



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Assurance-rapport en Verantwoording 2010 Producten van Logius

DigiD voor Burgers
Haagse Ring (onderdeel Diginetwerk)

Datum 17 mei 2011
Status Definitief

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: Rijksauditdienst

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 5 jaar! Met het enthousiasme van een jonge organisatie biedt Logius al 5 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 voor onze belangrijkste producten.

Het Assurance-rapport en de Verantwoording die voor u liggen heeft betrekking op de opzet, het bestaan en de werking van DigiD voor Burgers (hierna: DigiD) en Haagse Ring (onderdeel van Diginetwerk) 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 Rijksauditedienst (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. Wat betreft DigiD is er regelmatig publiciteit als zou DigiD fraudegevoelig zijn. Logius zit daar uiteraard boven op daar waar het gaat om het weerleggen van onjuiste berichtgeving en het voorkomen van fraudegevoeligheid. Het realiseren van de aanbevelingen die voortkomen uit de onderzoeken van de RAD, is inmiddels in gang gezet. De voorbereidingen voor realisatie van een verbeterde DigiD applicatie zijn in volle gang. Tijdens de verbouwing blijft de winkel uiteraard open. 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 de producten DigiD voor Burgers (hierna: DigiD) en Haagse Ring (onderdeel van Diginetwerk) van Logius. Het rapport dient uitsluitend in samenhang met de verantwoording over de periode 1 januari tot en met 31 december 2010 over deze producten 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 17 mei 2011, waarin de in de periode 1 januari tot en met 31 december 2010 beoogde en geïmplementeerde maatregelen en procedures bij Logius en betrokken leveranciers zijn opgenomen ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van de producten DigiD en het tactisch beheer van Haagse Ring 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 beheersdoelstellingen en normen (op te vragen bij Logius). Deze sluiten aan op algemeen aanvaarde uitgangspunten en op de contracten tussen Logius en haar leveranciers. Logius heeft zorg gedragen voor de afstemming van de beheersdoelstellingen en normen met een vertegenwoordiging van haar Programmaraad. 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 leveranciers;
- het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's in de externe omgeving en de betrokken organisaties en het onderzoeken in hoeverre deze risico's worden afgedekt door maatregelen en procedures en het beoordelen van de plausibiliteit van de informatie in de verantwoording;
- het beoordelen van de opzet en het vaststellen van het bestaan en de werking van de relevante maatregelen en procedures;
- het onderzoeken van de juistheid en volledigheid van de informatie in de Verantwoording, mede gelet op de informatiebehoeften van de huidige en potentiële afnemers van de producten van Logius;
- het evalueren van het algehele beeld van de Verantwoording, inclusief het beoordelen van de consistentie van de informatie, aan de hand van de bovengenoemde 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 de producten DigiD en Haagse Ring bij Logius en haar leveranciers betreffende het tijdvak 1 januari 2010 tot en met 31 december 2010 juist en volledig is.

Toelichting op het oordeel

De producten DigiD en Haagse Ring zijn bouwstenen voor de realisatie van betrouwbare digitale diensten. Organisaties dienen zich ervan bewust te zijn dat het toepassen van één of meerdere van deze bouwstenen alleen 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 de producten DigiD en Haagse Ring 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 DigiD. Voor nadere informatie verwijzen wij naar paragraaf 3.6 van de Verantwoording.

Den Haag, 17 mei 2011
Rijksauditedienst

A handwritten signature in black ink, consisting of a large, stylized loop on the left that extends into a long, thin horizontal stroke on the right.

mr. drs. J. Roodnat RE RA
Clustermanager RAD

A handwritten signature in black ink, featuring a complex, cursive style with multiple overlapping loops and a long horizontal tail extending to the right.

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

Inhoud

Colofon	II
Woord vooraf	III
Assurance-rapport	IV
Inhoud	1
1 Managementsamenvatting	3
2 Inleiding	5
2.1 Algemeen	5
2.2 Normstelling	5
2.3 Totstandkoming van de Verantwoording	6
2.4 Leeswijzer	6
3 Bevindingen DigiD	7
3.1 Algemeen	7
3.2 Tactisch beheer	7
3.3 Operationeel beheer	10
3.3.1 Beheer infrastructuur DigiD (rekencentrum).....	10
3.3.2 Print- en maildienstverlening	15
3.3.3 Callcenter	18
3.3.4 Ondersteuning SMS-authenticatie.....	21
3.4 Dienstspectifieke beheersingsmaatregelen DigiD.....	23
3.4.1 Wijze inloggen beheerders	24
3.4.2 Applicatielogging DigiD	24
3.4.3 Toepassen cryptografie	24
3.5 Naleving wet- en regelgeving.....	24
3.6 Conclusie.....	24
4 Bevindingen Haagse Ring	26
4.1 Algemeen	26
4.2 Rolverdeling en inrichting beheer	26
4.3 Informatiebeveiliging Haagse Ring.....	27
4.4 Conclusie.....	27
Bijlage I Lijst met afkortingen	28

Bijlage II Beheersdoelstellingen..... 29

1 Managementsamenvatting

Algemeen

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

De Verantwoording van Logius is mede gebaseerd op de uitkomsten van onderzoeken die door de Rijksauditdienst (RAD) zijn uitgevoerd naar de producten DigiD en Haagse Ring. 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 normenkaders met als doel geïmplementeerde maatregelen en procedures ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van de producten DigiD en Haagse Ring vast te stellen. Voor het opstellen van de normenkaders is gebruik gemaakt van wet- en regelgeving, contracten met leveranciers 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.

DigiD

De DigiD dienstverlening voldoet over het algemeen aan de daaraan gestelde eisen. Ten opzichte van controlejaar 2009 is met de implementatie van een nieuwe IT-Infrastructuur een behoorlijke stap gezet.

Wel is vastgesteld dat met het aanwezige stelsel van beheermaatregelen voor het product DigiD in de onderzoeksperiode op een beperkt aantal punten nog niet voldoende invulling is gegeven aan alle afgesproken normen. De belangrijkste punten hebben te maken met de logging van het gebruik van de applicatie van DigiD. Het betreft zowel de bewaking en analyse van afwijkingen als de verdere afhandeling van de afwijkingen.

Logius heeft geen aanwijzing dat genoemde punten in de Verantwoordingsperiode negatieve gevolgen hebben gehad voor de DigiD dienstverlening.

Het functioneren van de dienstspecifieke maatregelen in en rondom DigiD geeft in opzet, bestaan en werking voor de onderzoeksperiode een aantal bevindingen weer waaraan een middenrisico is gekoppeld. De verbeteringen worden of nog in de huidige versie van DigiD doorgevoerd of pas wanneer de nieuwe versie DigiD 4.0 in productie genomen wordt.

Haagse Ring

Logius is verantwoordelijk voor het tactisch beheer van Haagse Ring. De beheersmaatregelen voor het tactisch beheer van Haagse Ring worden in voldoende mate uitgevoerd. De formalisatie van de mogelijke nieuwe kaders voor rolverdeling en aansluitvoorwaarden, welke in najaar van 2010 is voorgelegd aan de Subcommissie Informatiebeveiliging van Directoraat Generaal Organisatie en Bedrijfsvoering Rijk (SIB/DGOBR), wordt in 2011 doorgevoerd.

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. Twee belangrijke producten die door Logius worden aangeboden, zijn:

- DigiD; DigiD staat voor Digitale Identiteit. DigiD is het digitale authenticatiesysteem voor de overheid en publieke dienstverleners. DigiD zorgt ervoor dat zij betrouwbaar zaken kunnen doen met burgers via hun website;
- Haagse Ring; een netwerk voor datatransport tussen de aangesloten netwerken van de departementen, de Hoge Colleges van Staat en andere organisaties die op voordracht van departementen zijn aangesloten. Het beheerdomein van Logius beperkt zich tot de uitvoering van onderdelen van het tactisch beheer voor Haagse Ring.

Klanten van deze producten 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 de twee genoemde producten gedurende het jaar 2010.

2.2 Normstelling

Logius heeft een normenkader opgesteld met als doel een objectief beeld te kunnen geven van de kwaliteit van (het beheer van) de producten. Dit normenkader beschrijft in hoofdlijnen aan welke eisen het beheer van de producten moet voldoen en vormt de basis voor deze Verantwoording. Het normenkader is samengesteld op basis van de relevante wet- en regelgeving, met name het 'Tijdelijk besluit nummergebruik overheidtoegangsvoorziening', 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 bijvoorbeeld voor de DigiD applicatie en voor de onderliggende IT-infrastructuur specifieke normen geformuleerd. De directeur van Logius heeft het normenkader in 2008 vastgesteld na afstemming met een

vertegenwoordiging van de Programmaraad. De Programmaraad bestaat uit een vertegenwoordiging van de (semi-)overheidsorganisaties die gebruik maken van de producten van Logius.

