMTP, X.400, FTP en POP3 in de periode 1 januari 2010 tot en met 31 december 2010. De Verantwoording is mede gebaseerd op de uitkomsten van onderzoeken die door de Rijksauditdienst (RAD) zijn uitgevoerd.

Het Assurance-rapport en de Verantwoording zijn niet alleen een waarborg voor klanten, maar ook een interne drijfveer om onze dienstverlening steeds verder te professionaliseren. Logius is volop in ontwikkeling. Om blijvend te kunnen voldoen aan de wensen en eisen van klanten, opdrachtgevers en eigenaar, wordt gewerkt aan (door-)ontwikkeling van producten en herinrichting van de organisatie. In 2010 is de nieuwe Digipoort applicatie in gebruik genomen. Het realiseren van de aanbevelingen die voortkomen uit de onderzoeken van de RAD is inmiddels in gang gezet. Middels dit Assurance-rapport en deze Verantwoording toont Logius aan dat u kunt blijven vertrouwen op onze dienstverlening.

Op naar het volgende lustrum elektronische dienstverlening!

Met vriendelijke groet,



Steven Luitjens
Directeur Logius



Assurance-rapport

Geadresseerde

Dit Assurance-rapport is bestemd voor de huidige en potentiële afnemers van Digipoort op de koppelvlakken SMTP, X.400, FTP en POP3 (hierna: Digipoort). Het rapport dient uitsluitend in samenhang met de Verantwoording over de periode 1 januari tot en met 31 december 2010 over Digipoort te worden verstrekt en heeft als doelstelling aanvullende zekerheid te geven over de juistheid en volledigheid van deze Verantwoording.

Opdracht

Ingevolge de opdracht van 5 juli 2007 met kenmerk 2007-238442 en de aanvullende opdracht van 1 september 2010 met kenmerk RAD/2010/679M hebben wij de Verantwoording van Logius van 20 juni 2011, waarin de in de periode 1 januari tot en met 31 december 2010 beoogde en geïmplementeerde maatregelen en procedures bij Logius en de betrokken leverancier zijn opgenomen ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van Digipoort beoordeeld.

Reikwijdte en gehanteerde normen

In dit kader verstaan wij onder de voornoemde kwaliteitsaspecten:

- beschikbaarheid: de mate waarin een object conform afspraken beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben;
- integriteit: de mate waarin de verwerking van de ingevoerde gegevens juist, volledig en tijdig verloopt en de programma's en bestanden ongeschonden blijven;
- exclusiviteit: de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen;
- controleerbaarheid: de mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is om vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.

Bij deze opdracht zijn wij uitgegaan van de door Logius vastgestelde beheerdoelstellingen en normen (op te vragen bij Logius). Deze sluiten aan op algemeen aanvaarde uitgangspunten en op het contract tussen Logius en haar leverancier van Digipoort. De normen zijn voldoende concreet en volledig om uitgaande hiervan de inhoud van de Verantwoording te kunnen onderzoeken.

Verantwoordelijkheden en werkzaamheden

De Verantwoording is opgesteld onder verantwoordelijkheid van de directeur van Logius. Het is onze verantwoordelijkheid om door middel van een onderzoek op onafhankelijke wijze een oordeel over deze Verantwoording te geven. Daartoe hebben wij werkzaamheden uitgevoerd die in overeenstemming zijn met de Nederlandse richtlijnen voor assurance-opdrachten en die gericht zijn op het signaleren van materiële afwijkingen en het verkrijgen van een redelijke mate van zekerheid.

Onze belangrijkste werkzaamheden waren:

- het verkrijgen van inzicht in relevante kenmerken van Logius en haar leverancier;
- review van de werkzaamheden, dossier en rapportage van de externe auditor van de leverancier, gericht op het beoordelen van de opzet en op het vaststellen van het bestaan en de werking van de relevante maatregelen en procedures bij de externe leverancier;
- het beoordelen van de opzet en het vaststellen van het bestaan en de werking van de relevante maatregelen en procedures bij Logius;
- het onderzoeken van de juistheid en volledigheid van de informatie in de Verantwoording, mede gelet op de informatiebehoeften van de huidige en potentiële gebruikers van Digipoort;
- het evalueren van het algehele beeld van de Verantwoording, inclusief het beoordelen van de consistentie van de informatie, aan de hand van de bovengenoemde beheerdoelstellingen c.q. normen.

Oordeel


Op grond van ons onderzoek zijn wij van oordeel dat de in de verantwoording van Logius opgenomen informatie over de maatregelen en procedures ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van Digipoort bij Logius en haar leverancier betreffende het tijdvak 1 januari 2010 tot en met 31 december 2010 juist en volledig is.

Toelichting op het oordeel

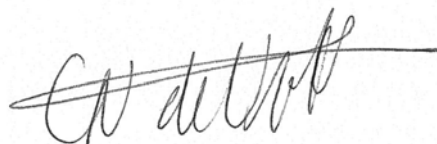
Digipoort is één van de bouwstenen voor de realisatie van betrouwbare digitale diensten. Organisaties dienen zich ervan bewust te zijn dat het toepassen van één of meerdere bouwstenen niet voldoende is om een betrouwbare digitale dienst te realiseren. Hiervoor dient de betreffende organisatie een analyse uit te voeren van de beveiligingseisen die samenhangen met het karakter van de eigen digitale dienstverlening. Vervolgens dient de organisatie vast te stellen dat de in de digitale dienstverlening gebruikte componenten gezamenlijk toereikend invulling geven aan de beveiligingseisen. Voor Digipoort kan hiervoor gebruik worden gemaakt van de informatie van Logius, waaronder de informatie die in deze Verantwoording is opgenomen.

