



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

TPM en Verantwoording 2009 Producten van Logius

DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid

Datum 30 maart 2010
Status Definitief

Colofon

Projectnaam	TPM 2009
Versienummer	1.0
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 servicecentrum@logius.nl
Bijlage(n)	Lijst van afkortingen
Auteurs	Verantwoording: Logius TPM: Rijksauditdienst

Inhoud

Colofon	2
Inhoud	3
Woord vooraf	5
1 Third Party Mededeling	6
2 Managementsamenvatting	9
3 Inleiding	11
3.1 <i>Algemeen</i>	11
3.2 <i>Normstelling</i>	12
3.3 <i>Totstandkoming</i>	12
3.4 <i>Leeswijzer</i>	12
4 Bevindingen DigiD voor Burgers	13
4.1 <i>Algemeen</i>	13
4.2 <i>Tactisch beheer</i>	13
4.3 <i>Operationeel beheer</i>	17
4.3.1 <i>Logius Apeldoorn</i>	17
4.3.2 <i>Beheer infrastructuur DigiD (rekencentrum)</i>	18
4.3.3 <i>Print & mail</i>	23
4.3.4 <i>Callcenter</i>	25
4.3.5 <i>Ondersteuning SMS Authenticatie</i>	28
4.4 <i>Dienstspectifieke beheersingsmaatregelen DigiD voor Burgers</i>	30
4.5 <i>Naleving wet- en regelgeving</i>	33
4.6 <i>Conclusie</i>	34
5 Bevindingen Digipoort	35
5.1 <i>Algemeen</i>	35
5.2 <i>Tactisch beheer</i>	35
5.3 <i>Operationeel beheer</i>	35
5.3.1 <i>Context</i>	35
5.3.2 <i>Mededeling externe leverancier Digipoort</i>	36
5.3.3 <i>Logius Apeldoorn</i>	36
5.4 <i>Dienstspectifieke beheersingsmaatregelen Digipoort</i>	36
5.5 <i>Naleving wet- en regelgeving</i>	37

5.6	<i>Conclusie</i>	37
6	Bevindingen Haagse Ring	38
6.1	<i>Algemeen</i>	38
6.2	<i>Rolverdeling en inrichting beheer</i>	38
6.3	<i>Informatiebeveiliging Haagse Ring</i>	39
6.4	<i>Aansluitingenbeheer</i>	39
6.5	<i>Conclusie</i>	40
7	Bevindingen PKIoverheid	41
7.1	<i>Algemeen</i>	41
7.2	<i>Certificaatautoriteit en -dienstverleners</i>	41
7.3	<i>Audit certificaatautoriteit</i>	42
7.4	<i>Conclusie</i>	42
	Bijlage I Lijst met afkortingen	43

Woord vooraf

Met genoegen bied ik u hierbij de verantwoording over de betrouwbaarheid van de producten DigiD voor Burgers, Digipoort, Haagse Ring (onderdeel van Diginetwerk) en PKIoverheid aan. Deze verantwoording heeft betrekking op de periode 1 januari 2009 tot en met 31 december 2009. De verantwoording gaat in op de opzet, het bestaan en de werking van DigiD voor Burgers, Digipoort en PKIoverheid en op de opzet en bestaan van Haagse Ring.

Sinds 1 januari 2006 is 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. Een groeiend aantal klanten binnen en buiten de Rijksoverheid maakt gebruik van deze producten. Hun bedrijfsvoering is afhankelijk van de betrouwbaarheid van deze producten. Om aan deze klanten aantoonbaar zekerheid te verschaffen over de betrouwbaarheid van de dienstverlening heb ik aan de Rijksauditedienst verzocht om jaarlijks een Third Party Mededeling (TPM) af te geven bij de verantwoording van Logius. Met het jaarlijks vragen van een TPM streeft Logius ernaar haar producten continu te verbeteren. Dat past binnen ons kwaliteitsbeleid dat richting geeft aan de wijze waarop Logius haar organisatie op orde heeft.

In het afgelopen jaar heeft Logius een flinke stap voorwaarts gemaakt ten aanzien van de inrichting van haar beheerprocessen. In overleg met de leveranciers zijn actieplannen opgesteld om de verbeterpunten op te lossen. De voortgang van de uitvoering van de actieplannen wordt periodiek bewaakt door het managementteam van Logius en gerapporteerd aan haar eigenaar (BZK) en de Programmaraad. Opvolging van verbeterpunten wordt eveneens meegenomen in de verantwoording over 1 januari 2010 tot en met 31 december 2010. De voorbereidingen voor de verantwoording 2010 zijn inmiddels gestart.

Met vriendelijke groet,

A handwritten signature in black ink, appearing to read 'S. Luitjens', with a long horizontal stroke extending to the right.

Steven Luitjens
Directeur Logius



1 Third Party Mededeling

Assurance-rapport

Geadresseerde

Dit assurance-rapport is bestemd voor de huidige en potentiële afnemers van de voorzieningen DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid van Logius. Het rapport dient uitsluitend in samenhang met de verantwoording over de voorzieningen van Logius, periode 1 januari – 31 december 2009 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 15 juli 2009 met kenmerk RAD 2009-457 hebben wij de verantwoording van Logius van 30 maart 2010, waarin de in de periode 1 januari t/m 31 december 2009 beoogde en geïmplementeerde maatregelen en procedures bij Logius en betrokken leveranciers zijn opgenomen ter waarborging van de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van de voorzieningen DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid, 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 normen (op te vragen bij Logius). Deze normen sluiten aan op algemeen aanvaarde normen en op de contracten tussen Logius en leveranciers. Logius heeft zorg gedragen voor de afstemming van deze normen met een vertegenwoordiging van haar Programmaraad. De normen zijn verder 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 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 waarbij op onderdelen gebruik is gemaakt van de mededeling van de externe leverancier m.b.t. Digipoort en het Webtrust certificaat van PKIoverheid;
- het onderzoeken van de toereikendheid van de informatie in de verantwoording, mede gelet op de informatiebehoeften van de huidige en potentiële afnemers van de voorzieningen 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

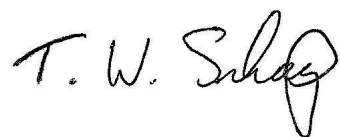
Op grond van ons onderzoek zijn wij van oordeel dat de in de verantwoording van Logius opgenomen informatie over de beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid van de voorzieningen DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid bij Logius en leveranciers betreffende het tijdvak 1 januari 2009 t/m 31 december 2009 juist en volledig is.

Toelichting op het oordeel

De voorzieningen DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid zijn bouwstenen voor de realisatie van betrouwbare digitale diensten. Organisaties dienen zich ervan bewust te zijn dat toepassing 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 voorzieningen DigiD voor Burgers, Digipoort, Haagse Ring en PKIoverheid 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 Burgers. Voor nadere informatie verwijzen wij naar paragraaf 4.6 van de verantwoording.