2.3 Totstandkoming van de Verantwoording

De auditor heeft op basis van de normenkaders onderzoeken uitgevoerd bij Logius en de leveranciers. 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 auditor 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 de hoofdstukken drie en verder wordt in meer detail ingegaan op het beheer en de doorontwikkeling van de producten. 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 DigiD

3.1 Algemeen

DigiD staat voor Digitale Identiteit. DigiD is het digitale authenticatiesysteem voor de overheid en publieke dienstverleners. DigiD zorgt ervoor dat zij betrouwbaar zaken kunnen doen met burgers via hun website. Voor burgers die deze diensten via internet afnemen is DigiD een handig hulpmiddel. Met één inlogcode krijgt de burger toegang tot elektronische diensten van steeds meer overheidsinstellingen en publieke dienstverleners.

In totaal zijn er in 2010 31 nieuwe organisaties aangesloten op DigiD. Als gevolg van herindeling zijn 14 gemeenten vervallen. Het aantal aansluitingen in 2010 is daarmee van 487 naar 504 gestegen, wat 20% van de jaarbegroting is. Het aantal gelukke authenticaties voor 2010 was ruim 37 miljoen en daarmee is de jaarbegroting met 16% overschreden. Het aantal eindgebruikers is in 2010 gegroeid van 7,5 naar 8,1 miljoen.

In 2010 is de DigiD dienstverlening verbeterd. In december is in verband met de Webrichtlijnen een release met aanpassingen in productie gebracht. In deze release zijn ook de nieuwe eisen voor sterkere wachtwoorden opgenomen.

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 Service Organisatie 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. Aandacht gaat uit naar het beter inschatten van de capaciteitsvraag naar producten van Logius door (nieuwe) klanten die nieuwe diensten verlenen (Capacity Management) en 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

Het proces Incidentmanagement wordt uitgevoerd door het Servicecentrum. Het Servicecentrum is een onderdeel van de afdeling Markt en is in december 2010 verhuisd van Apeldoorn naar Den Haag. Voor het registreren van de incidenten en het bewaken van de termijnen voor afhandeling maakt Logius gebruik van een registratiesysteem. Voor het incidentproces zijn in 2010 een incidentenhandboek en Quick Reference Cards opgesteld. Daarnaast hebben functioneel beheerders 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.

Wijzigingenbeheer en Transitie management

Eind 2010 is gestart met het efficiënter inrichten van de overlegstructuren binnen deze processen. Daar wordt in 2011 een vervolg aan gegeven door actualisering van de processen waarin de verantwoordelijkheden per functie duidelijk belegd zullen worden.

Capaciteitsmanagement

Het proces Capaciteitsmanagement vindt plaats bij de afdeling Servicemanagement. De servicemanager stemt de benodigde capaciteit af met de verschillende leveranciers van DigiD. In 2010 is het enkele malen gebeurd dat het verwachte gebruik van de producten niet tijdig is doorgegeven. Dit heeft echter niet geleid tot verstoringen in de verwerkingscapaciteit bij de leverancier. In 2011 zal de afdeling Markt minimaal twee keer per jaar de verwachte prognose van gebruik door klanten in kaart brengen, zodat de capaciteit beter kan worden ingeschat en worden gecommuniceerd met de leveranciers.

Continuïteitsmanagement

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 van de ICT-voorziening binnen Logius waren in de onderzoeksperiode niet geheel toereikend. Het risico voor DigiD en Haagse Ring wordt ingeschat als beperkt. Logius volgt de aanbeveling op om zo spoedig mogelijk zorg te dragen voor een aangescherpte back-up procedure voor de diverse netwerkschijven en een getest continuïteitsplan voor de ICT-ondersteuning van Logius. Inmiddels heeft de huidige IT-dienstverlener op het belangrijkste risico (back-up procedure) afdoende maatregelen genomen. Overigens wordt de ICT-ondersteuning in de eerste helft van 2011 overgenomen door een professionele dienstverlener.

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 nog 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/controlen op de uitvoering van het beleid. De lijnorganisatie is verantwoordelijk voor de uitvoering van het beleid.

De concept informatiebeveiligingsplannen voor DigiD, Haagse Ring en Logius intern zijn inmiddels opgezet. Deze zijn gebaseerd op risicoanalyses die zijn uitgevoerd door de lijnorganisatie binnen de productgroepen. Begin 2011 worden de concept plannen nader uitgewerkt.

Nieuwbouw applicatie DigiD 4.0

Het Assurance-rapport van 2010 richt zich voor wat betreft DigiD op de versie die nu productie draait. De verwachting is dat DigiD 4.0 – voorheen DigiD X – in de loop van 2011 in productie wordt genomen.

De huidige DigiD applicatie kent onder andere de volgende zwakke punten die niet op doelmatige wijze kunnen worden weggenomen:

- de broncode bestaat voor een aanzienlijk deel uit 'oude' code die niet voldoet aan de huidige standaarden op dit gebied;
- de applicatie kent geen gelaagde architectuur wat aanpassen van de code complex en risicovol maakt.

Deze punten worden niet meer opgelost in de huidige applicatie. Logius zal verifiëren of de geconstateerde knelpunten in DigiD 4.0 daadwerkelijk zijn opgelost. Indien mocht blijken dat DigiD 4.0 uitloopt, dan moeten risico's voor de huidige DigiD applicatie mogelijk zwaarder worden gewogen, aangezien ze langer aanwezig blijven.

3.3 Operationeel beheer

3.3.1 Beheer infrastructuur DigiD (rekencentrum)

Algemeen

Logius heeft het beheer van de IT-infrastructuur van DigiD uitbesteed aan een externe leverancier. Hiertoe is een overeenkomst afgesloten tussen Logius en deze leverancier. De leverancier heeft een aantal IT-beheerprocessen ingericht om de afgesproken dienstverlening te realiseren. Er is onderzoek uitgevoerd naar zowel het algemeen beheer als naar (het beheer van) de IT-infrastructuur, voorzover betrekking hebbend op de beschikbaarheid en betrouwbaarheid van de DigiD dienstverlening. Op basis van onderzoek is de conclusie dat het beheer in voldoende mate invulling heeft gegeven aan de daaraan gestelde eisen, met als kanttekening een aandachtspunt voor 2011 voor het proces Operations Management en Infrastructure Management. Op de volgende pagina's is per beheerproces een samenvatting van de bevindingen opgenomen.

Generieke Beheersaspecten

De leverancier heeft een actuele, door het management vastgestelde Information Security Policy. Hierin hebben vertrouwelijkheid en integriteit van informatie en het voldoen aan nationale wetgeving zoals de Wet bescherming persoonsgegevens aandacht. Om invulling te geven aan de gestelde beheersdoelstellingen zijn beheerprocessen ingericht volgens het door de leverancier gehanteerde Continuous Service Delivery Model (CSDM, gebaseerd op Information Technology Infrastructure Library (ITIL)). Het beheer van DigiD wordt door voldoende functionarissen verzorgd, met aandacht voor het verder ontwikkelen van vaardigheden, competenties en kennis. Voor wijzigingsverzoeken, incidenten, problemen en andere klantvragen heeft de leverancier een servicedesk tool ingericht. Processtappen, controleactiviteiten en informatie over de productieverwerking worden hierin geregistreerd. Conform het Service Delivery Plan worden kwaliteitscontroles en reviews door onafhankelijke functionarissen uitgevoerd. De resultaten worden in rapportages opgenomen. Specifiek voor DigiD is in het kader van het Assurance-rapport over 2010 een interne review uitgevoerd.

Service Level Management

Er is een Service Delivery Plan voor DigiD beschikbaar, met daarin de door de leverancier te leveren diensten in het kader van de DigiD dienstverlening. Ook is er een Service Niveau Overeenkomst (SNO) voor Infrastructuur en Applicatiebeheer DigiD. Afspraken zijn geconcretiseerd in een Dossier Afspraken en Procedures (DAP). Het DAP bevat operationele afspraken en procedures tussen Logius en de leverancier. Het DAP wordt aangepast na goedkeuring van Logius, na afstemming met de leverancier. Volgens het DAP worden incidenten, problemen en wijzigingen pas afgesloten als deze door Logius zijn goedgekeurd.

De leverancier rapporteert maandelijks over de dienstverlening aan Logius. In het regulier overleg tussen de leverancier en Logius komen de maandelijksse rapportages van de leverancier aan Logius aan de orde.

Security Management

De leverancier heeft een actuele, door het management vastgestelde Information Security Policy. Het treffen van beveiligingsmaatregelen, reageren op beveiligingsincidenten en laten uitvoeren van beveiligingsaudits is de verantwoordelijkheid van de proceseigenaren van de diverse beheerprocessen. Uitgangspunten voor het treffen van beveiligingsmaatregelen is een risicoanalyse.

In de architectuurvisie Infrastructuur DigiD is rekening gehouden met onder meer de eisen uit het Informatiebeveiligingsplan van Logius. Ook in de impactanalyse wordt op risico's ingegaan en het Project Initiation Document (PID) DigiD Plan A (17 mei 2009) is voorzien in diverse risicologs.