Ondanks dat ons oordeel zich positief uitspreekt over de juistheid en volledigheid van deze Verantwoording, wijzen wij de lezer erop dat gedurende de verantwoordingsperiode op onderdelen niet voldoende invulling is gegeven aan de afgesproken normen voor Digipoort. Voor nadere informatie verwijzen wij naar paragraaf 3.4 van de Verantwoording.

Den Haag, 30 juni 2011
Rijksauditedienst

A handwritten signature in black ink, consisting of a large, stylized initial 'J' followed by a long, horizontal, wavy line that ends in a small hook.

mr. drs. J. Roodnat RE RA
Clustermanager RAD

A handwritten signature in black ink, featuring a large, stylized initial 'C' followed by the letters 'N de Vette' in a cursive script, ending with a long horizontal line.

mw. drs. C.N. de Vette RE
Senior Auditor

Inhoud

1	Managementsamenvatting	2
2	Inleiding.....	4
2.1	Algemeen.....	4
2.2	Normstelling	4
2.3	Totstandkoming van de Verantwoording.....	4
2.4	Leeswijzer.....	5
3	Bevindingen Digipoort.....	6
3.1	Algemeen.....	6
3.2	Tactisch beheer	6
3.3	Operationeel beheer.....	9
3.3.1	Context.....	9
3.3.2	Bevindingen Servicecentrum Logius	9
3.3.3	Bevindingen externe leverancier Digipoort	9
3.3.4	Belangrijkste bevindingen (over de periode 1 juni 2010 – 31 december 2010)	10
3.4	Conclusie.....	12
	Bijlage I Lijst met afkortingen.....	13
	Bijlage II Beheersdoelstellingen.....	14

1 Managementsamenvatting

Algemeen

Logius is verantwoordelijk voor het beheer en de verdere (door)ontwikkeling van het product Digipoort. Voor de klanten binnen de overheid en gelieerde organisaties is het betrouwbaar en veilig functioneren van dit product van groot belang in hun keten van dienstverlening aan burgers en bedrijven. Met deze Verantwoording inclusief Assurance-rapport geeft Logius aanvullende zekerheid aan haar klanten over de kwaliteit van één van haar belangrijkste producten.

De Verantwoording van Logius is mede gebaseerd op de uitkomsten van onderzoeken die door de Rijksauditedienst (RAD) zijn uitgevoerd naar het product Digipoort. De in de Verantwoording beschreven situatie heeft - tenzij anders vermeld - betrekking op de periode 1 januari 2010 tot en met 31 december 2010 (hierna: onderzoeksperiode). De onderzoeken zijn uitgevoerd aan de hand van beheersdoelstellingen met als doel geïmplementeerde maatregelen en procedures ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van het product Digipoort vast te stellen. Voor het opstellen van de beheersdoelstellingen en normenkaders is gebruik gemaakt van wet- en regelgeving, contracten met de leverancier en algemeen aanvaarde standaarden.

Logius is als groeiende organisatie in 2010 volop in beweging geweest. Dit komt tot uiting in de organisatorische wijzigingen als gevolg van de integratie van de Service Organisatie uit Apeldoorn, het toekennen van 50 FTE formatieve ruimte en de start van de reorganisatie - met als doel het meer toekomstvast maken van de organisatie - die in 2011 afgerond wordt. De aanstelling van nieuwe medewerkers heeft tot vertrek van externen geleid. Tijdens deze veranderingen zijn de voor de dienstverlening relevante processen binnen Logius onverminderd op peil gebleven. Dit vergt continue aandacht van het management. Het managementteam heeft dan ook eind 2010 besloten de huidige set procesbeschrijvingen te actualiseren en uit te breiden zodat aansluiting bij de nieuwe organisatie geborgd blijft.

Digipoort

Het tactisch beheer geeft over het algemeen in voldoende mate invulling aan de daaraan gestelde eisen. De aangetroffen maatregelen van Logius ten aanzien van de verschillende beheerprocessen bij Logius zijn voldoende om een betrouwbare verwerking van Digipoort te waarborgen. Aandacht gaat uit naar de continuïteitsmaatregelen met betrekking tot de back-up voorziening voor de kantoorautomatisering van Logius (Continuity Management).

In het eerste kwartaal van 2010 is voor het oude Digipoort systeem sprake geweest van dezelfde (toereikende) operationele beheersituatie als in 2009. Daarna is een nieuw Digipoort systeem in gebruik genomen. In de overgangsfase tot 1 juni 2010 is geen sprake geweest van een reguliere beheerorganisatie. Hierdoor waren bij de externe leverancier nog niet alle operationele beheerprocessen op het vereiste niveau effectief. In de applicatie Digipoort zijn evenwel voldoende controlemaatregelen getroffen om de volledigheid en tijdigheid van de berichten en de

bestandsverwerking te waarborgen. Ook is de beschikbaarheid van het nieuwe Digipoort systeem in de periode van 1 april tot en met 31 december 2010 100% geweest behoudens voor het FTP-koppelvlak. De beschikbaarheid voor dit koppelvlak was door storingen in september en oktober enkele dagen onder de afgesproken norm. Deze storingen zijn verklaard en ook is, waar nodig, gepaste actie ondernomen. Overigens zijn geen berichten verloren gegaan. Hierdoor heeft de Digipoort-dienstverlening aan klanten in 2010 vrijwel geheel voldaan aan de daaraan gestelde eisen met betrekking tot volledigheid, tijdigheid en beschikbaarheid.