Den Haag, 30 maart 2010
Rijksauditedienst

A handwritten signature in black ink, appearing to read 'T. W. Schaap'. The signature is written in a cursive style with a large, looped 'S' at the end.

ir. T.W. Schaap RE CISA
Auditmanager

2 Managementsamenvatting

Algemeen

Logius is verantwoordelijk voor het beheer en de verdere ontwikkeling van de producten DigiD voor Burgers (verder genoemd: DigiD), Digipoort (voorheen Overheidstransactiepoort koppelvlakken X.400 en SMTP), Haagse Ring (onderdeel van Diginetwerk) en PKIoverheid. Voor de klanten binnen de overheid en gelieerde organisaties is het betrouwbaar en veilig functioneren van deze producten van groot belang voor hun bedrijfsvoering. Met de verantwoording inclusief de Third Party Mededeling geeft Logius aanvullende zekerheid aan haar klanten over de kwaliteit van haar producten.

De verantwoording van Logius is gebaseerd op de uitkomsten van onderzoeken naar de producten DigiD, Digipoort, Haagse Ring en PKIoverheid. Deze onderzoeken zijn in de periode 1 januari 2009 tot en met 28 februari 2010 uitgevoerd. De in de verantwoording beschreven situatie heeft - tenzij anders vermeld - betrekking op de periode 1 januari 2009 tot en met 31 december 2009. De onderzoeken zijn uitgevoerd aan de hand van normenkaders met als doel een objectief beeld te kunnen geven van de kwaliteit van de producten. Voor het opstellen van de normenkaders is gebruik gemaakt van wet- en regelgeving, contracten met leveranciers en algemeen aanvaarde standaarden. De directeur van Logius heeft het normenkader vastgesteld na afstemming met een vertegenwoordiging van de Programmaraad Logius.

DigiD voor Burgers

Voor DigiD voor Burgers is het beeld dat in vergelijking met het controlejaar 2008 de controleerbaarheid van de IT-infrastructuur en de kwaliteit van het ontwikkelproces in 2009 aanzienlijk zijn verbeterd. Daarbij komt dat 2009 moet worden beschouwd als een overgangsjaar. In 2009 is gebouwd aan een nieuwe IT-infrastructuur voor DigiD die in januari 2010 in productie is gegaan. De verwachting is dat deze IT-infrastructuur de beschikbaarheid van DigiD in 2010 verder zal verhogen. Voor 2009 is vastgesteld dat met het aanwezige stelsel van beheersingsmaatregelen voor het product DigiD in de periode 1 januari 2009 tot en met 31 december 2009 nog niet voldoende invulling is gegeven aan alle afgesproken normen. Het betreft concreet:

- de wijze waarop logbewaking en -analyse worden ingezet om afwijkingen te detecteren in het gebruik van DigiD, dient te worden verbeterd op de aspecten aantoonbare samenhang van de getroffen maatregelen en de pro-actieve uitvoering hiervan;
- eind 2009 is evenals in 2008 een beperkt aantal kwetsbaarheden ontdekt op het gebied van geprogrammeerde webapplicatiecontroles; hierop is adequaat gereageerd;
- de implementatie van het informatiebeveiligingsbeleid en -plan heeft niet voldoende aantoonbaar plaatsgevonden. De nadruk is blijven liggen op de beleidsfase. De invulling van de uitvoerings- en evaluatiefase op het gebied van informatiebeveiliging is nog niet voldoende.

In 2009 heeft Logius acties in gang gezet om deze punten op te pakken. Het eerste punt wordt waarschijnlijk pas definitief opgelost bij de geplande nieuwbouw van DigiD. Logius heeft de indruk dat genoemde punten in de verantwoordingsperiode negatieve gevolgen hebben gehad voor de DigiD dienstverlening.

Digipoort

Voor de huidige Digipoort omgeving is het beeld dat het stelsel van beheersingsmaatregelen in de verantwoordingsperiode een voldoende invulling aan het normenkader heeft gegeven. Een restrisico vormt het gegeven dat de ICT-infrastructuur van de huidige Digipoort omgeving, zoals geleverd door de externe leverancier, geen uitwijkfaciliteit bevat. Bij een calamiteit op de locatie van de externe leverancier zal Digipoort als geheel (tijdelijk) niet te gebruiken zijn. Met de nieuwe Digipoort omgeving die waarschijnlijk in het voorjaar van 2010 in gebruik wordt genomen, wordt ook dit risico ondervangen.

PKIoverheid

Voor PKIoverheid is vastgesteld dat de beheersmaatregelen bij de certificaatautoriteit in de verantwoordingsperiode in voldoende mate invulling hebben geven aan het normenkader.

Haagse ring

Haagse Ring is voor het eerst opgenomen in de verantwoording van Logius. Conform de standaard werkwijze van Logius wordt over Haagse Ring gerapporteerd naar de stand van 31 december 2009. Het beeld op hoofdlijnen is dat de beheersmaatregelen voor Haagse Ring bij Logius voldoende zijn ingevuld. Het betreft hier met name het aansluitingenbeheer op tactisch niveau voor Haagse Ring. Een belangrijk voornemen van Logius is om in de eerste helft van 2010 het Referentiekader Informatiebeveiliging Haagse Ring voor te leggen aan het Informatiebeveiligingsberaad met de vraag of met het huidige gebruik van dit kader de belangrijkste risico's van Haagse Ring in voldoende mate worden afgedekt.

3 Inleiding

3.1 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. Vier belangrijke producten aangeboden door Logius zijn:

- DigiD voor Burgers; dit staat voor Digitale identiteit van burgers en is een gemeenschappelijk authenticatiesysteem van en voor overheidsinstellingen waarmee zij de identiteit van eindgebruikers die gebruik maken van hun elektronische diensten kunnen verifiëren;
- Digipoort; dit is het elektronische postkantoor voor bedrijven voor het snel en efficiënt uitwisselen van informatie met een aantal overheidsinstellingen;
- PKIoverheid; met behulp van de Public Key Infrastructure overheid is het mogelijk de informatie die personen en organisaties over het internet sturen te beveiligen op een hoog niveau van betrouwbaarheid;
- Haagse Ring; is 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 product van Logius beperkt zich tot de uitvoering van onderdelen van het tactisch beheer voor Haagse Ring. Haagse Ring is onderdeel van Diginetwerk.

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 Third Party Mededeling (TPM). Een TPM is een mededeling van een auditor (register accountant of register EDP-auditor) waarin in dit geval een uitspraak wordt gedaan over de juistheid en volledigheid van de verantwoording.

Logius heeft de Rijksauditdienst (verder aangeduid als 'de auditor') gevraagd deze jaarlijkse TPM te verzorgen. De verantwoording gaat in op de opzet, het bestaan en de werking van drie van de vier genoemde producten gedurende het jaar 2009. Uitzondering is Haagse Ring. Aangezien Haagse Ring voor de eerste maal in de verantwoording wordt opgenomen, wordt gerapporteerd over opzet en bestaan per 31 december 2009.