Het ontwerp voor de nieuwe DigiD omgeving (Plan A) is op 18 januari 2010 geïmplementeerd. Met behulp van een monitoringtool wordt vastgesteld of blijvend wordt voldaan aan de Security Baseline van de leverancier. Hierover wordt periodiek gerapporteerd. Zie verder Infrastructure management.

Capacity Management

De leverancier heeft een capaciteitsplan voor de generieke ICT-dienstverlening dat moet waarborgen dat de in de Service Niveau Overeenkomst (SNO) overeengekomen dienstverlening ingevuld kan worden. Gerealiseerde serviceniveaus worden bewaakt en vergeleken met de overeengekomen niveaus. Analyse op de signalering van trends in de benutting van de capaciteit vindt niet plaats. De leverancier heeft geen DigiD specifiek capaciteitsplan opgesteld.

Indien Logius op basis van de in Service Niveau Rapportages (SNR) gesignaleerde trends aanvullende dienstverlening c.q. capaciteit verlangt, kan Logius hierover aanvullende afspraken maken met de leverancier. Dit is in 2010 niet nodig gebleken. Mede naar aanleiding van capaciteitsproblemen in het verleden is het twin-datacenter concept geïmplementeerd. Zie verder Infrastructure Management.

Availability Management

De leverancier heeft Availability Management ingericht, waarbij aandacht is besteed aan risico's en bedreigingen voor de beschikbaarheid van de generieke ICT-dienstverlening. Voor DigiD is een beschikbaarheids- (failover)plan aanwezig voor de database. Het plan beschrijft:

- een beknopt ontwerp van de beschikbaarheidsvoorziening, inclusief een overzicht van de (redundantie in de) systemen;
- een draaiboek voor het uitvoeren van een omschakeling naar de secundaire database indien de primaire is uitgevallen;
- scenario's voor het uitvoeren van failovertests.

De beschikbaarheidsvoorziening van de DigiD omgeving is getest tijdens de oplevering van deze omgeving. Hieruit is gebleken dat de failovervoorziening in diverse omgevingen goed heeft gefunctioneerd. De beschikbaarheid van de services wordt gemonitord en hierover wordt periodiek gerapporteerd in het kader van Service Level Management. Availability Management met betrekking tot de infrastructuur wordt nader beschreven onder Infrastructure Management.

Continuity Management

Er is een uitwijk (failover)plan voor de DigiD dienstverlening. De nieuwe infrastructuur van Plan A (zie Security Management) die sinds 18 januari 2010 operationeel is, maakt voor de waarborging van de continuïteit en beschikbaarheid gebruik van een clusteromgeving. Deze clusteromgeving is verdeeld over twee datacenters die elkaars activiteit kunnen overnemen als zich problemen voordoen. Deze omgeving is tijdens de oplevering getest. Daaruit is gebleken dat de failovervoorziening in diverse omgevingen goed heeft gefunctioneerd.

Infrastructure Management

Bij de leverancier is per 18 januari 2010 het door Logius goedgekeurde plan "Architectuur visie voor de nieuwe infrastructuur DigiD Burger" geïmplementeerd. Vanaf deze datum bestaat de DigiD omgeving uit twee volledig nieuw ingerichte fysiek gescheiden datacenters, ingericht volgens het twin-datacenter concept. Dit houdt in dat beide datacenters identiek zijn ingericht en in geval van calamiteiten bij één van de datacenters, de andere de gewenste functionaliteit blijft bieden. Door het redundant uitvoeren van netwerk- en hardwarecomponenten in de nieuwe IT-infrastructuur zijn waarborgen getroffen die tegemoet komen aan de door Logius gestelde eis van hoge beschikbaarheid voor de voorziening DigiD.

Een belangrijk aandachtspunt voor het huidige twin-datacenter concept is het correct functioneren van het mechanisme van automatische failover. In de SNO is daartoe overeengekomen dat de leverancier twee maal per jaar deze voorziening test. Dit kan ook op verzoek van Logius worden uitgevoerd. De leverancier heeft deze periodieke tests gedurende het jaar 2010 niet uitgevoerd. Ook vanuit Logius is hiertoe geen verzoek ingediend. De werkzaamheden die zijn uitgevoerd bij het implementeren van DigiD release 2.17 in december (onder andere het stil leggen van de web- en applicatieserver aan één kant) hebben echter geen verstoringen laten zien met betrekking tot het automatische failover-mechanisme.

Voor de nieuwe omgeving gelden de Security Baselines van de leverancier. Bij de controle op de inrichting van de servers is gebleken dat een passend beveiligingsniveau is geïmplementeerd.

De leverancier voert geautomatiseerde controles uit op de terechtheid van aanwezige hardware, bestaande Unix systeemconfiguraties en geïmplementeerde (persoonsgebonden) beheeraccounts. Ook controle op een juiste configuratie van de netwerkcomponenten vindt geautomatiseerd plaats.

Op basis van de SMART-rapportages (leverancierspecifieke rapportage) is vastgesteld dat de feitelijke beveiligingsinstellingen afwijken van het door de leverancier gehanteerde Unix chassis (=een Unix omgeving die volgens het standaardbeleid van de leverancier is gehardened). Voor een deel worden deze afwijkingen door de leverancier verklaard door de benodigde functionaliteit van de servers (need-to-use), voor een ander deel ontbreken deze verklaringen vooralsnog en wordt gewerkt aan het nader toelichten en analyseren hiervan. De leverancier heeft in het laatste kwartaal van 2010 daartoe een inhaalslag uitgevoerd (84% compliancy en 16% non-compliancy aan de daarvoor afgesproken normen).

Access Management

De terechtheid van de in de systemen aanwezige (beheer)accounts en de daaraan gekoppelde autorisaties voor de DigiD infrastructuur worden periodiek getoetst. Ook voor netwerk accounts vinden dergelijke toetsingen op de toegangsservers plaats.

Op basis van een deelwaarneming is voor een aantal servers vastgesteld dat sterke wachtwoorden niet worden afgedwongen. Het risico is echter beperkt, omdat de toegang tot het DigiD beheernetwerk door verschillende beveiligingsschillen is afgeschermd. Een verbeteractie van de leverancier heeft ertoe geleid dat vijf default wachtwoorden, die nooit gebruikt zijn, zijn gewijzigd.

Er vindt continue vergelijking plaats tussen de formele rechten zoals opgenomen in het personeelsbestand van de leverancier en de daadwerkelijk toegekende rechten in de IT-systemen .

Logius heeft als eis gesteld dat binnen de DigiD omgeving beheerders uitsluitend dienen te beschikken over minimale beheerrechten. Nagenoeg alle op de systemen aangemaakte beheergroepen beschikten gedurende 2010 via het sudo-mechanisme over een beperkte set aan beheerrechten. Een belangrijk aandachtspunt daarbij is het toekennen van rootrechten (absolute rechten) aan de reguliere DigiD beheerders. De leverancier

heeft aangegeven dat deze rechten uit oogpunt van doelmatig beheer en continuïteit van de bedrijfsprocessen strikt noodzakelijk zijn. Het risico voor de DigiD dienstverlening is beperkt door de inrichting van een adequaat stelsel van procedurele en logische maatregelen, dat voldoende waarborgen biedt tegen ongeautoriseerde beheerhandelingen. Het daadwerkelijk bestaan van deze risicobeperkende maatregelen en de effectiviteit daarvan is gedurende 2010 vastgesteld en getoetst.

Configuration Management

De leverancier heeft het Configuration Management Proces beschreven. Hierin staan de taken en verantwoordelijkheden van de bij het configuratiemanagementproces betrokken medewerkers. Alle configuratie-items (hardware en software) worden met een versienummer geregistreerd. Wijzigingen in (de status van) configuratie-items worden continu bewaakt, evenals afwijkingen tussen de registratie en de feitelijke aanwezigheid. Bij afwijkingen worden automatisch calls aangemaakt.

De verificaties vinden plaats, geconstateerde fouten zijn vastgelegd en afgehandeld.

Change Management

Aan wijzigingen wordt op basis van de impact een classificatie toegekend. Niet-standaard wijzigingsverzoeken van Logius worden door de leverancier intern ter instemming aangeboden aan het Change Control Board (CCB) van de leverancier. Er is specifiek aandacht voor ondermeer patches en urgente wijzigingen. Classificatie van een wijziging vindt plaats (standaard, medium, large, urgent, etc.). Een impactanalyse wordt uitgevoerd, waarin ook risico's van een wijziging worden beoordeeld.

In geval van een standaard wijziging mag direct met de ontwikkeling worden begonnen. Het doorvoeren van urgente wijzigingen gebeurt in overleg met de klant. Bij urgente wijzigingen worden de stappen versneld doorlopen. Eventueel overgeslagen stappen dienen achteraf alsnog te worden uitgevoerd. Er hebben in 2010 geen urgente wijzigingen plaatsgevonden. Voor medium en major changes is een change implementation plan vereist. Hierin wordt het uitvoeren van een risicoanalyse verplicht gesteld. Deze wijzigingen verlopen via het CCB. Voor een dergelijke wijziging is vastgesteld dat de vereiste bescheiden aanwezig zijn. De change manager is verantwoordelijk voor de voortgangsbewaking op de afhandeling van de wijziging.