Logius is van mening dat de operationele beheersmaatregelen voor de betrouwbaarheid en beschikbaarheid van Digipoort als geheel en voor de blijvende integrale werking van de applicatieve maatregelen in het bijzonder nog verbeterd moeten worden in 2011. Het betreft beheersmaatregelen op onder meer Continuity Management (maatregelen om bijvoorbeeld storingen en alarmeringen tijdig te voorzien en verhelpen), Change Management en Security-, Infrastructure- en Access Management.

2 Inleiding

2.1 Algemeen

Logius is verantwoordelijk voor het beheer en de verdere ontwikkeling van een aantal overheidsbrede ICT-producten. Deze ICT-producten worden gebruikt door klanten binnen de overheid en gelieerde organisaties die voor hun bedrijfsvoering afhankelijk zijn van het betrouwbaar en veilig functioneren van deze producten. Eén van de belangrijke producten die door Logius wordt aangeboden is Digipoort (koppelvlakken SMTP, X.400, FTP en POP3) (voorheen: Overheidstransactiepoort (OTP); verder genoemd: Digipoort); dit is het elektronische postkantoor voor bedrijven voor het snel en efficiënt uitwisselen van informatie met overheden. Voorliggende Verantwoording betreft alleen het systeem Digipoort met koppelvlakken SMTP, X.400, FTP en POP3.

Klanten van Digipoort hebben behoefte aan zekerheid over de kwaliteit van de dienstverlening van Logius. Gehanteerde kwaliteitsaspecten zijn beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid. Logius geeft invulling aan deze klantbehoefte door deze Verantwoording op te stellen en te laten voorzien van een Assurance-rapport. In een Assurance-rapport is de conclusie van een auditor (registeraccountant of register IT-auditor) opgenomen waarin in dit geval met een redelijke mate van zekerheid -dit is tevens de hoogst mogelijke mate van zekerheid- een uitspraak wordt gedaan over de juistheid en volledigheid van de Verantwoording.

Logius heeft de Rijksauditedienst gevraagd dit jaarlijkse Assurance-rapport te verzorgen. De Verantwoording gaat in op de opzet, het bestaan en de werking van de beheersmaatregelen en –procedures van Digipoort gedurende het jaar 2010.

2.2 Normstelling

Logius heeft beheersdoelstellingen opgesteld met als doel een toetsingskader te hebben van de kwaliteit van (het beheer van) Digipoort. De beheersdoelstellingen beschrijven in hoofdlijnen aan welke eisen het beheer van Digipoort moet voldoen en vormen de basis voor deze Verantwoording. Het normenkader, dat een nadere uitwerking is van de beheersdoelstellingen is samengesteld op basis van de relevante wet- en regelgeving, met name de Wet bescherming persoonsgegevens, het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) en algemeen aanvaarde kaders voor IT-omgevingen zoals 'Business Information Services Library' (BiSL) en 'Normen voor de beheersing van uitbestede ICT-beheerprocessen' van de NOREA (de beroepsorganisatie voor IT-auditors). Het normenkader richt zich voor een belangrijk deel op tactische en operationele beheerprocessen. Daarnaast zijn voor Digipoort en voor de onderliggende IT-infrastructuur specifieke beheersdoelstellingen geformuleerd.

2.3 Totstandkoming van de Verantwoording

In het eerste kwartaal van 2010 is voor het oude Digipoort systeem sprake geweest van dezelfde (toereikende) operationele beheerssituatie als in 2009. Logius heeft met een externe leverancier voor infrastructuur- en applicatiebeheer van Digipoort afspraken gemaakt over de van toepassing

zijnde beheersdoelstellingen voor het stelsel van beheerprocessen voor het nieuwe Digipoort systeem. De leverancier heeft een controleraamwerk opgesteld, met beheersmaatregelen die aansluiten bij de overeengekomen beheersdoelstellingen. Dit controleraamwerk is op 9 november 2010 formeel vastgesteld. Een door de leverancier aangewezen externe auditor heeft opzet, bestaan en werking van de beheersmaatregelen bij de leverancier getoetst. In 2010 is onderzoek uitgevoerd naar het infrastructuur- en applicatiebeheer van het nieuwe Digipoort systeem gedurende twee perioden:

- 1 april 2010 tot en met 31 mei 2010;
- 1 juni 2010 tot en met 31 december 2010.

RAD heeft onderzoeken uitgevoerd bij Logius en aanvullend onderzoek gedaan bij de externe leverancier naar opzet, bestaan en werking van maatregelen voor de volledigheid en tijdigheid van de berichtverwerking door Digipoort. De uitkomsten van deze onderzoeken zijn mede gebruikt als basis voor deze Verantwoording en het Assurance-rapport. De directeur van Logius is verantwoordelijk voor de inhoud van de Verantwoording. De RAD is verantwoordelijk voor het Assurance-rapport.

2.4

Leeswijzer

De lezer die globaal kennis wil nemen van de inhoud van het rapport kan zich beperken tot het Assurance-rapport, de inleiding en de managementsamenvatting. In hoofdstuk drie wordt in meer detail ingegaan op het beheer en de doorontwikkeling van Digipoort. In bijlage I is een overzicht opgenomen van de meest gebruikte afkortingen en begrippen. In bijlage II is een overzicht opgenomen van de getoetste beheersdoelstellingen.