3.2 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 op hoofdlijnen aan welke eisen de producten moeten 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 (WBP), 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 (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 vastgesteld na afstemming met een vertegenwoordiging van de Programmaraad.

3.3 Totstandkoming

De auditor heeft op basis van de normenkaders onderzoeken uitgevoerd bij Logius (vestiging Den Haag en vestiging Apeldoorn) en de leveranciers. De uitkomsten van deze onderzoeken zijn tezamen met de mededeling van de externe leverancier met betrekking tot Digipoort en het Webtrust certificaat van PKIoverheid gebruikt als basis voor deze verantwoording en de TPM. De directeur van Logius is verantwoordelijk voor de inhoud van de verantwoording.

3.4 Leeswijzer

De lezer die globaal kennis wil nemen van de inhoud van het rapport kan zich beperken tot de Third Party Mededeling, de inleiding en de managementsamenvatting. In de hoofdstukken vier 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.

4 Bevindingen DigiD voor Burgers

4.1 Algemeen

DigiD staat voor Digitale Identiteit. DigiD voor Burgers (verder genoemd: DigiD) is een gemeenschappelijk authenticatiesysteem van en voor de overheid, waarmee de identiteit kan worden geverifieerd van burgers die gebruikmaken van elektronische overheidsdiensten. 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. In totaal zijn er in 2009 73 nieuwe organisaties aangesloten op DigiD (van 414 naar 487). Het aantal gelukte authenticaties DigiD voor 2009 was ruim 24 miljoen en daarmee is de jaarbegroting ruim overschreden (132%). Het aantal eindgebruikers is in 2009 gegroeid van 6,7 naar ruim 7,5 miljoen.

In 2009 heeft doorontwikkeling van de DigiD dienstverlening plaatsgevonden. Het betreft ondermeer de ondersteuning van 'officiële elektronische bekendmaking' met DigiD. Verder is een aantal verbeteringen gerealiseerd op het gebied van de beheersbaarheid van DigiD, bijvoorbeeld voor de ondersteuning van de klanten van de Sociale Verzekeringsbank (SVB) in het buitenland. In de volgende paragrafen wordt ingegaan op de samenstellende delen van de DigiD dienstverlening waarbij ook de belangrijkste bijzonderheden en verbeterpunten in beeld worden gebracht.

4.2 Tactisch beheer

Inrichting tactische beheerprocessen

Logius heeft een aantal tactische processen geïmplementeerd voor het beheer van de producten die zij onder haar hoede heeft. Doelstelling 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 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 derdelijns 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

De verdere verbetering van haar beheerprocessen is voor Logius een continu aandachtspunt. Regelmatig onderzoekt Logius de kwaliteit van haar beheerprocessen aan de hand van het normenkader. Positief is te melden dat het proces functionaliteitenbeheer (met name gericht op de doorontwikkeling van DigiD) weer voldoende invulling aan de daaraan gestelde normen geeft. De conclusie van dit onderzoek is dat de processen in voldoende mate zijn ingericht conform de eisen uit het normenkader. Ook wordt in de praktijk in voldoende mate conform de procesbeschrijvingen gewerkt. Uitzondering is het proces tactisch security management dat zich richt op het borgen van de samenhang in informatiebeveiliging over de samenstellende delen van de diensten van Logius heen. De opzet van het proces is op hoofdpunten toereikend, maar de werking van het proces gemeten naar de aantoonbare implementatie van het informatiebeveiligingsbeleid en -plan beantwoordt niet in voldoende mate aan het normenkader.

Op de volgende pagina's wordt ingegaan op een aantal onderwerpen op het gebied van de tactische processen inclusief eventuele verbeteracties. Per onderwerp wordt tevens ingegaan op gerealiseerde verbeteringen ten opzichte van de verantwoording van 2008.

Informatiebeveiliging

De voorgenomen nadere implementatie van het informatiebeveiligingsbeleid en -plan van Logius is in 2009 onvoldoende aantoonbaar gerealiseerd. De oorzaak hiervan is ten eerste gelegen in de operationele druk die onder andere het in beheer nemen van nieuwe diensten voor de betrokken medewerkers van Logius met zich meebrengt. Ten tweede heeft Logius vastgesteld dat het actuele informatiebeveiligingsbeleid en -plan niet meer in voldoende mate aansluiten op de huidige inrichting van Logius en haar groeiende aantal producten. Vanuit een procesvisie voor tactisch security management kan worden gesteld dat de nadruk in 2009 is blijven liggen op de beleidsfase. De invulling van de uitvoerings- en evaluatiefase voldoet dan ook nog niet aan de norm. In 2009 zijn genoemde tekortkomingen voor een deel gecompenseerd doordat:

- in het wijzigingenbeheerproces is geborgd dat elke relevante wijziging wordt beoordeeld vanuit informatiebeveiligingsperspectief;
- Logius de richtlijn hanteert dat periodiek technische beveiligingsonderzoeken worden uitgevoerd op de belangrijkste producten. In dit kader is eind 2009 een aantal van deze onderzoeken uitgevoerd (onder meer op DigiD).

Logius is zich er van bewust dat op de langere termijn deze compenserende maatregelen niet alle risico's afdekken. Daarom is eind 2009 een project gestart gericht op het aanpassen van het beleid en plan als basis voor het tactisch security management proces.

Een ander punt op het gebied van informatiebeveiliging is dat de in het self-assessment 2008 geconstateerde verbeterpunten voor Logius vestiging Den Haag in 2009 niet zijn opgelost. Gegeven het karakter van de werkzaamheden bij Logius vestiging Den Haag in 2009 leidt dit niet tot het melden van aanvullende risico's in deze verantwoording op het niveau van de DigiD dienstverlening. Logius is voornemens deze punten zo spoedig mogelijk op te lossen, ook omdat met de opheffing van Logius

vestiging Apeldoorn tevens operationele werkzaamheden vanuit Logius vestiging Den Haag zullen worden uitgevoerd.

Contractmanagement

DigiD maakt gebruik van Gemeentelijke Basis Administratie Verstrekkingen (GBA-V) voor de controle van gegevens bij het aanvragen van een nieuwe toegangscode. De GBA-V is een dienst waarmee een deelverzameling van de gegevens uit de Gemeentelijke Basis Administratie (GBA) kan worden geraadpleegd. In de huidige situatie is de GBA-V 7 x 24 uur opengesteld, maar ondersteuning bij storingen is conform dienstverleningsafspraken alleen tijdens kantooruren beschikbaar. In 2009 is wel informeel een piketdienst ingeregeld voor de GBA-V. Het risico is dat (nieuwe) gebruikers van DigiD geen toegangscode kunnen aanvragen zolang een storing in de GBA-V buiten kantooruren niet wordt opgelost. Logius vindt het bijbehorende beschikbaarheidsrisico voorlopig acceptabel aangezien een verstoring alleen de mogelijkheid tot aanvraag van nieuwe DigiD inlogcodes treft.