Voorafgaand aan de implementatie van een wijziging wordt deze getest. Daartoe zijn diverse templates voor testplannen, overdracht en testbasis beschikbaar. Hierin is opgenomen welke testen in welke situatie moeten worden uitgevoerd. Indien nodig wordt een back-out plan opgesteld.

Incident Management

Voor Incident Management is een tool ingericht als loket. De registratie van gegevens over incidenten is gestandaardiseerd en wordt vastgelegd in de servicedesk tool. Incidenten krijgen een prioriteit toebedeeld. Registratie van bekende incidenten en beschikbare oplossingen is aanwezig en raadpleegbaar op locatie bij de leverancier.

Uit ticketregistraties en diverse maandrapportages over incidenten en problemen inzake DigiD, blijkt het afsluiten van incidenten en het bewaken van normtijden en de tevredenheid van de melder.

Problem Management

Uitgangspunt voor Problem Management bij de leverancier is dat incidenten systematisch worden geanalyseerd ter signalering van problemen. Problemen worden geprioriteerd. De verantwoordelijkheid voor het bewaken van de voortgang is belegd. De problem manager waarborgt dat een probleem pas wordt afgesloten indien het opgelost is, of indien wordt besloten dat het niet is op te lossen. Eén en ander blijkt uit ticket registraties en diverse maandrapporthages over incidenten en problemen inzake DigiD. Hieruit blijkt ook het afsluiten van problemen en het bewaken van normtijden en de tevredenheid van de melder.

Operations Management

Voor het proces Production blijkt dat back-up jobs moeten worden ingepland. Aan batch jobs moeten afspraken ten grondslag liggen. De uitvoering van jobs wordt dagelijks bewaakt. Hiermee wordt, voor wat betreft het inplannen van batchopdrachten, voldaan aan de beheersdoelstellingen voor operations management.

Veilige afvoer c.q. vernietiging van gegevensdragers maakt geen onderdeel uit van het control framework van de leverancier. De leverancier heeft medegedeeld dat er wel een procedure beschrijving "Asset Life Cycle Management Process" is. Tot nu toe zijn er geen gegevensdragers vernietigd of afgevoerd. Dit is een aandachtspunt voor 2011, wanneer de apparatuur van de oude DigiD infrastructuur wordt afgevoerd. Bij de leverancier is bekend dat overtollige gegevensdragers van DigiD gecertificeerd vernietigd moeten worden.

3.3.2 Print- en maildienstverlening

Algemeen

Logius heeft de print- en maildienstverlening uitbesteed aan een externe leverancier (verder: print- en mailleverancier). Hiertoe is een overeenkomst afgesloten tussen Logius en deze leverancier. Er is een onderzoek uitgevoerd naar de beheersing van het print- en mailproces. De conclusie van Logius is dat het print- en mailproces en de daaraan gerelateerde beheerprocessen bij de leverancier in voldoende mate invulling geven aan de daaraan gestelde eisen met betrekking tot de betrouwbaarheid en de beschikbaarheid. Ondanks verbeteringen in de vastleggingen van het ICT-beheer ten opzichte van 2009, is met name Access Management nog een punt van aandacht. Een nadere toelichting wordt hierna gegeven.

Primair proces

Het bronbestand met NAW-gegevens van de aanvragers van een DigiD inclusief de bijbehorende activeringscode wordt op veilige wijze aangeboden bij de print- en mailleverancier. Hiertoe wordt het bronbestand dagelijks op een beveiligde server bij de print- en mailleverancier geplaatst. Toegang tot deze server wordt vastgelegd. De leverancier draagt zorg voor het afdrukken en vervolgens verzenden van de activeringscodes naar de aanvragers op basis van de informatie in het bronbestand.

De print- en mailleverancier maakt gebruik van gecompartmenteerde ruimtes. Alleen geautoriseerde medewerkers krijgen, op basis van hun werkzaamheden, via verstrekte badges toegang tot deze ruimtes. Geprinte DigiD brieven voor aanvragers worden in de regel op de dag van productie verzonden. Indien dit, bij uitzondering, niet het geval is worden de DigiD brieven tot tijdstip van verzending opgeslagen in een afgesloten en beveiligde ruimte.

De juiste en volledige afhandeling van print- en mailopdrachten tijdens het productieproces wordt op geautomatiseerde wijze bewaakt. Dit gebeurt door de zogenoemde ADF-machine. In combinatie met een controle door de productieverantwoordelijke wordt de procesgang gewaarborgd. Tevens controleren de ADF-machine en de productieverantwoordelijke dat de DigiD brieven conform de specificaties van Logius zijn geprint. Daarna vindt de verdere verwerking van geprinte en goedgekeurde brieven of de vernietiging van afgekeurde brieven plaats. Vervolgens draagt de leverancier zorg voor verzending. De leverancier rapporteert periodiek aan Logius over onder andere over het aantal geprinte en verzonden brieven en eventuele incidenten.

Generieke beheersaspecten

De generieke beheersaspecten die mede relevant zijn voor de DigiD dienstverlening hebben de aandacht van de print- en mailleverancier. Ten opzichte van de bevindingen over 2009 zijn in 2010 verbeteringen zichtbaar. Het kwaliteitshandboek van de print- en mailleverancier is aangevuld met nieuwe procedures en in 2010 is het draaiboek voor DigiD verder uitgewerkt. De print- en mailleverancier streeft naar een eenduidige werkwijze op al haar locaties.

Een reeds in 2010 in gang gezette ontwikkeling bij de print- en mailleverancier is dat de ICT-beheerprocessen worden uitbesteed aan een externe partij. De print- en mailleverancier streeft met deze uitbesteding naar een verdere professionalisering van haar ICT-beheerprocessen. De uitbesteding omvat onder meer de generieke beheersaspecten en de beheerprocessen Availability Management, Continuity Management en Access Management. De outsourcing van de ICT-beheerprocessen zal volgens planning in mei 2011 geëffectueerd zijn.

Wat betreft de sturing en beheersing van ICT-beheerprocessen is in hoofdlijnen vastgelegd op welke wijze controle van de ICT-beheerprocessen plaatsvindt. De print- en mailleverancier geeft aan dat ook in 2010 om pragmatische redenen is gekozen voor ad hoc controle, waarneming ter plaatse door of namens het hoofd ICT, van naleving van ICT-beheerprocessen. Van deze controles zijn vastleggingen beschikbaar.

De print- en mailleverancier geeft voldoende invulling aan de voor de DigiD dienstverlening relevante generieke beheersaspecten. Punt van aandacht is de outsourcing van ICT-beheerprocessen. Het is van belang dat de print- en mailleverancier na outsourcing aantoonbaar "in control" is en blijft over de uitbesteede ICT-beheerprocessen.

Availability Management

In het productieproces (de verwerking van DigiD bestanden) hebben zich in 2010 geen ernstige verstoringen in de DigiD dienstverlening voorgedaan. Over de uitkomsten van de verwerking wordt geautomatiseerd aan Logius gerapporteerd middels zogeheten verwerkingsdagbestanden.

Continuity Management

Het productieproces is sinds 2010 gecentraliseerd op locatie Leuven. Daar waar voorheen sprake was van twee verschillende netwerken op de locaties Leuven en Turnhout, zijn deze samengevoegd tot één netwerk, het NT-netwerk. In het geval van een calamiteit wordt uitgeweken naar de alternatieve locatie Turnhout, zodat de productie met minimale verstoring voortgang kan hebben.

Ten behoeve van het productieproces is in het draaiboek DigiD een hoofdstuk Disaster Recovery Plan opgenomen. De print- en mailleverancier heeft in december 2010 een (beperkte) uitwijktest op de alternatieve locatie in Turnhout uitgevoerd. Tijdens deze test is nagegaan of het printen en couverteren van DigiD brieven succesvol verloopt.

Access Management

Bij de print- en mailleverancier is Acces Management nog een punt van aandacht. De print- en mailleverancier heeft 2010 gebruikt om autorisaties inzichtelijk te krijgen. De print- en mailleverancier streeft ernaar om met de geplande outsourcing naar een externe partij in 2011 een geactualiseerde autorisatiematrix te implementeren, zodat gedurende het jaar de toegang van gebruikers (en hun rechten) tot servers, applicaties, mappen en bestanden kan worden gemonitord.

In 2010 heeft de print- en mailleverancier gebruik gemaakt van een autorisatiematrix op het niveau van zogenaamde "shares". Dit zijn gedeelde mappen en bestanden in het besturingssysteem Windows. Deze autorisatiematrix dient nog geactualiseerd en vervolgens geïmplementeerd te worden.

Toegang tot het netwerk met complexe wachtwoorden wordt afgedwongen. Gebruikers zijn ingedeeld volgens een bepaalde rol (taken, verantwoordelijkheden) op basis waarvan zij toegangsrechten hebben. In de praktijk worden autorisaties schriftelijk en/of per e-mail aangevraagd en toereikend afgehandeld en vastgelegd.