3 Bevindingen Digipoort

3.1 Algemeen

Digipoort is het elektronische postkantoor van de overheid voor bedrijven. Het verzorgt de gemeenschappelijke infrastructuur voor het berichtenverkeer tussen bedrijven enerzijds en overheden anderzijds. Digipoort maakt het uitwisselen van deze gegevens eenvoudiger, omdat bedrijven één elektronische ingang bij de overheid hebben om hun gegevens voor verschillende overheidsinstanties aan te leveren. Digipoort draagt zorg voor gegarandeerde aflevering van berichten aan overheidsinstellingen. Na ontvangst van een bericht kan op verzoek van de aanleverende partij een ontvangstbevestiging naar aanleverende partij gestuurd waarna Digipoort de aflevering aan de overheidsinstelling bewaakt.

Het gebruik van de Digipoort is het afgelopen jaar verder toegenomen met een stijging van 22 miljoen berichten in 2009 tot ca. 40 miljoen berichten in 2010.

Logius is verantwoordelijk voor het tactisch en operationeel beheer van Digipoort. Infrastructuur- en applicatiebeheer is uitbesteed aan een externe leverancier.

3.2 Tactisch beheer

Inrichting tactische beheerprocessen

Logius heeft een aantal tactische processen geïmplementeerd voor het beheer van de producten die zij onder haar hoede heeft. Het doel van deze processen is om de kwaliteit van de producten van Logius op een voldoende niveau en in overeenstemming met wet- en regelgeving te borgen. In de praktijk zijn de werkzaamheden van Logius ondermeer:

- het onderhouden van de relatie met klanten inclusief het inventariseren van functionele wensen en eisen en capaciteitsplanning;
- het aansturen van leveranciers en het beheren van contracten;
- het beheersen van wijzigingen inclusief de aansturing van de realisatie van wijzigingen;
- het onderhouden van de architectuur van de producten inclusief de aansturing van het softwareonderhoud en de aanpassing van de bijbehorende niet geautomatiseerde informatievoorziening;
- het uitvoeren van incidentmanagement.

De tactische beheerprocessen zijn ingericht op basis van Business Information Services Library (BiSL), een procesmodel voor functioneel beheer en informatiemanagement. Gegeven de aard van haar werkzaamheden beperkt Logius zich tot de expliciete inrichting van de processen behoeftemanagement en contractmanagement op het sturende niveau en alle processen op het uitvoerende niveau. Aanvullend op BiSL heeft Logius een proces voor (tactisch) beveiligingsbeheer ingericht.

Onderzoek tactische beheerprocessen

In 2010 is Logius volop in beweging geweest. Dit komt tot uiting in de organisatorische wijzigingen als gevolg van de integratie van de Serviceorganisatie uit Apeldoorn in de afdelingen Markt en Servicemanagement en de start van de herinrichting van Logius in de drie afdelingen Dienstverlening, Productregie en Bedrijfsvoering. Tevens is in 2010 een extra formatieve ruimte van 50 FTE toegekend. Dit heeft tot de aanstelling van nieuwe en het vertrek van externe medewerkers geleid. Tijdens deze veranderingen is de dienstverlening van Logius onverminderd op kwalitatief niveau gehandhaafd. Dit vergt aandacht van het management, bijvoorbeeld voor het actueel houden van de tactische beheerprocessen.

Het tactisch beheer geeft over het algemeen in voldoende mate invulling aan de daaraan gestelde eisen. De aangetroffen maatregelen van Logius ten aanzien van de verschillende beheerprocessen bij Logius zijn voldoende om een betrouwbare verwerking van Digipoort te waarborgen. Aandacht gaat uit naar de continuïteitsmaatregelen voor de kantoorautomatisering van Logius (Continuity Management). Op de volgende pagina's wordt ingegaan op een aantal onderwerpen op het gebied van de tactische processen inclusief eventuele verbeteracties.

Behoeftemanagement

De afdeling Markt heeft in 2010 het proces Behoeftemanagement aangescherpt. Ter ondersteuning van Behoeftemanagement is een CRM-systeem ingericht. Klantwensen worden vertaald in een request for change (RFC) of project, waarop de afdeling Servicemanagement een impactanalyse kan uitvoeren. Zowel het Servicecentrum als de afdeling Servicemanagement hebben behoefte aan inzicht in de kwantitatieve verwachtingen over het gebruik van bestaande producten. De communicatie over het verwachte gebruik van de diensten vanuit de afdeling Markt richting de afdeling Servicemanagement is in 2010 beperkt geweest. De afdeling Markt gaat haar klanten om input vragen ter verbetering van de dienstverlening.

Contractmanagement

Het proces Contractmanagement wordt uitgevoerd door de afdeling Leveranciers- en Contractmanagement/Juridische Zaken (L&C/JZ), een samenvoeging van het team dat verantwoordelijk is voor leveranciers- en contractmanagement en het team dat verantwoordelijk is voor juridische ondersteuning. Expertise op het gebied van leveranciersmanagement, contractmanagement, inkoop en juridische zaken is gebundeld. Binnen L&C/JZ vindt aanbesteding van diensten, contractonderhandeling en -administratie plaats. Toezicht op naleving vindt plaats door de afdeling Servicemanagement. Aandachtspunt is het beter matchen van totstandkoming van wijzigingen en de registratie daarvan.