Vanaf november 2008 is het gebruik van DigiD mogelijk gemaakt voor klanten van de Sociale Verzekeringsbank (SVB) die in het buitenland wonen. Hiervoor wordt mede gebruik gemaakt van een intern register van de SVB. Het contract waarin de afspraken tussen SVB en Logius op dit gebied zijn vastgelegd, is in de loop van 2009 geformaliseerd.

Capaciteitsmanagement

Als onderdeel van het proces behoeftemanagement is capaciteitsmanagement ingericht. Logius heeft in 2009 gewerkt aan de verdere verbetering van het capaciteitsmanagementproces, onder meer door op basis van klantgesprekken prognoses op te stellen voor het gebruik van DigiD. Periodiek rapporteert Logius (intern) over de prognose versus de realisatie voor het aantal aansluitingen en authenticaties. Er is in 2009 binnen DigiD voldoende capaciteit aanwezig geweest om pieken in de vraag op te vangen.

Transitiemanagement

Logius vindt het noodzakelijk om zekerheid te hebben over de specifieke versie van de DigiD software die in productie staat. Hiervoor is een procedure ingericht waarbij na het in productie nemen van een nieuwe softwarerelease voor DigiD een vergelijking wordt uitgevoerd tussen de originele softwarerelease op cd-rom en de software die op de DigiD servers in productie staat. Deze procedure is echter in 2009 niet consequent gevolgd. Logius heeft niet de indruk dat dit negatieve gevolgen heeft gehad voor de DigiD dienstverlening.

Ontwikkelproces

Het proces functionaliteitenbeheer maakt onderdeel uit van de tactische beheerprocessen. Dit proces richt zich op de beheerste doorontwikkeling van producten bij Logius. Het betreft onder meer het specificeren, ontwerpen en toetsen van aanpassingen aan de software voor DigiD, inclusief de inrichting van de niet-geautomatiseerde informatievoorziening (procedures etc.) rondom het systeem.

De werking van het proces functionaliteitenbeheer is in vergelijking met 2008 aanzienlijk verbeterd. Concreet is vooruitgang geboekt op de volgende gebieden:

- voor de functionele en technische ontwerpdocumentatie van DigiD is met versie 2.13 een nieuwe basisset gecreëerd, waarbij gebruik is gemaakt van geautomatiseerde ondersteuning;
- de herleidbaarheid van functionele wijzigingen via technische documentatie naar veranderingen in de broncode is controleerbaar gemaakt;
- in het derde kwartaal 2009 heeft Logius de dienstverlening van en de samenwerking met de externe leverancier van ontwikkeldiensten voor DigiD geëvalueerd. Het beeld is dat zowel de dienstverlening van als de samenwerking met deze leverancier in vergelijking met 2008 aanzienlijk is verbeterd, mede als resultaat van de gezamenlijke inspanning op dit gebied;
- de kwaliteit van het testen van nieuwe versies van DigiD is op een aantal manieren verbeterd. Ten eerste wordt er nu standaard een systeemtest uitgevoerd door de ontwikkelaar waarover ook wordt gerapporteerd aan Logius. Ten tweede is er vooruitgang geboekt op het gebied van het geautomatiseerd testen van DigiD. Ten derde worden nu ook beveiligingstesten op applicatieniveau ingezet als onderdeel van het reguliere testproces;
- de ontwikkelaar van DigiD heeft in opdracht van Logius een volledige analyse van de applicatie uitgevoerd vanuit beveiligingsperspectief. Het plan is om de verbeteringen die hier uit voortkomen in de loop van 2010 te realiseren.

Dankzij deze verbeteringen is de doorontwikkeling van de DigiD software beter beheersbaar en controleerbaar is geworden. Het aantal storingen bij het in productie nemen van nieuwe releases van DigiD software is aanzienlijk verminderd. De conclusie is dat het proces functionaliteiten-beheer in 2009 in voldoende mate invulling heeft gegeven aan de hiervoor geldende normen.

Nieuwbouw DigiD applicatie

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.

Op korte termijn compenseert Logius deze punten door het aantal functionele wijzigingen zo veel mogelijk te beperken en uitgebreid te testen. Op de langere termijn moet de applicatie echter worden vervangen vanuit het oogpunt van beheer- en aanpassingskosten en gevraagde flexibiliteit in het doorvoeren van wijzigingen. Logius is de voorbereidingen hiervoor gestart onder de werknaam DigiD-X. De functionele specificaties voor DigiD-X zijn hiervoor opgesteld en de voorbereiding voor de aanbesteding van de bouw wordt getroffen. De sturing van het project is in handen van de beleidseigenaar van DigiD (ministerie van BZK, programma Dienstverlening, Regeldruk en Informatiebeleid). ICTU zal hierbij optreden als opdrachtnemer en Logius als opdrachtgever en toekomstige beheerpartij. Het ICTU team wordt versterkt met expertise vanuit Logius. De verwachting is dat DigiD-X in de loop van 2011 in productie kan worden genomen.

4.3 Operationeel beheer

4.3.1 Logius Apeldoorn

Binnen Logius Apeldoorn zijn in 2009 de beheeronderdelen servicedesk en servicebeheer uitgevoerd voor een aantal producten die door Logius worden geleverd. DigiD voor Burgers is een van deze producten. De beheerprocessen die invulling geven aan de servicedesk en het servicebeheer sluiten aan op de processen van Logius Den Haag en leveranciers en hebben als doel de kwaliteit van de producten op een voldoende niveau te borgen.

Logius Apeldoorn is de voortzetting van de vroegere Serviceorganisatie die per 1 januari 2009 is overgegaan van de Belastingdienst naar Logius. Eind 2009 is besloten om Logius Apeldoorn in de loop van 2010 als zelfstandige locatie op te heffen en de werkzaamheden voor servicedesk en servicebeheer organisatorisch bij twee verschillende afdelingen van Logius Den Haag onder te brengen. Zo opereert de Servicedesk in het vervolg onder de afdeling Markt van Logius Den Haag als onderdeel van het Servicecentrum Logius (gestart per 1 december 2009) en wordt Servicebeheer geïntegreerd in de afdeling Servicemanagement. Om de integratie van de servicedesk en het servicebeheer goed te laten verlopen, past Logius Den Haag op onderdelen haar procesbeschrijvingen en interne werkafspraken aan. Ook is Logius Den Haag voornemens om aandacht te besteden aan de borging van de kennis die aanwezig is bij Logius Apeldoorn in het kader van opheffing.