Alvorens een (externe) gebruiker toegang tot het netwerk van de print- en mailleverancier krijgt, wordt filtering van het netwerkverkeer door een firewall afgedwongen. De print- en mailleverancier voert dagelijks controle uit op verdachte activiteiten. Hiervoor wordt gebruik gemaakt van standaard automatisch door het netwerk en de firewall gegenereerde rapportages.

De uitwisseling van DigiD bronbestanden vindt door het gebruik van wachtwoorden en een firewall op een veilige wijze plaats. Aanvullend worden DigiD bronbestanden geplaatst op een apart beveiligde (SFTP-) server. De toegang tot deze server wordt gelogd en bewaakt. Toegang van buitenaf, de zogenaamde externe toegang, tot deze server is beperkt tot geautoriseerde systemen uit de DigiD (rekencentrum)omgeving van Logius.

Voor de afhandeling van het print- en mailproces hebben verschillende geautoriseerde interne gebruikers toegang tot de DigiD bronbestanden. Het benaderen hiervan wordt door de print- en mailleverancier gelogd met behulp van een softwaretool. Over 2010 is vastgesteld dat de controleerbaarheid van de interne toegang tot de DigiD bronbestanden dient te worden verbeterd. Uit een in 2010 uitgevoerde interne controle op het systeembeheer zijn geen bijzonderheden gebleken.

In 2010 is via software op basis van certificaten verbinding gemaakt met de SFTP server. Het door de print- en mailleverancier gebruikte certificaat is afkomstig van een Certificate Authority. De public keys zijn uitgewisseld met DigiD. Het beheer van deze certificaten vindt plaats via de software Certificate Manager en is alleen toegankelijk via een beheerdersaccount. De SFTP server software kan op zich alleen opgestart worden na ingave van een wachtwoord.

3.3.3 *Callcenter*

Algemeen

Logius heeft de callcenteractiviteiten voor de eerste lijn DigiD ondersteuning uitbesteed aan een callcenterleverancier. Hiertoe is een overeenkomst afgesloten tussen Logius en de callcenterleverancier. Er is een onderzoek uitgevoerd naar de beheersing van het callcenterproces. De conclusie is dat het telefoonafhandelingsproces en de daaraan gerelateerde dienstverlening bij de callcenterleverancier in voldoende mate invulling geven aan de daaraan gestelde eisen met betrekking tot de betrouwbaarheid en de beschikbaarheid. Ondanks verbeteringen ten opzichte van 2009 zijn de ICT-beheerprocessen die de callcenterleverancier heeft uitbesteed, met name Access Management, nog steeds een punt van aandacht. Een nadere toelichting wordt hierna gegeven.

Primair proces

Het callcenter zorgt voor de afhandeling en/of routing van vragen, klachten en incidenten van eindgebruikers (burgers) over het gebruik van DigiD per telefoon en e-mail. Daarnaast beantwoordt het callcenter eenvoudige vragen van klanten (overheidsinstellingen) over de DigiD dienstverlening. Afhandeling van incidenten, vragen en klachten vindt plaats op basis van de DigiD kennisbank. Vragen die door het callcenter niet via deze kennisbank kunnen worden afgehandeld en klachten worden per e-mail doorgezet naar het Servicecentrum van Logius. Aanvullingen op de DigiD kennisbank worden uitgevoerd op basis van wijzigingsbeheerprocedures waarin de goedkeuring door Logius van een wijziging een onderdeel is. De medewerkers van het callcenter zijn verantwoordelijk voor het registreren, toewijzen en volgen van meldingen. Meldingen worden onder vermelding van een uniek ticketnummer geregistreerd. Ook wordt de fase van afhandeling van meldingen in een beheertool geregistreerd. De medewerkers worden gemonitord door leidinggevende, waarbij wordt vastgesteld dat calls en e-mailberichten tijdig en met voldoende deskundigheid worden afgehandeld. De inzet van de medewerkers wordt afgestemd op de door Logius verwachte en met de callcenterleverancier gecommuniceerde werklast voor DigiD.

Generieke Beheersaspecten

De voor de DigiD dienstverlening relevante beheerprocedures zijn beschreven. In 2010 hebben de callcenterleverancier en Logius een bewerkersovereenkomst opgesteld waarin afspraken zijn vastgelegd met betrekking tot de verwerking van persoonsgegevens. De callcenterleverancier heeft een procedure Vernietiging Persoonsgegevens. De registratie van persoonsgegevens is gewijzigd van 0,45% in 2009 naar 0,64% in 2010. Het gaat dan om 2060 van de in totaal 321.881 aanvragen. De callcenterleverancier gaat ervan uit dat deze verhoging toe te wijzen is aan de uitbreiding van de DigiD dienstverlening met het onderdeel Machtigen.

Het primaire proces van de callcenterleverancier, te weten het telefoonafhandelingsproces voor DigiD, is toereikend geborgd. Voor de ondersteuning van de DigiD dienstverlening wordt een specifieke applicatie (hierna: applicatie Primair Proces) gebruikt. Registratie van meldingen vindt hierin plaats. Iedere melding wordt uniek geïdentificeerd door een ticketnummer. Ook vermeldt deze vastlegging de status en de classificatie (vraag, klacht en verstoring). Daarnaast wordt gebruik gemaakt van een planningsapplicatie. In de applicatie Primair Proces worden de service levels continu gemonitord en op basis hiervan wordt aan Logius gerapporteerd.

De callcenterleverancier heeft in 2010 met een externe partij, tevens de leverancier van de applicatie Primair Proces, een contract afgesloten waarin de dienstverlening van deze externe partij aan de callcenterleverancier is vastgelegd. Het contract betreft ondermeer het beheer van de applicatie Primair Proces, de bijbehorende database en de DigiD kennisbank. In 2011 worden de gemaakte afspraken meer geoperationaliseerd om verdere aanvulling te geven aan Continuïteit/Uitwijk, Backup & Recovery, Toegangsbeveiliging en Autorisaties van de applicatie Primair Proces, de database en de DigiD kennisbank.

Continuity Management

De callcenterleverancier beschikt over een calamiteitenplan dat zich onder andere richt op de uitval van telefoons, databases en intranet. Het telefoonafhandelingsproces wordt geregistreerd om de applicatie Primair Proces. In 2010 hebben zich geen productiebelemmerende verstoringen voorgedaan.

Sinds medio mei maakt de callcenterleverancier voor haar telefonische dienstverlening gebruik van een ander callcenterplatform, geleverd door een externe leverancier (hierna: platformleverancier). De callcenterleverancier heeft een (concept) overeenkomst afgesloten met de platformleverancier voor levering, implementatie en onderhoud van het callcenterplatform. De platformleverancier garandeert een 99,98% beschikbaarheid per maand. In aanvulling daarop heeft de callcenterleverancier overeenkomsten met twee telefonie dienstverleners die een 99,9% beschikbaarheid van de keten voor de telefonische dienstverlening garanderen. De leverancier ontvangt periodiek rapportages hierover. De keten bestaat uit een contactcenter, de callmanager, het IP-netwerk en de (redundant uitgevoerde) verbindingen van het Cyber Center op Schiphol naar de verschillende locaties van de callcenterleverancier. Als een locatie onverhoopt mocht uitvallen, kunnen de diensten worden doorgeschakeld naar een andere locatie.

Capacity Management

Het inschatten, toewijzen en plannen van capaciteit gebeurt door de driemaandelijke werklastvoorspellingen afkomstig van Logius te matchen met de gemiddelde afhandelingstijd per callcentermedewerker. De realisatie van het tussen Logius en de callcenterleverancier overeengekomen service level voor de afhandeling van meldingen wordt geautomatiseerd bewaakt. Indien noodzakelijk kunnen extra callcentermedewerkers worden opgeroepen om de capaciteit uit te breiden. De callcenterleverancier heeft hierover afspraken gemaakt met uitzendbureaus.

De resultaten van de capaciteitsmetingen en -registraties worden maandelijks in het SNR-overleg tussen Logius en de callcenterleverancier besproken. Als er aanleiding toe is, vindt bijstelling plaats. Gedurende 2010 is geen sprake geweest van een tekort aan capaciteit.

Access Management

De callcenterleverancier heeft richtlijnen voor toegang van gebruikers tot systemen en applicaties, de uitgifte van wachtwoorden en toegangsrechten. Wanneer een medewerker de eerste keer toegang krijgt tot de applicatie Primair Proces moet een nieuw wachtwoord worden ingevoerd. Dit wordt afgedwongen door het netwerk. Een medewerker krijgt alleen toegang tot het netwerk en applicaties wanneer hij is geregistreerd in het personeelssysteem.

Medewerkers hebben alleen toegang tot de DigiD kennisbank via hun netwerkaccount. Medewerkers (onder andere teamleiders en medewerkers van het callcenter) hebben op basis van hun functie toegangsrechten. Medewerkers (behalve medewerkers van het callcenter) hebben persoonlijke accounts met een persoonlijk wachtwoord. Voor medewerkers van het callcenter is er een collectief account. Zowel teamleiders als medewerkers van het callcenter hebben alleen raadpleegrechten in de DigiD kennisbank. Hun activiteiten worden op de werkvloer tot op de minuut gelogd in de applicatie Primair Proces, daarnaast is er direct oogtoezicht door de teamleiders.