Incidentmanagement

Logius heeft een proces ingericht voor het aannemen en afhandelen van verstoringen in de ICT-dienstverlening. Dit proces valt gedeeltelijk onder tactisch beheer en gedeeltelijk onder operationeel beheer van Digipoort. Het operationeel beheer betreft eerstelijns ondersteuning. Hiervoor verwijzen we naar paragraaf 3.3. Het tactisch beheer betreft tweede- en derdelijns ondersteuning. Functioneel beheerders hebben de rol van incidentmanager gekregen. Zij staan roulerend 24 uur per dag, 7 dagen per week stand-by, zodat incidenten tijdig kunnen worden opgelost. Bij

calamiteiten wordt opgeschaald naar het MT-lid dat op dat moment dienst heeft.

Capacity Management

Het proces Capaciteitsmanagement vindt plaats bij de afdeling Servicemanagement. Met de externe leverancier voor applicatie- en infrastructuurbeheer zijn afspraken gemaakt over capaciteit. De leverancier rapporteert maandelijks aan Logius over deze prestatie indicatoren. In 2011 zal de afdeling Markt minimaal twee keer per jaar de verwachte prognose van gebruik door klanten in kaart brengen, zodat de benodigde capaciteit kan worden gecommuniceerd met het Servicecentrum en de leverancier.

Continuity Management

In het kader van de Verantwoording en het Assurance-rapport is een onderzoek gedaan naar de continuïteit van de ICT-ondersteuning, zoals het netwerk en de kantoorautomatisering, die door ICTU wordt geleverd aan Logius. Deze ICT-ondersteuning treft niet rechtstreeks de productie van de in beheer genomen producten, maar is met name ondersteunend aan de tactische processen en activiteiten zoals Logius die uitvoert. Opzet, bestaan en werking voor Continuïteitsmanagement (met name de back-up voorziening) van de ICT-voorziening binnen Logius waren in de onderzoeksperiode niet geheel toereikend. Het risico voor Digipoort wordt ingeschat als beperkt. Logius heeft hierop in maart 2011 gepaste actie ondernomen. De IT-dienstverlener heeft op het belangrijkste risico, te weten de back-up procedure afdoende maatregelen genomen.

Functionaliteitenbeheer

Het algemene beeld voor Functionaliteitenbeheer (het ontwikkelproces) is dat op hoofdpunten voldoende invulling is gegeven aan de beheersdoelstellingen voor de onderzoeksperiode.

Access Management

Logius heeft het actieplan uitgevoerd ter verbetering van Access Management. Zowel de procedures, de autorisatiematrix per ondersteunende applicatie als de monitoring door het bedrijfsbureau zijn in de loop van 2010 geïmplementeerd. Daardoor kon de werking niet over de gehele onderzoeksperiode toereikend worden vastgesteld. De rol van het MT bij monitoring van uitgegeven autorisaties moet beter opgepakt en beschreven worden.

Security Management

Het informatiebeveiligingsbeleid van Logius, de sturing en organisatorische inbedding zijn in 2010 volledig herzien. De staffunctie informatiebeveiliging is nu verantwoordelijk voor de actualisatie van het informatiebeveiligingsbeleid en de toezicht/controler op de uitvoering van het beleid. De lijnorganisatie is verantwoordelijk voor de uitvoering van het beleid.

De concept informatiebeveiligingsplannen voor Digipoort en Logius intern zijn gereed. Deze zijn gebaseerd op risicoanalyses die zijn uitgevoerd door de lijnorganisatie binnen de productgroepen. Medio 2011 worden de conceptplannen definitief gemaakt.

Juridische zaken

Het blijvend voldoen aan wet- en regelgeving wordt geborgd door onder meer bij wijzigingen van Digipoort een impactanalyse uit te voeren waarin de juridische aspecten worden meegenomen en door aan dit onderwerp aandacht te geven in het informatiebeveiligingsbeleid en -plan. Ook heeft de afdeling L&C/JZ van Logius in 2010 voor Digipoort een analyse in de breedte uitgevoerd aan de hand van relevante wet- en regelgeving:

- Wet bescherming persoonsgegevens (WBP);
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handel.

In het kader van compliance met wet- en regelgeving zijn de vorig jaar ontwikkelde checklists door L&C/JZ bijgewerkt voor de producten waarover Assurance wordt afgegeven. Voor Digipoort geldt dat de naleving van het informatiebeveiligingsbeleid en -plan een belangrijk aandachtspunt is. Een onderdeel hiervan is het afsluiten van de bewerkersovereenkomst met de externe leverancier.

De klanten van Logius stellen zelf de inhoud, en daarmee ook het doel voor het verwerken van persoonsgegevens, van het berichtenverkeer via Digipoort vast. Logius faciliteert met behulp van Digipoort de afnemer in haar de gegevensuitwisseling met aanleverende partijen. Kortgezegd bepalen de klanten ten aanzien van de berichtstromen de "wat" (berichtstroomdefinitie) en Logius ten opzichte van de gegevensuitwisseling de "hoe" (koppelvlakspecificaties). De afbakening van verantwoordelijkheden tussen klanten van Logius, Logius en de externe leverancier ten aanzien van de middelen dient nader te worden uitgewerkt in 2011.

3.3 Operationeel beheer

3.3.1 Context

Het operationeel beheer van de dienst Digipoort is belegd bij het Servicecentrum van de afdeling Markt van Logius en een externe leverancier. Het Servicecentrum verzorgt het servicebeheer (o.a. een aantal gestandaardiseerde taken als aansluiten van nieuwe klanten en berichtenstromen) en de eerstelijns ondersteuning (o.a. ondersteuning voor het afhandelen van incidenten). De externe leverancier is verantwoordelijk voor infrastructuur- en applicatiebeheer.