Onderzoek beheerprocessen Logius Apeldoorn

De kwaliteit van de beheerprocessen bij Logius Apeldoorn is onderzocht aan de hand van het normenkader. Conclusie uit dit onderzoek is dat de beheerprocessen bij Logius Apeldoorn voldoen aan de eisen uit het normkader. Wel behoeft de beheersing van een aantal procesonderdelen verbetering. Deze procesonderdelen worden besproken in de volgende paragrafen.

Incidentenbeheer en probleembeheer

Logius Apeldoorn registreert eenduidig de incidenten en klachten per dienst. Voor DigiD voor Burgers wordt hiermee invulling gegeven aan het tweedelijns incidentenbeheer. Er zijn nog geen specifieke eisen gesteld aan de afhandelingstermijn voor deze incidenten. Logius Apeldoorn bewaakt de afhandeling van de incidenten. Beveiligingsincidenten worden apart behandeld en worden altijd doorgegeven aan beveiligingsfunctionarissen van Logius Apeldoorn en Logius Den Haag. Vanaf 2010 zal Logius Apeldoorn meldingen van beveiligingsrisico's van GOVCERT.NL beoordelen op mogelijke risico's voor de in beheer zijnde producten.

Logius Apeldoorn besteedt aandacht aan het verhelpen van structurele problemen. Evenals voorgaande jaren is er in 2009 nog geen procesmatige borging voor het beheer van problemen geweest, waarbij het proces garanties biedt voor een correcte vastlegging van de structurele verstoringen en voortgangsbewaking van de realisatie van de oplossingen.

Continuïteitsbeheer

Over bijna geheel 2009 heeft Logius Apeldoorn zelf zorg gedragen voor het maken en extern opslaan van reservekopieën van haar eigen IT-omgeving die haar werkzaamheden op het gebied van servicedesk en

servicebeheer ondersteunt. Begin december 2009 is deze taak in het kader van de verdergaande integratie overgedragen aan de leverancier voor de IT-omgeving van Logius Den Haag. Het samenvattend beeld is, dat er in 2009 onvoldoende maatregelen aanwezig zijn geweest om de continuïteit van de dienstverlening na een ernstige calamiteit op de locatie waar Logius Apeldoorn is gevestigd, te waarborgen. Zo is er geen continuïteitsplan aanwezig geweest. Dit is een kosten/baten afweging geweest, gegeven de naderende sluiting van Logius Apeldoorn. Om deze reden wordt er ook in 2010 geen nadere actie ondernomen.

Het eventueel niet beschikbaar zijn van Logius Apeldoorn heeft geen directe gevolgen voor de authenticatie –en aanvraagmogelijkheden van DigiD. Pas als Logius Apeldoorn enkele dagen niet beschikbaar is, heeft dat gevolgen voor de kwaliteit van de DigiD dienstverlening. Eerstelijns ondersteuning aan gebruikers van DigiD wordt bijvoorbeeld verzorgd door de leverancier van de callcenter dienstverlening. Mede als gevolg van de verdere integratie met Logius, ook voor wat betreft de ICT voorzieningen, zal worden aangesloten op de continuïteitsvoorzieningen van Logius Den Haag.

Toegangsbeheer

Autorisaties voor de applicatie voor ondersteuning van de interne werkprocessen en de beheerapplicatie voor DigiD aan medewerkers van Logius Apeldoorn en beheerders bij het externe rekencentrum worden alleen verleend na goedkeuring van de beveiligingsfunctionaris. Periodiek vindt een toetsing op actualiteit en juistheid plaats van de geïmplementeerde autorisaties.

Controle overdracht bestand activeringsbrieven

Logius Apeldoorn voert ad hoc controles uit op de volledige en (technisch) juiste ontvangst van het bestand met daarin de af te drukken brieven met activeringscode door de printleverancier. Evenals in 2008 ontbreekt een aansluiting van het aantal af te drukken brieven met de applicatiegegevens. Om deze controle mogelijk te maken is inmiddels een aanpassing van de applicatie DigiD voor Burgers aangevraagd.

4.3.2 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. Op basis van onderzoek is de conclusie dat in 2009 deze processen in voldoende mate aantoonbaar hebben gefunctioneerd.

In 2008 was al vastgesteld dat in de DigiD IT-infrastructuur een aantal verbeterpunten aanwezig was. Ter verbetering hiervan is begin 2009 een aantal veranderingen doorgevoerd in de bestaande IT-infrastructuur in afwachting van een volledige vervanging hiervan. In 2009 heeft de leverancier door verschillende oorzaken een aantal maanden minder dan de afgesproken 99,95% beschikbaarheid van DigiD kunnen realiseren. Zo heeft ook ten tijde van de aangifte inkomstenbelasting in maart 2009 een aantal verstoringen plaatsgevonden. Vanuit Logius en in overleg met de leverancier hebben deze verstoringen tot een aantal acties geleid.

Een eerste actie lag op het gebied van het doorzetten van een verbeterplan voor de IT-infrastructuur van DigiD waartoe ultimo 2008 reeds besloten was. Dit zogenoemde 'plan A' is door de leverancier in opdracht van Logius opgesteld. De kern van dit plan betreft de ontwikkeling van een volledig nieuwe IT-infrastructuur, die is toegesneden op het toenemende gebruik van DigiD. Uitvoering van dit plan heeft gedurende 2009 plaatsgevonden. De nieuwe IT-infrastructuur is op 17 januari 2010 in gebruik genomen. Aangezien de nieuwe IT-infrastructuur is ingericht conform de standaarden van de leverancier, is de verwachting dat in 2010 meer dan voorheen gebruik kan worden gemaakt van de beheerprocessen conform het aanwezige standaard 'Control Framework' van de leverancier. Dit biedt in beginsel aanvullende mogelijkheden voor het bij voortdurend monitoren en bewaken van getroffen procedurele- en technische beveiligingsmaatregelen. Ook zijn in het ontwerp van de nieuwe IT-infrastructuur de bekende zwakke plekken weggenomen die in de oude omgeving ook in 2009 nog aanwezig waren. Gekozen is voor een twin-datacenter concept. Dit betreft een uitwijkmodel waarbij de omgevingen identiek (dubbel) zijn ingericht en het risico op dataverlies en downtime tot een minimum is beperkt.

Een tweede actie betrof het nemen van onder andere de volgende bestuurlijke en organisatorische maatregelen:

- de leverancier wordt eigenaar van de nieuwe IT-infrastructuur waarmee de verantwoordelijkheden rondom deze infrastructuur duidelijker worden;
- een eventuele contractverlenging is afhankelijk gemaakt van de realisatie van kwaliteitsverbetering door de leverancier op een aantal gebieden;
- in de nieuwe Service Niveau Overeenkomst (SNO) die van kracht wordt na het in productie gaan van de nieuwe IT-infrastructuur is een aantal key performance indicators opgenomen die betere aansturing van de leverancier door Logius mogelijk maken; ook is een compensatieregeling opgenomen in het geval de afgesproken prestaties niet worden geleverd;
- het voeren in 2009 van een maandelijks strategisch overleg tussen Logius en leverancier (naast het bestaande tactische en service niveau rapportage overleg) onder meer gericht op de beheersing van de verschillende verbeteracties.