Wanneer een medewerker uit dienst gaat wordt dit geregistreerd in het personeelssysteem. Dit leidt tot het blokkeren van het netwerkaccount van de betreffende medewerker. Eens per maand worden de accounts van de medewerkers die uit dienst zijn getreden verwijderd.

De callcenterleverancier heeft nog geen volwaardige SLA met de externe partij die het beheer voert over de applicatie Primair Proces, de database en de DigiD kennisbank. Dit wordt door de callcenterleverancier onderkend en hiertoe zullen in 2011 nadere stappen worden ondernomen.

Incident Management

Alle calls worden gelogd. Medewerkers classificeren een melding naar vraag, klacht of incident. Dit wordt vastgelegd in de applicatie Primair Proces. Wanneer een vraag niet kan worden beantwoord op basis van de DigiD kennisbank, wordt de melding door middel van een genormaliseerde e-mail als incident doorgezonden naar Logius voor afhandeling. Logius bevestigt de ontvangst van de melding met het doorgeven van een meldingsnummer, waarna de melding door de callcenterleverancier als afgehandeld wordt beschouwd. Deze meldingen (incidenten) worden

maandelijks gerapporteerd in de SNR aan Logius en besproken in het serviceniveau overleg. Gedurende 2010 zijn geen productiebelemmerende incidenten aan de orde geweest in de periodieke overleggen tussen Logius en de callcenterleverancier.

3.3.4 *Ondersteuning SMS-authenticatie*

Algemeen

De DigiD dienstverlening omvat voor het 'zekerheidsniveau midden' authenticatie op basis van een combinatie van naam, wachtwoord en een per SMS-bericht verzonden code. De DigiD applicatie stelt het SMS-bericht beschikbaar aan de SMS-gateway (de ontvangstfaciliteit), waar het geconverteerd wordt naar het juiste formaat voor routing naar een SMS-centrale (de verzendfaciliteit). De verzendfaciliteit distribueert de SMS-berichten naar de netwerken van verschillende operators.

Voor de distributie van SMS-berichten inclusief het beschikbaar stellen en het beheren van de technische producten waarmee deze functionaliteit wordt gerealiseerd, is een overeenkomst afgesloten tussen Logius en een SMS-dienstverlener binnen de overheidsbrede mantelovereenkomst Overheidstelecommunicatie 2006 (OT2006). De SMS-dienstverlener maakt gebruik van een onderaannemer die het dagelijkse beheer uitvoert over de ontvangstfaciliteit.

Onderzoek SMS-dienstverlening

Bij de SMS-dienstverlening staan de volgende aspecten centraal: het vaststellen dat het verzendverzoek afkomstig is van de bevoegde instantie Logius; het volledig afhandelen van het verzendverzoek door middel van het verzenden van het SMS-bericht; het verantwoorden over de volledige en tijdige afhandeling van verzendverzoeken in de vorm van een end-to-end rapportage.

Mede op basis van deze uitgangspunten is onderzoek gedaan naar de beheersing van het SMS-proces. De conclusie is dat het SMS-proces en de daaraan gerelateerde beheerprocessen bij de SMS-dienstverlener in voldoende mate invulling geven aan de daaraan gestelde eisen. Een nadere toelichting wordt gegeven in de hierna volgende paragrafen.

Generieke beheersaspecten

De generieke beheersaspecten hebben de aandacht van de SMS-dienstverlener en zijn adequaat uitgewerkt. De relevante documenten zijn geactualiseerd. De uitkomsten per proces worden periodiek beoordeeld in relatie tot de afgesproken ICT-diensten, beleidsaspecten en dienstenniveaus. Logius heeft SNR's ontvangen van de SMS-dienstverlener over alle maanden in 2010. In deze rapportages is inzichtelijk gemaakt dat een score van 100% is behaald voor de verschillende prestatie-indicatoren.

Capacity Management

Logius en de SMS-dienstverlener hebben de afspraken over capaciteitsbeheer vastgelegd in een SNO en Dossier Afspraken Procedures (DAP, horend bij SNO). Indien er redenen zijn om de capaciteit van de verzendfaciliteit te verhogen, wordt er door Logius een serviceaanvraag ingediend bij de SMS-dienstverlener. De belasting van de

infrastructuurcomponenten wordt doorlopend aan de hand van monitoringsystemen bewaakt. Uit onderzoek blijkt dat zich geen problemen hebben voorgedaan met capaciteitsbeheer.

Availability Management

De afspraken over beschikbaarheidsbeheer zijn vastgelegd in de SNO en het DAP tussen Logius en de SMS-dienstverlener. De beschikbaarheid wordt realtime getest in de productie. De beschikbaarheid wordt continu gemonitord. Verschillende verstoringen hebben zich voorgedaan, veelal bij de SMS-dienstverlener. In alle gevallen is adequaat gehandeld en met succes is uitgeweken naar een redundante verzendfaciliteit. Prestaties met betrekking tot beschikbaarheid zijn vermeld in de maandrapportages. In 2010 was de beschikbaarheid van redundant uitgevoerde ontvangstfaciliteit en de redundant uitgevoerde verzendfaciliteit 100%.

Continuity Management

In de SNO en het DAP zijn afspraken gemaakt met de SMS-dienstverlener over continuïteitsbeheer. Voor de ontvangstfaciliteit is een platform exclusief voor behandeling van DigiD verkeer geïmplementeerd door de onderaannemer te Amsterdam. Mocht dit platform onverhoopt niet beschikbaar zijn, dan kan het DigiD verkeer worden gerouteerd naar een ander platform van de onderaannemer. Op dit platform, dat zich bevindt in Utrecht, is de dienstverlening voor meerdere klanten van de onderaannemer operationeel. Indien de dienstverlening op het primaire platform langdurig niet ter beschikking is, treedt het calamiteitenplan in werking.

Voor de verzendfaciliteit is de SMS-centrale van de SMS-dienstverlener primair ingericht voor het verwerken van aangeboden SMS-berichten. Indien dit platform onverhoopt niet beschikbaar is, kan de onderaannemer het verkeer routeren via de SMS-centrale van een andere Nederlandse mobiele operator. Indien de SMS-centrale van de SMS-dienstverlener langdurig niet meer beschikbaar is, treedt het rampenplan (onderdeel van OT2006) in werking. Gedurende deze situatie is de dienstverlening voor DigiD beperkt tot de condities beschreven in de SNO.

Tijdens het onderzoek is vastgesteld dat er zich geen problemen hebben voorgedaan met continuïteitsbeheer. Bij verstoringen is met succes uitgeweken naar de redundante verzendfaciliteit.

Access Management

Een actuele, gedocumenteerde en door het management van de ICT-dienst geaccordeerde autorisatiematrix is beschikbaar. Unieke identiteitskenmerken (zoals gebruikersnamen en pasjes) worden toegekend aan gebruikers na controle van de identiteit en na goedkeuring door de lijnmanager en het management van de ICT-dienst. Aan gebruikers worden individuele en geheime toegangssleutels (zoals wachtwoorden) uitgegeven zodanig dat de sleutels niet in handen komen van ongeautoriseerde gebruikers. Toegangsrechten worden gedeactiveerd of ingetrokken nadat van deze rechten gedurende een vastgestelde periode geen gebruik is gemaakt. In de technische infrastructuur en de fysieke omgeving hiervan zijn voldoende preventieve, detectieve en correctieve maatregelen getroffen om de autorisatiematrix en de controle hierop te effectueren.

Overige normen

De primaire ontvangsfaciliteit is een dedicated resource van DigiD. Daardoor kan worden gerapporteerd over het aantal aangeboden berichten. De secundaire ontvangsfaciliteit is een shared resource en daar is van oorsprong geen rapportagemogelijkheid voor aangeboden berichten. Rapporteren op de secundaire locatie is alleen mogelijk op afgeleverde berichten op de verzendfaciliteit. Over de aangeboden en afgeleverde berichten tussen ontvangst- en verzendfaciliteit wordt maandelijks gerapporteerd. SMS-berichten die door de onderaannemer naar de provider zijn verzonden, sluiten volledig aan op de berichten die door het Servicecentrum van Logius aan de onderaannemer zijn verstrekt.

Er is inzicht in de SMS-berichten die niet aangekomen zijn bij de eindgebruiker (bijvoorbeeld door verkeerd ingestelde telefoonparameters). Hierover rapporteert de provider wekelijks aan Logius.

Het HTTPS-verkeer is beveiligd met een PKI-overheid Secure Sockets Layer (SSL-)certificaat. Dit certificaat is ondertekend door een PKI-overheid Certificate Authority. Logius is primair verantwoordelijk voor het verlengen van de PKI-overheid certificaten. De technisch beheerders van de servers waarop de certificaten van DigiD geïnstalleerd zijn, houden een lijst met de geldigheid van de certificaten bij. Indien geen nieuwe certificaten ontvangen worden, wordt hiervan melding gemaakt bij Logius, die de certificaten aanvraagt en oplevert.