3.3.2 Bevindingen Servicecentrum Logius

Het Servicecentrum is een onderdeel van de afdeling Markt en is in december 2010 verhuisd van Apeldoorn naar Den Haag. Het servicebeheer en de eerstelijns ondersteuning zijn toereikend uitgevoerd.

3.3.3 Bevindingen externe leverancier Digipoort

Begin 2010 is het systeem Digipoort vervangen. Het infrastructuur- en applicatiebeheer van zowel het oude als het nieuwe Digipoort systeem zijn belegd bij dezelfde externe leverancier. Het vernieuwde systeem bevordert de beschikbaarheid en de betrouwbaarheid van Digipoort. De nieuwe Digipoort beschikt over een gemoderniseerd systeem met een uitwijkomgeving. Daarnaast is de bandbreedte van de verbinding uitgebreid, zodat in de toekomst meer berichten tegelijk kunnen worden verstuurd. Voor bedrijven is een nieuw koppelvlak voor postbussen (POP3) gerealiseerd.

In het eerste kwartaal van 2010 is voor het oude Digipoort systeem sprake geweest van dezelfde (toereikende) beheersituatie als in 2009. Het nieuwe Digipoort systeem is in de loop van het eerste kwartaal van 2010 in gebruik genomen, waarna de eerste klanten zijn aangesloten. In de overgangsfase tot 1 juni 2010 is het nieuwe Digipoort systeem beheerd door een projectorganisatie, bestaande uit betrokkenen vanuit Logius en de leverancier verantwoordelijk voor ontwikkeling van het vernieuwde Digipoort. Van een reguliere beheerorganisatie kon in deze periode derhalve nog geen sprake zijn. Uit de Service Niveau Rapportages blijkt dat de beschikbaarheid van Digipoort in de periode van 1 april tot en met 31 mei 2010 100% is geweest.

Formele decharge van de projectorganisatie heeft per 1 juni 2010 plaatsgevonden. De nieuwe beheerorganisatie van de leverancier bestaat uit een applicatiebeheergroep en een technisch beheergroep op twee verschillende locaties.

3.3.4 Belangrijkste bevindingen (over de periode 1 juni 2010 – 31 december 2010)

Generieke beheersaspecten en Service Level Management

Het controleraamwerk is sinds 9 november 2010 formeel vastgesteld en van kracht voor kwaliteitsmanagement.

Voor Digipoort is sinds augustus 2010 een rapportagetool beschikbaar, waarmee rapportages (ook over voorgaande periodes) gegenereerd kunnen worden over aantallen berichten. In de periode van 1 augustus tot en met 31 december 2010 heeft de rapportage maandelijks plaatsgevonden. De geaggregeerde cijfers van de voorgaande maanden zijn met terugwerkende kracht aan Logius gerapporteerd. Uit de Service Niveau Rapportages blijkt dat de beschikbaarheid van Digipoort in de periode van 1 juni tot en met 31 december 2010 100% is geweest behoudens voor het FTP-koppelvlak. De beschikbaarheid voor dit koppelvlak was door storingen in september en oktober enkele dagen onder de afgesproken norm. Deze storingen zijn verklaard en ook is, waar nodig, gepaste actie ondernomen. Overigens zijn geen berichten verloren gegaan.

Security, Infrastructure en Access Management

De leverancier heeft initiatieven gestart om de vertaling te maken van haar generieke beveiligingsbeleid en -handboek naar een Digipoort-specifiek beveiligingshandboek. Een eerste inventarisatie voor een Logius-specifiek beveiligingshandboek heeft plaatsgevonden.

Een monitoringtool controleert de Digipoort applicatie automatisch op beschikbaarheid en correcte werking. De tool kon voor FTP-servers op moment van onderzoek nog niet de volledige keten monitoren. Dit verbeterpunt is opgepakt en wordt naar verwachting in de tweede helft van 2011 gerealiseerd.

Een autorisatiematrix voor de Digipoort dienst is aanwezig. Deze bevat nog niet alle autorisaties voor de verschillende Digipoort omgevingen en bijbehorende systeemlagen. Daarnaast hebben een aantal beheerders en de ontwikkelaar in de periode juni tot en met december 2010 rechten gehad tot zowel de ontwikkel- en test- als productieomgeving. Het is

Logius niet gebleken dat dit heeft geleid tot incidenten in de productieverwerking.

Access management zal in 2011 verder worden ingericht.

Capacity, Availability en Continuity Management

De leverancier heeft beheersmaatregelen ten aanzien van onderhoud, availability en capaciteitsmanagement in praktijk geïmplementeerd.

Proces- en procedurebeschrijvingen ten aanzien van beschikbaarheid zijn gedocumenteerd, echter niet formeel vastgesteld. Een deel van de Digipoort omgeving wordt gemonitord op basis van best effort, waardoor de kans bestaat dat buiten kantoor tijden geen directe actie wordt ondernomen. In 2010 heeft dit geen invloed gehad op de Digipoort dienstverlening.

Een concept calamiteitenplan (onderdeel uitwijk) ligt thans bij Logius ter goedkeuring. In afwachting hiervan is in 2010 geen volledige calamiteitentest en -evaluatie uitgevoerd.

Configuration en Change Management

Sinds oktober 2010 zijn configuratie items van de Digipoort applicaties en systemen gestructureerd vastgelegd en worden wijzigingen op de configuratie items gestructureerd verwerkt in de configuratie-documentatie.