Een derde actie lag op het gebied van het verbeteren van de operationele samenwerking tussen leverancier en Logius, met name op het gebied van eenduidige classificatie, identificatie en communicatie van incidenten, het opstellen van een wijzigingskalender en het plannen van extra onderhoudswindows.

Beheerprocessen

De overeenkomst tussen leverancier en Logius voor het beheer van DigiD is uitgewerkt in een Service Niveau Overeenkomst (SNO) waarop weer een Dossier Afspraken en Procedures (DAP) is gebaseerd. Hierin staan operationele afspraken en procedures tussen Logius en de leverancier. Intern hanteert de leverancier een Service Delivery Plan, waarin de te leveren diensten met betrekking tot DigiD zijn uitgewerkt.

Beheerrollen en autorisaties voor DigiD zijn beschreven, alsmede het toekennen, beheren en intrekken van de autorisaties. De feitelijke situatie wordt driemaandelijks getoetst. Resultaten van deze toetsing zijn

beschikbaar, evenals vastleggingen van de activiteiten voor deze toetsing. Per 26 november 2009 is een verbeterde procedure voor autorisatiebeheer van kracht geworden. In een Information Security Policy garandeert de leverancier de betrouwbaarheid en integriteit van informatie alsmede het voldoen aan wetgeving zoals de Wet Bescherming Persoonsgegevens. Hiertoe zijn beheerprocessen ingericht. Het nemen van beveiligingsmaatregelen, reageren op beveiligingsincidenten en laten uitvoeren van beveiligingsaudits is de verantwoordelijkheid van de proceseigenaren van de diverse beheerprocessen.

In het kader van het beheerproces capaciteitsbeheer beschikt de leverancier over een capaciteitsplan voor de generieke ICT-dienstverlening. Behaalde service niveaus worden bewaakt. De leverancier informeert Logius periodiek middels Service Niveau Rapportages. Logius kan op basis hiervan aanvullende afspraken maken met de leverancier.

Voorts heeft de leverancier een uitwijkplan en uitwijkdraaiboek voor DigiD. Begin 2009 heeft een geslaagde uitwijktest plaatsgevonden. Op 1 april 2009 heeft een echte (geslaagde) uitwijk plaatsgevonden. De uitwijk is aan Logius gemeld. Naar aanleiding van een evaluatie van deze twee gebeurtenissen is het uitwijkplan herzien. Sinds 17 januari 2010 is de nieuwe infrastructuur operationeel. Naar ons is medegedeeld is hierin ook een uitwijkvoorziening geïmplementeerd. In de verantwoording 2010 zal hierop nader worden ingegaan.

Een configuration management proces voor DigiD is beschreven. Alle configuratie-items (hardware en software) worden met een versienummer geregistreerd in de Configuration Management Database (CMDB). Sinds medio 2009 is in de bestaande DigiD voor Burgers infrastructuur op een aantal systemen monitoring software geïnstalleerd, waarmee geautomatiseerde controles worden uitgevoerd op aanwezige hardware, bestaande systeemconfiguraties en useraccounts (Ist-situatie). Deze installatie kan worden gezien als een onderdeel van de voorbereiding op de realisatie van het verbeterplan voor de IT-infrastructuur. Naar verwachting wordt toepassing van de monitoring software op de nieuwe IT-infrastructuur in 2010 volledig operationeel.

Voor wijzigingsverzoeken, incidenten, problemen en andere klantvragen heeft de leverancier een Servicedesk ingericht. Processtappen, controleactiviteiten en informatie over de productieverwerking worden geregistreerd. Er is specifiek aandacht voor patches, urgente wijzigingen en standaard wijzigingen. Een impactanalyse wordt uitgevoerd, waarin ook risico's van de wijziging worden beoordeeld. Acceptatie van een wijziging namens de leverancier geschiedt door de change validator. Mede op basis van een impactanalyse wordt de wijziging geaccepteerd of geweigerd door de wijzigingsaanvrager. De change management procedure is niet in alle gevallen aantoonbaar nageleefd. De leverancier heeft dit onderkend en heeft toegezegd actie te ondernemen.

De registratie van gegevens over incidenten is gestandaardiseerd. Incidenten krijgen een prioriteit toebedeeld. Een registratie van bekende fouten en beschikbare oplossingen is aanwezig. Uitgangspunt voor problem management is dat incidenten systematisch worden geanalyseerd ter signalering van problemen. De werkwijze bij problemen is vergelijkbaar met die van incidenten.

Veilige afvoer, danwel vernietiging van gegevensdragers maakt geen onderdeel uit van het control framework van de Leverancier. De leverancier is echter bekend dat bij afvoer van gegevensdragers van DigiD deze gecertificeerd vernietigd moeten worden. Deze situatie heeft zich in 2009 volgens de leverancier niet voorgedaan.

Rechten beheerwerkzaamheden

Uitgangspunt is dat beheerders binnen de DigiD omgeving dienen te beschikken over zo beperkt mogelijke beheerrechten en dat gebruik van beheerrechten controleerbaar is. Begin 2009 zijn als onderdeel van de eerder genoemde verbeteractie aanvullende controle-/beveiligingsmaatregelen getroffen rondom het gebruik van beheerrechten, danwel de uitvoering van beheerhandelingen in de IT-infrastructuur van DigiD. Hierdoor worden onder andere de handelingen van beheerders vanaf januari 2009 op een centrale plaats vastgelegd. De beheerders van DigiD hebben zelf alleen leestoegang tot deze centrale vastlegging. Het beheer van deze centrale vastlegging is ondergebracht bij een ander beheerteam binnen de leverancier dan het reguliere DigiD beheerteam. Vastgesteld is dat de maatregelen op het gebied van het vastleggen van beheerhandelingen inclusief het alleen met leesrechten toegankelijk zijn van deze vastlegging in 2009 in voldoende mate hebben gefunctioneerd.