3.4 Dienstspectifieke beheersingsmaatregelen DigiD

Het functioneren van de dienstspectifieke maatregelen in en rondom DigiD geeft in opzet, bestaan en werking voor de onderzoeksperiode voor de meeste onderdelen voldoende invulling aan de beheersdoelstellingen. Een aantal bevindingen is aanwezig waaraan een middenrisico is gekoppeld. Met deze bevindingen wordt afgeweken van de norm die is gebaseerd op de controledoelstellingen. Op een aantal van deze bevindingen wordt individueel of in samenhang ingegaan inclusief de bijbehorende aanbevelingen.

In en rondom het DigiD systeem is een aantal handmatige en geprogrammeerde controlemaatregelen getroffen dat gezamenlijk het betrouwbaar functioneren van de authenticatiedienst mogelijk maakt.

Voorbeelden zijn:

- maatregelen rondom de veilige uitgifte van de DigiD inlogcode, zoals bijvoorbeeld een automatische controle van adresgegevens aan de hand van de GBA-V (Gemeentelijke Basis Administratie Verstrekkingen) of SVB-register (register van de Sociale Verzekeringsbank voor niet ingezetenen) en de veilige verzending van de activeringscodes aan burgers;
- de toepassing van een veilig protocol om authenticatie van burgers te laten plaatsvinden op basis van een DigiD inlogcode, eventueel uitgebreid met SMS-authenticatie;
- beveiligingsmaatregelen in de DigiD applicatie, zoals wachtwoordcontrole, inputvalidatie, sessiemanagement en versleuteling van vertrouwelijke gegevens;
- vastlegging van loggegevens over handelingen van gebruikers en beheerders.

3.4.1 *Wijze inloggen beheerders*

De beheerders van DigiD bij Logius kunnen inloggen met gebruikersnaam en wachtwoord zonder verder gebruik te maken van een token of vergelijkbare maatregel. Dit is in afwijking van de norm. De auditor heeft geadviseerd "ervoor te zorgen dat beheertoegang tot DigiD alleen mogelijk is met 'kennis' (=wachtwoord) en 'bezit' (= b.v. token). Het ligt hierbij voor de hand gebruik te maken van de PKI smartcards die bij Logius aanwezig zijn". In 2011 gaat DigiD 4.0 in productie. Daarbij wordt bovenstaande maatregel gerealiseerd.

3.4.2 *Applicatielogging DigiD*

Algemeen beeld op basis van onderzoek is dat de applicatielogging inclusief de geautomatiseerde en handmatige analyse/afhandeling hiervan vanuit beveiligingsperspectief verbetering behoeven. Logius zal met de productiegang van DigiD 4.0 de verbeterpunten zoveel mogelijk oplossen.

3.4.3 *Toepassen cryptografie*

Voor de huidige DigiD 2.x lijn wordt in afwijking van de norm geen gecertificeerde cryptografische bibliotheek gebruikt. Logius gaat verbeteringen aanbrengen in de gebruikte cryptotechnieken. Bij de ontwikkeling van DigiD 4.0 wordt gebruik gemaakt van een open source bibliotheek en open source cryptografie.

3.5 **Naleving wet- en regelgeving**

Het blijvend voldoen aan wet- en regelgeving wordt geborgd door onder meer bij wijzigingen van DigiD 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 DigiD en Haagse Ring 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 checklist door L&C/JZ bijgewerkt voor de producten waarover Assurance wordt afgegeven. De bewerkersovereenkomsten zijn afgerond en ondertekend. Voor de nieuwbouw van DigiD is de bewerkersovereenkomst reeds meegenomen bij de Europese aanbesteding.

3.6 **Conclusie**

De DigiD dienstverlening voldoet over het algemeen aan de daaraan gestelde eisen. Ten opzichte van controlejaar 2009 is met de implementatie van een nieuwe IT-Infrastructuur een behoorlijke stap gezet.

Wel is vastgesteld dat met het aanwezige stelsel van beheermaatregelen voor het product DigiD in de onderzoeksperiode op een beperkt aantal punten nog niet voldoende invulling is gegeven aan alle afgesproken normen. De belangrijkste punten hebben te maken met de logging van het gebruik van de applicatie van DigiD. Het betreft zowel de bewaking en analyse van afwijkingen als de verdere afhandeling van de afwijkingen.

Logius heeft geen aanwijzing dat genoemde punten in de Verantwoordingsperiode negatieve gevolgen hebben gehad voor de DigiD dienstverlening.

Het functioneren van de dienstspecifieke maatregelen in en rondom DigiD geeft in opzet, bestaan en werking voor de onderzoeksperiode een aantal bevindingen weer waaraan een middenrisico is gekoppeld. De verbeteringen worden of nog in de huidige versie van DigiD doorgevoerd of pas wanneer de nieuwe versie DigiD 4.0 in productie genomen wordt.

4 Bevindingen Haagse Ring

4.1 Algemeen

Haagse Ring is een netwerk voor datatransport tussen de aangesloten netwerken van:

- de 'aangesloten organisaties' en de daaronder ressorterende baten-/lastendiensten (waarbij is afgesproken dat de aangesloten organisaties zorgen voor de koppeling van deze diensten);
- de Hoge Colleges van Staat (voor zover zij dat wensen) en andere direct aan de rijksoverheid gelieerde organisaties;
- externe leveranciers van diensten/services aan de aangesloten organisaties.

Logius is verantwoordelijk voor het tactische aansluitproces op Haagse Ring. De juiste en volledige uitvoering van het aansluitproces en de generieke tactische processen vormt één van de randvoorwaarden voor de betrouwbare werking van Haagse Ring.

Binnen Haagse Ring wordt gebruik gemaakt van virtuele private netwerken (VPN's) waarmee naar wens verbindingen tussen aangesloten organisaties kunnen worden gerealiseerd. In december 2010 waren 20 VPN's beschikbaar op Haagse Ring.

In dit hoofdstuk wordt ingegaan op de uitvoering van de taken van Logius met betrekking tot Haagse Ring in de onderzoeksperiode.

4.2 Rolverdeling en inrichting beheer

De basis voor Haagse Ring is een mantelovereenkomst tussen alle 'aangesloten organisaties', Logius en de bedrijfsgroep Informatievoorziening en -technologie (IVENT) van het Commando Diensten Centrum van het ministerie van Defensie. Het ministerie van BZK is de bestuurlijke opdrachtgever van Haagse Ring.

IVENT is opdrachtnemer voor Haagse Ring en realiseert de daadwerkelijke dienstverlening inclusief het technisch en operationeel beheer. Logius is verantwoordelijk voor het bewaken van de dienstverlening van IVENT, het tactische wijzigingenbeheerproces voor aansluitingen en werkzaamheden op het gebied van behoeftemanagement en het tactisch security management.

Logius vult de bewaking van de dienstverlening van IVENT in door maandelijks kennis te nemen van de geleverde rapportages en hierover, indien daar aanleiding toe is, nadere informatie te vragen. Ook worden de rapportages in een samenwerkingsruimte op Rijksweb geplaatst, zodat de 'aangesloten organisaties' hiervan kennis kunnen nemen. Verder neemt Logius deel aan het platform Connectiviteit, mede om haar rol voor Haagse Ring invulling te geven. Dit platform richt zich op de kennisuitwisseling en afstemming bij de ontwikkelingen rond de connectiviteit bij de (Rijks)overheid.

Het onderzoek heeft zich gericht op de verantwoording naar de (beperkte) taken van Logius rondom Haagse Ring zoals vastgelegd in de contractuele

afspraken en onderliggende documenten. Algemeen beeld is dat het wijzigingenbeheerproces toereikend is ingevuld.

Een proactieve bewaking van de inrichting van Haagse Ring is bij Logius niet ingericht. Logius ziet niet direct grote risico's voortkomen uit het ontbreken van de bewakingsfunctie.

Het periodiek vaststellen dat relevante en actuele kaders aanwezig zijn voor het uitvoeren van het aansluitbeheerproces is toereikend ingevuld. Zo heeft Logius in september 2010 aan SIB/DGOBR een notitie voorgelegd met de vraag of de werkwijze van Logius met betrekking tot handhaving van de aansluitvoorwaarden nog voldoet. Logius heeft daarbij een voorstel gedaan voor wijziging van de rolverdeling en aansluitvoorwaarden uitgebracht aan SIB/DGOBR. Er is nog geen reactie ontvangen op de voorstellen gericht aan SIB/DGOBR betreffende de invulling van de bewakingsfunctie van Logius, waardoor het risico bestaat dat Logius aangesproken wordt op de discrepantie tussen oude kaders en huidige werkwijze, die nog niet is geformaliseerd. Deze formalisatie zal in 2011 plaatsvinden.