Een change managementproces en –procedurebeschrijving zijn aanwezig en geaccordeerd. Definities van standaard changes en emergency changes en een beschrijving van het ontwikkel-, test-, acceptatie- en productieproces ontbreken nog. Sinds 1 oktober 2010 wordt de doorlooptijd van voorgestelde wijzigingen accuraat gemonitord.

Incident en Problem Management

Een incident managementproces en -procedure beschrijving is aanwezig en geaccordeerd, evenals werkinstructies voor incident management. Sinds oktober 2010 wordt de beschreven werkwijze ook ondersteund door de bericht tooling, zodat de beheergroepen per SMS op de hoogte worden gebracht in het geval van een major incident.

Sinds oktober 2010 wordt het problem management proces bij de applicatiebeheergroep in Rotterdam ondersteund door een service management tool en kunnen aparte tickets worden aangemaakt. Incidenten worden wekelijks geanalyseerd tijdens het werkoverleg van de beheergroep ter signalering van problemen.

Diensts specifieke beheersingsmaatregelen Digipoort

Indien een door een aanleverende partij ingebracht bericht niet (goed) is verwerkt, kan Logius volgens een bepaalde procedure het bericht indien mogelijk opnieuw aanbieden ter verwerking (herinjectie). Indien herinjectie plaatsvindt, dient de volledigheid en tijdigheid van de berichtenverwerkingen te worden gecontroleerd. Het herinjectieproces is op hoofdlijnen beschreven, maar dient nog nader te worden uitgewerkt. Het herinjecteren van berichten, waardoor mogelijk de integriteit van die berichtenstroom gevaar loopt, heeft in 2010 niet plaatsgevonden.

Waarborgen in de applicatie Digipoort

De volledigheid en tijdigheid van de berichten- en bestandsverwerking worden voldoende gewaarborgd door de controlemaatregelen in de applicatie Digipoort.

3.4

Conclusie

Het tactisch beheer geeft over het algemeen in voldoende mate invulling aan de daaraan gestelde eisen. De aangetroffen maatregelen van Logius ten aanzien van de verschillende beheerprocessen bij Logius zijn voldoende om een betrouwbare verwerking van Digipoort te waarborgen. Aandacht gaat uit naar de continuïteitsmaatregelen voor de kantoorautomatisering van Logius (Continuity Management).

In het eerste kwartaal van 2010 is voor het oude Digipoort systeem sprake geweest van dezelfde (toereikende) operationele beheersituatie als in 2009. Daarna is een nieuw Digipoort systeem in gebruik genomen. In de overgangsfase tot 1 juni 2010 is geen sprake geweest van een reguliere beheerorganisatie. Hierdoor waren bij de externe leverancier nog niet alle operationele beheerprocessen op het vereiste niveau effectief. In de applicatie Digipoort zijn evenwel voldoende controle maatregelen getroffen om de volledigheid en tijdigheid van de berichten en de bestandsverwerking te waarborgen. Ook is de beschikbaarheid van het nieuwe Digipoort systeem in de periode van 1 april tot en met 31 december 2010 100% geweest behoudens voor het FTP-koppelvlak. De beschikbaarheid voor dit koppelvlak was door storingen in september en oktober enkele dagen onder de afgesproken norm. Deze storingen zijn verklaard en ook is, waar nodig, gepaste actie ondernomen. Overigens zijn geen berichten verloren gegaan.

Hierdoor heeft de Digipoort dienstverlening aan klanten in 2010 vrijwel geheel voldaan aan de daaraan gestelde eisen met betrekking tot volledigheid, tijdigheid en beschikbaarheid.

Logius is echter van mening dat de operationele beheersmaatregelen voor de betrouwbaarheid en beschikbaarheid van Digipoort als geheel en voor de blijvende integere werking van de applicatieve maatregelen in het bijzonder nog verbeterd moeten worden in 2011. Het betreft beheersmaatregelen op onder meer Continuity Management (maatregelen om bijvoorbeeld storingen en alarmeringen tijdig te voorzien en verhelpen), Change Management en Security-, Infrastructure- en Access Management.

Bijlage I Lijst met afkortingen

BiSL	Business Information Services Library
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
FTP	File Transfer Protocol
ICT	Informatie- en Communicatietechnologie
IT	Informatietechnologie
ITIL	Information Technology Infrastructure Library
L&C/JZ	Leveranciers- en Contractmanagement/Juridische Zaken
MT	Management Team
POP3	Post Office Protocol 3
RAD	Rijksauditdienst
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
VIR	Voorschrift Informatiebeveiliging Rijksoverheid

Bijlage II Beheersdoelstellingen

Tactisch beheer

Behoeftemanagement

- Bedrijfsprocessen van een organisatie worden ondersteund of ingevuld door een goede informatievoorziening en een functionele beheerorganisatie;
- Bestaande en nieuwe behoeften binnen het bedrijfsproces worden onderkend en hierover vindt besluitvorming plaats.

Contractmanagement:

- Er worden goede en adequate afspraken gemaakt over de geautomatiseerde informatievoorziening, deze worden bewaakt en beheerd;
- Er worden goede en adequate afspraken gemaakt over de dienstverlening door de ICT-leverancier, deze worden bewaakt en beheerd.

Incidentmanagement:

- Incidenten dienen tijdig, volledig en effectief te zijn afgehandeld.

Wijzigingenbeheer

- De juiste besluiten, gebaseerd op de kenmerken van de wijzigingen, worden genomen over het aanbrengen van wijzigingen of vernieuwingen in de informatievoorziening;
- Wijzigingen in de informatievoorziening worden geïnventariseerd, geprioriteerd, ten uitvoer gebracht, gemonitord en geëvalueerd.