Autorisaties worden sinds 2009 aan DigiD beheerders toegekend op basis van functioneel gecreëerde groepslidmaatschappen (per beheerteam) op de DigiD systemen. Nagenoeg alle op de systemen aangemaakte beheergroepen hebben gedurende 2009 via een controlemechanisme over een beperkte set aan beheerrechten beschikt. Uitzondering is het beheerteam van de reguliere DigiD beheerders die middels hun groepslidmaatschap beschikken over volledige rechten op de betreffende DigiD systemen. De beheerorganisatie geeft aan dat deze rechten uit het oogpunt van doelmatig beheer en continuïteit van de bedrijfsprocessen strikt noodzakelijk zijn. De risico's die het bezit van de volledige rechten voor de DigiD omgeving met zich meebrengen, wordt gemitigeerd door:

- slechts een beperkt aantal beheerders is lid van het beheerteam van de reguliere DigiD beheerders. Deze beheerders zijn aangesteld conform de door de leverancier gehanteerde procedures, waarbij de terechtheid van het groepslidmaatschap driemaandelijks (op grond van het "User Review Process") door de verantwoordelijke teammanager wordt beoordeeld;
- het eerder genoemde controlemechanisme voor de vastlegging van beheerhandelingen zorgt er voor dat alle beheerhandelingen centraal worden vastgelegd en controleerbaar zijn. Bovendien is op de logservers een controlescript actief dat bij voortduring beheerhandelingen monitort op security gerelateerde events. Feitelijk worden door deze maatregel alle beheerhandelingen onder een vergrootglas geplaatst;
- alle vastleggingen van systeemgebeurtenissen worden "on-the-fly" op afzonderlijk ingerichte systemen veiliggesteld. Deze vastlegging is voor interne en externe controledoelinden beschikbaar. De leverancier heeft in 2009 toereikende bewaartermijnen voor deze vastlegging bepaald;
- de beheerders uit het reguliere DigiD beheerteam beschikken niet standaard over het wachtwoord voor het account waaraan de volledige rechten zijn gekoppeld. Voor dit wachtwoord is begin 2009 een enveloppenprocedure ingesteld voor alle systemen

binnen de DigiD omgeving voor gebruik in noodgevallen. Ook is voorzien in periodieke wijziging van dit wachtwoord.

Bovenstaande procedurele- en technische maatregelen hebben gedurende 2009 naar behoren gefunctioneerd. Het risico van te hoge rechten voor reguliere DigiD beheerders is door het implementeren van voornoemde compenserende maatregelen controleerbaar, hetgeen de kans op misbruik vermindert.

Toegang IT-infrastructuur DigiD voor Burgers

De IT-infrastructuur van DigiD voor Burgers heeft in 2009 bestaan uit een productie-/uitwijkomgeving alsmede een aantal andere omgevingen (bijvoorbeeld acceptatieomgeving). Deze verantwoording richt zich met name op de productieomgeving.

De gehele infrastructuur is gebaseerd op Internettechnologie. De DigiD IT-infrastructuur is op een aantal manieren gekoppeld met de buitenwereld. Een eerste koppeling is met het Internet via welke de primaire dienstverlening aan (webdiensten van) klanten en burgers plaatsvindt. Een tweede koppeling is met het beheernetwerk van de leverancier waarlangs het beheer plaatsvindt. Verder is bijvoorbeeld een koppeling aanwezig met de GBA-V voor de controle van adresgegevens van personen die zich aanmelden voor een DigiD.

De toegang tot de DigiD infrastructuur vanaf het Internet is beveiligd middels een firewall. De inrichting van de DigiD firewall is voldoende waarbij in 2008 een belangrijk aandachtspunt was dat op de firewall geen vastlegging plaatsvond van aan beveiliging gerelateerde gebeurtenissen. Hierdoor bestond het risico dat aanvalspogingen van buitenaf onopgemerkt bleven. In 2009 is deze situatie verbeterd doordat een Intrusion Detection systeem is geïnstalleerd. Na het doorlopen van een inregelperiode van enkele maanden is het systeem door de leverancier effectief ingezet voor het continu monitoren en bewaken van datastromen in de IT-infrastructuur. Het genoemde risico in de DigiD firewall is hiermee in voldoende mate weggenomen.

De toegang tot het DigiD beheernetwerk verloopt trapsgewijs vanaf het algemene netwerk van de leverancier via specifiek daartoe ingerichte 'steppingstones' die de uiteindelijke routes (paden) naar de klantomgevingen definiëren. Voor toegang tot een steppingstone wordt de techniek van two-factor authentication (unieke gebruikersnaam met wachtwoord en smartcard) gehanteerd. Alle netwerkverbindingen in het DigiD beheernetwerk maken uit oogpunt van beveiliging gebruik van encryptie waarmee is geborgd dat commando's en wachtwoorden niet kunnen worden aangepast of achterhaald. Een beperkt aantal beheerders van de leverancier, ingedeeld naar beheerteams, heeft op deze wijze toegang tot het beheernetwerk voor de DigiD infrastructuur. De conclusie is dat de toegang van beheerders tot de DigiD infrastructuur in 2009 voldoende veilig is geweest.

Beschikbaarheid DigiD infrastructuur

Onder de kop 'algemeen' is reeds ingegaan op de beschikbaarheid van de DigiD dienstverlening. In aanvulling wordt gemeld dat in 2009 de DigiD IT-infrastructuur was ondergebracht in twee geografisch gescheiden rekencentra van de leverancier. De leverancier heeft in januari 2009 een uitwijktest uitgevoerd. Hiertoe is door de leverancier een draaiboek

opgesteld, hetgeen na afloop is aangevuld met evaluatieverslagen afkomstig van de testuitkomsten. Deze uitwijk is op 1 april 2009 vanwege een aantal storingen in de voorziening DigiD voor Burgers, in de praktijk noodgedwongen en met succes beproefd.

Vooruitblik 2010

Het jaar 2009 kan voor met name (het beheer van) de IT-infrastructuur voor DigiD worden gekarakteriseerd als een overgangsjaar. De resultaten van alle inspanningen voor de bouw van een nieuwe IT-infrastructuur voor DigiD kunnen waarschijnlijk in 2010 en verder worden genoten.

4.3.3

Print & mail

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 kwaliteit. Wel verdient het beheerproces access management aandacht.

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 informeert door middel van rapportages Logius periodiek over de dienstverlening. De leverancier rapporteert 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. In vergelijking met 2008 is in 2009 een aantal verbeteringen zichtbaar. Het kwaliteitshandboek van de print -en mailleverancier is aangevuld met nieuwe procedures en het draaiboek DigiD dienstverlening is verder uitgewerkt. Verder streeft de print -en mailleverancier naar een eenduidige werkwijze op al haar locaties waar print- en maildienstverlening kan worden uitgevoerd.

Een nieuwe ontwikkeling bij de print -en mailleverancier is dat de ICT-beheerprocessen in 2010 worden uitbesteed aan een externe partij. In 2009 is de print -en mailleverancier hiervoor gestart met een project outsourcing. Momenteel beslist de print -en mailleverancier aan welke leverancier het beheer van ICT-beheerprocessen (zowel ten behoeve van de DigiD-dienstverlening alsook de dienstverlening aan andere klanten van de print- en mailleverancier) zal worden gegund. De uitbesteding omvat onder meer de generieke beheersaspecten en de beheerprocessen availability-, continuity- en accessmanagement. De print- en mailleverancier streeft met deze uitbesteding naar een verdere professionalisering van haar ICT-beheerprocessen. Om die reden zijn in gang gezette ontwikkelingen ten aanzien van het beheer van ICT-processen in 2009 pragmatisch uitgevoerd. De print- en mailleverancier stelt zich voor 2010 tot doel het structureel een aantoonbaar monitoren, toetsen en bijsturen van ICT-beheerprocessen onderdeel te laten zijn van de uitbesteding.