4.3 Informatiebeveiliging Haagse Ring

In de afspraken voor Haagse Ring met IVENT is opgenomen dat het standaard beveiligingsniveau van Haagse Ring 'departementaal vertrouwelijk' is, zoals bedoeld in het VIR-BI. Voor de realisatie hiervan wordt vertrouwd op IVENT. Met IVENT is niet afgesproken dat zij zich over het voor Haagse Ring gerealiseerde beveiligingsniveau verantwoordt middels bijvoorbeeld een rapportage. De werkzaamheden van Logius hebben geen directe relevantie voor het informatiebeveiligingsniveau van Haagse Ring en aangesloten partijen aangezien Logius niet is betrokken bij het technisch en operationeel beheer. Het enige raakvlak is het aansluitingenbeheerproces van Logius waarbij het foutief doorgeven van wijzigingen kan leiden tot onbedoelde verbindingen of verstoringen.

4.4 Conclusie

Logius is verantwoordelijk voor het tactisch beheer van Haagse Ring. De beheersmaatregelen voor het tactisch beheer van Haagse Ring worden in voldoende mate uitgevoerd. De formalisatie van de mogelijke nieuwe kaders voor rolverdeling en aansluitvoorwaarden, in najaar 2010 voorgelegd aan SIB/DGOBR, wordt in 2011 doorgevoerd.

Bijlage I Lijst met afkortingen

ADF	Automatic Document Feeder
BiSL	Business Information Services Library
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CCB	Change Control Board
CSDM	Continuous Service Delivery Mode
DAP	Dossier Afspraken en Procedures
DigiD	Digitale Identiteit
FTP	File Transfer Protocol
ICT	Informatie- en Communicatietechnologie
HTTPS	Secure Hypertext Transfer Protocol
IT	Informatietechnologie
ITIL	Information Technology Infrastructure Library
IVENT	De bedrijfsgroep Informatievoorziening en -technologie van het Commando Diensten Centrum van het ministerie van Defensie
GBA-V	Gemeentelijke Basis Administratie Verstrekkingen
L&C/JZ	Leveranciers- en Contractmanagement/Juridische Zaken
NAW	Naam, adres en woonplaats
MT	Management Team
OT2006	Overheidstelecommunicatie 2006
PID	Project Initiation Document
RAD	Rijksauditdienst
RFC	Request For Change
SIB/DGOBR	Subcommissie Informatiebeveiliging van de Interdepartementale Commissie van CIO's (ICCIO)/Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
SMS	Short Message Service
SNO	Service Niveau Overeenkomst
SNR	Service Niveau Rapportage
SSL	Secure Sockets Layer
SVB	Sociale Verzekeringsbank
VIR	Voorschrift Informatiebeveiliging Rijksoverheid
VIR-BI	Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie
VPN	Virtual Private Network

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.

DigiD specifiek

- Het stelsel van application en user controls waarborgt het betrouwbaar functioneren van de authenticatiedienst DigiD in overeenstemming met wet- en regelgeving op het voorgeschreven niveau (WBP gegevensklasse II en Tijdelijk besluit nummergebruik overheidstoegangsvoorziening).
- Het stelsel van application en user controls bestaat uit het authenticatieprotocol inclusief de bijbehorende cryptografie en geautomatiseerde en handmatige procedures en (controle)maatregelen. Het protocol is logisch sluitend en maakt gebruik van algemeen aanvaarde (cryptografische) standaarden. Het voorziet in een veilige en betrouwbare authenticatie via Internet. De gegevens die binnen DigiD worden opgeslagen dienen door de getroffen maatregelen te worden beschermd.
- De authenticatievoorziening biedt de mogelijkheid belanghebbenden volledig en juist te informeren over de prestaties inclusief de werking van de controles.

Operationeel beheer DigiD

Beheersdoelstellingen Beheer infrastructuur DigiD

Generieke Beheersaspecten

- Het proces dient beheersbaar te zijn.
- Het proces dient controleerbaar te zijn.
- Belanghebbenden dienen juist en volledig over het proces te zijn geïnformeerd.

Service Level Management

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

Security Management

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

Capacity Management

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

Availability Management

- De ICT-dienst dient onder normale bedrijfsomstandigheden te voldoen aan het overeengekomen niveau van beschikbaarheid.

Continuity Management

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

Infrastructure Management

- Beheer: De instellingen van de ICT-middelen dienen overeen te komen met het geautoriseerde ontwerp.
- Beheer: Pogingen tot ongeautoriseerde toegang tot ICT-middelen dienen tijdig te zijn gedetecteerd.
- Infra: Er dient een stelsel te zijn geïmplementeerd waarin voorzien is in (passieve en actieve) security monitoring. Dit betekent ondermeer dat er procedurele en technische maatregelen dienen te zijn getroffen die bij voortdurende integriteit van het beveiligingsontwerp waarborgen. Daarnaast dienen bij afwijkingen op het beveiligingsontwerp toereikende acties te worden ondernomen;
- Infra: De integriteit van opgeslagen logbestanden dient te zijn gewaarborgd (security logmanagement). Alle beveiligingskritieke gebeurtenissen worden gelogd en inbreuken op het beoogde niveau van security (blijkend uit het beveiligingsontwerp) worden gedetecteerd, geanalyseerd en toereikend afgehandeld.
- Infra: De database van de DigiD applicatie dient te allen tijde betrouwbare data te bevatten;
- Ingeval van verstoringen en calamiteiten dient de dienstverlening aan de burger in korte tijd hersteld te kunnen worden. Alle kritieke componenten van de DigiD dienstverlening dienen bij voortdurende gemonitord te worden.

Access Management

- Beheer: Toegang tot ICT-diensten en -middelen dient te zijn beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers.
- Infra: Personen buiten de beheerorganisatie mogen geen enkele toegang hebben tot de DigiD systemen en data anders dan voor de DigiD dienstverlening noodzakelijk is;
- Infra: Toegangsrechten van beheerders moeten zoveel mogelijk beperkt worden ("het customizen van beheerrechten"). Alle beveiligingskritieke handelingen van beheerders moeten gelogd worden. Pogingen van beheerders tot misbruik moeten detecteerbaar en traceerbaar zijn naar uitvoeringsverantwoordelijke personen.

Configuration Management

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

Change Management

- Wijzigingen dienen te zijn geautoriseerd met inachtneming van de risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-diensten.
- Wijzigingen dienen tijdig en volledig te zijn doorgevoerd.
- Wijzigingen dienen effectief te zijn.

Incident Management

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

Problem Management

- Problemen dienen tijdig en volledig te zijn gesignaleerd en afgehandeld.

Operations Management

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

Beheersdoelstellingen Print- en maildienstverlening DigiD

Generieke Beheersaspecten

- Het proces van DigiD dienstverlening door de leverancier dient beheersbaar te zijn.
- Het proces van DigiD dienstverlening door de leverancier dient controleerbaar te zijn.
- Belanghebbenden dienen juist en volledig over het proces van DigiD dienstverlening te zijn geïnformeerd.

Availability Management

- De DigiD dienstverlening door de leverancier dient onder normale bedrijfsomstandigheden te voldoen aan het overeengekomen niveau van beschikbaarheid.

Continuity Management

- De DigiD dienstverlening door de leverancier dient in het geval van een calamiteit tijdig herstelbaar te zijn.

Access Management

- Toegang tot de DigiD dienstverlening door de leverancier dient te zijn beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers.

Beheersdoelstellingen Callcenter DigiD

Generieke Beheersaspecten

- Het proces van DigiD dienstverlening door de leverancier dient beheersbaar te zijn.
- Het proces van DigiD dienstverlening door de leverancier dient controleerbaar te zijn.
- Belanghebbenden dienen juist en volledig over het proces van DigiD dienstverlening te zijn geïnformeerd.

Continuity Management

- De DigiD dienstverlening door de leverancier dient in het geval van een calamiteit tijdig herstelbaar te zijn.

Capacity management

- De DigiD dienstverlening door de leverancier dient de overeengekomen werklast te kunnen verwerken.

Access Management

- Toegang tot de DigiD dienstverlening door de leverancier dient te zijn beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers.

Incident management

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

Beheersdoelstellingen SMS-authenticatie DigiD

Generieke Beheersaspecten

- Het proces dient beheersbaar te zijn;
- Het proces dient controleerbaar te zijn;
- Belanghebbenden dienen juist en volledig over het proces te zijn geïnformeerd.

Capacity Management

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

Availability Management

- De ICT-dienst dient onder normale bedrijfsomstandigheden te voldoen aan het overeengekomen niveau van beschikbaarheid.

Continuity Management

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

Access Management

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

Haagse Ring

Beheersdoelstellingen Haagse Ring

- Informatie voor het tactisch aansluitingenbeheerproces zoals gebruikers/aansluitingen, geautoriseerde medewerkers van gebruikers, VPN's en opdrachten aan de leverancier dient juist en volledig te zijn vastgelegd en te zijn beschermd tegen ongeautoriseerde kennisname.
- Het tactisch aansluitingenbeheerproces draagt op beheersbare en controleerbare wijze zorg voor de vertaling van gebruikersverzoeken in opdrachten aan de leverancier waarmee wordt bijgedragen aan de betrouwbaarheid en beschikbaarheid van Haagse Ring.