Transitiemanagement:

- Een transitieplan is in proces 'Voorbereiden transitie' opgesteld met daarin alle afspraken en acties die noodzakelijk zijn om de verandering te effectueren;
- Communicatie over de transitie vindt op de juiste tijdstippen plaats naar gebruikers, ICT-leveranciers en functioneel beheer;
- Documentatie (werkinstructies en procedures waarop de verandering van invloed is) wordt op juiste manier bewaard, onderhouden en gedistribueerd.

Capaciteitsmanagement:

- De ICT-dienst dient de overeengekomen werklast te kunnen verwerken.

Continuïteitsmanagement:

- De ICT-dienst dient in het geval van een calamiteit tijdig herstelbaar te zijn.

Functionaliteitenbeheer:

- De wijzigingen worden eenduidig gespecificeerd op basis van de gewenste functionaliteit.
- Niet-geautomatiseerde informatievoorziening is beschreven en wordt onderhouden. Daarbij is aandacht voor het gebruik van het informatiesysteem en ondersteunende hulpmiddelen zoals formulieren.
- Gewenste veranderingen worden vlekkeloos in de organisatie doorgevoerd, gebruikte instrumenten, hulpmiddelen en andere ondersteuningsvormen werken correct.

- Probleemloze ingebruikname van de nieuwe of gewijzigde functionaliteit wordt geborgd door het opstellen van een transitieplan waarin tevens alle benodigde randvoorwaarden worden beschreven.

Access Management

- Toegang tot ICT-diensten en -middelen dient te zijn beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers.

Security Management:

- De samenhang tussen de individuele Security Management processen is geborgd.

Digipoort specifiek:

- Nieuwe berichtenstromen worden op een beheersbare en controleerbare wijze aan OTP toegevoegd.
- Nieuwe aansluitingen (deelnemers) worden op een beheersbare en controleerbare wijze gerealiseerd.
- Wijzigingen in berichtenstromen worden op een beheersbare en controleerbare wijze doorgevoerd.
- Wijzigingen in aansluitgegevens worden op een beheersbare en controleerbare wijze doorgevoerd.
- De volledigheid en tijdigheid van de berichtenverwerkingen door OTP wordt bewaakt en is controleerbaar.
- Alle relevante wet- en regelgevingen zijn vertaald naar inrichting en exploitatie eisen.

Beheersdoelstellingen Operationeel beheer Digipoort

Generieke beheersaspecten

- Het Digipoort proces dient te worden gegarandeerd.
- Het Digipoort proces dient controleerbaar te zijn.
- Het Digipoort proces dient aan de actuele vereisten te voldoen
- Belanghebbenden dienen juist en volledig over het Digipoort proces te worden geïnformeerd.

Service Level Management

- De geleverde ICT-diensten dienen aan de overeengekomen dienstenniveaus en beheersdoelstellingen te voldoen

Security Management

- Alle risico's voor de vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van de ICT-diensten dienen te worden geadresseerd.

Infrastructure Management

- De ICT-middelen dienen te worden ingesteld in overeenstemming met het geautoriseerde ontwerp.
- Pogingen tot ongeautoriseerde toegang tot ICT-middelen dienen tijdig te worden gedetecteerd.

Access Management

- Toegang tot ICT-diensten en -middelen dient te worden beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers en beheerders.

Capacity Management

- De ICT-diensten dienen de overeengekomen werklast te kunnen verwerken.

Availability Management

- De ICT-diensten dienen onder normale bedrijfsomstandigheden aan het overeengekomen niveau van beschikbaarheid te voldoen.

Continuity Management

- De ICT-diensten dienen in het geval van een calamiteit tijdig herstelbaar te zijn.

Configuration Management

- Configuration items, hun kenmerken en onderlinge samenhang dienen juist en volledig te worden geïdentificeerd en vastgelegd.

Change Management

- Wijzigingen dienen te worden geautoriseerd met inachtneming van de risico's voor de ICT-diensten.
- Wijzigingen dienen tijdig en volledig te worden doorgevoerd.
- Wijzigingen dienen te worden beoordeeld op doeltreffendheid.

Incident Management

- Incidenten dienen tijdig en volledig te worden afgehandeld.
- Incidenten dienen doeltreffend te worden afgehandeld.

Problem Management

- Problemen dienen tijdig en volledig te worden gesignaleerd en afgehandeld.
- Problemen dienen doeltreffend te worden afgehandeld.

Operations Management

- Productieopdrachten dienen te worden geautoriseerd.
- Productieopdrachten dienen juist, volledig en tijdig te worden verwerkt.
- Verwijderbare opslagmedia en hun kenmerken dienen juist en volledig te worden geïdentificeerd en vastgelegd.

Digipoort specifiek

- De levenscyclus van aansluitingen en berichtenstromen worden op controleerbare wijze beheerst.
- De volledigheid en tijdigheid van de herinjectie door Digipoort wordt bewaakt en is controleerbaar.
- De volledigheid en tijdigheid van de berichtenverwerkingen door Digipoort wordt bewaakt en is controleerbaar.
- Het informatiebeveiligingsbeleid van Digipoort is vertaald naar inrichting en exploitatie eisen.
- Alle relevante beheerhandelingen aan de Digipoort applicatie en infrastructuur zijn controleerbaar en worden aantoonbaar bewaakt.
- Alle afgesproken bewaartermijnen zijn op de juiste wijze vertaald naar juiste instellingen in Digipoort.