Availability Management

In 2009 is door de print- en mailleverancier met behulp van een zogenaamde monitoring tool alsmede manueel de beschikbaarheid van ICT-services bewaakt. Verder is de werkwijze voor ICT Availability management aangescherpt. Gedurende 2009 hebben zich geen uitzonderlijke verstoringen in de DigiD-dienstverlening voorgedaan.

Continuity Management

In 2009 is door de print- en mailleverancier het draaiboek dienstverlening DigiD aangevuld met een werkwijze voor Disaster Recovery Planning in het geval van een calamiteit. In 2009 is de uitwijk getest en succesvol uitgevoerd.

De netwerken op de twee productielocaties van de print- en mailleverancier zijn in 2009 tot één netwerk samengevoegd. Zo kan in het geval van een calamiteit uitgeweken worden naar de andere locatie zodat de productie met minimale verstoring voortgang kan vinden. Tevens is een voorziening getroffen zodat in noodgevallen gebruik kan worden gemaakt van een back-up server voor ontvangst van het DigiD bronbestand. De print- en mailleverancier is voornemens in 2010 alle print- en maildienstverlening te centraliseren op één locatie.

Access Management

Bij de print- en mailleverancier is access management nog een punt van aandacht. De print- en mailleverancier is in 2009 gestart met een project om autorisaties inzichtelijk te maken en op orde te krijgen. Dit project is in volle gang.

Complexe wachtwoorden worden afgedwongen en gebruikers worden ingedeeld volgens een bepaalde rol (taken, verantwoordelijkheden) op basis waarvan zij toegangsrechten hebben. Autorisaties worden schriftelijk en/of per e-mail aangevraagd en afgehandeld, danwel vastgelegd.

Een autorisatiematrix op het niveau van applicaties, gebruikers en bijbehorende rechten is in ontwikkeling, maar ontbreekt in 2009. De print- en mailleverancier beschikt voor 2009 wel over een autorisatieschema dat inzicht geeft in de toegang tot diverse mappen en bestanden.

De print- en mailleverancier heeft een firewall geïmplementeerd die de toegang tot het netwerk afschermt. Zoals eerder aangegeven vindt de uitwisseling van DigiD bronbestanden op veilige wijze plaats en wordt externe toegang tot de daarvoor gebruikte (beveiligde) server gelogd c.q. vastgelegd. Externe toegang tot deze server is beperkt tot geautoriseerde systemen uit de DigiD (rekencentrum) omgeving.

Voor de afhandeling van het print- en mailproces hebben verschillende geautoriseerde interne gebruikers toegang tot de DigiD bronbestanden. Deze interne toegang wordt vastgelegd met behulp van logging. Echter, over 2009 is vastgesteld dat de controleerbaarheid van deze interne toegang tot het bronbestand dient te worden verbeterd.

In 2009 heeft de print- en mailleverancier zelf geen structurele monitoring, toetsing en bijsturing op basis van de logging uitgevoerd. Wel heeft eind 2009 een interne controle op het systeembeheer plaatsgevonden. Hierbij zijn geen bijzonderheden gebleken.

4.3.4 *Callcenter*

Algemeen

Logius heeft de callcenter-activiteiten 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 callcenterproces en de daaraan gerelateerde dienstverlening bij de callcenterleverancier in voldoende mate invulling geven aan de daaraan gestelde eisen met betrekking tot de kwaliteit. Een punt van aandacht vormen evenwel de ICT-beheerprocessen die de callcenterleverancier heeft uitbesteed.

Primair proces

Het callcenter zorgt voor de afhandeling en/of routing van vragen, klachten en incidenten van eindgebruikers over het gebruik van DigiD per telefoon en e-mail. Daarnaast beantwoordt het callcenter eenvoudige vragen van klanten (overheidswebdiensten) over de DigiD dienstverlening. Afhandeling van incidenten, vragen en klachten vindt plaats op basis van de kennisbank. Vragen die door het callcenter niet via een kennisbank kunnen worden afgehandeld en klachten worden per e-mail doorgezet naar de Servicedesk van Logius. Aanvullingen op de kennisbank worden uitgevoerd op basis van wijzigingsbeheerprocedures waarin de goedkeuring door Logius van een wijziging een onderdeel is. De agents van het callcenter zijn verantwoordelijk voor het registreren, toewijzen en volgen van meldingen. Meldingen worden onder vermelding van een uniek ticketnummer geregistreerd. Tevens wordt de fase van afhandeling van

meldingen in een beheertool geregistreerd. De agents worden gemonitord door supervisors, waarbij wordt vastgesteld dat calls en e-mailberichten tijdig en met voldoende deskundigheid worden afgehandeld. De inzet van de agents 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. De callcenterleverancier heeft op vestigingsniveau interne audits uitgevoerd naar (interne) processen die ook de DigiD-dienstverlening raken.

Informatiebeveiliging en de naleving van de Wet Bescherming Persoonsgegevens hebben de aandacht. In dit kader is bepaald dat het aantal incidenten, vragen en klachten in het kader waarvan persoonsgegevens worden vastgelegd, is verminderd van 2,6% in 2008 naar 0,45% in 2009. Logius heeft aangegeven dat in overleg met de callcenterleverancier een bewerkersovereenkomst zal worden opgesteld (zie hiervoor ook paragraaf 4.5).

Voor de DigiD-dienstverlening wordt een specifieke applicatie gebruikt. Registratie van meldingen vindt hierin plaats. Iedere melding wordt uniek geïdentificeerd door een ticketnummer. Tevens vermeldt deze vastlegging de status en de classificatie (vraag, klacht en verstoring). In deze applicatie worden de servicelevels continu gemonitord en op basis hiervan wordt aan Logius gerapporteerd.

Capacity Management

Voor het inschatten, plannen en toewijzen van capaciteit gebruik wordt gemaakt van twee applicaties. De ene dient voor de forecastplanning, danwel planning op langere termijn. Dit gebeurt op basis van de werklastvoorspelling die van Logius wordt ontvangen. De andere applicatie voorziet in de dagelijkse operationele planning, bezetting en capaciteitverdeling. Op basis van door Logius aangeleverde verwachte aantallen meldingen en historische gegevens inzake de afhandelingstijd wordt het benodigde aantal agents per dag voor DigiD bepaald. De realisatie van het tussen Logius en de callcenterleverancier overeengekomen servicelevel voor de afhandeling van meldingen wordt per kwartier bewaakt. Indien noodzakelijk kunnen extra agents worden opgeroepen om de capaciteit uit te breiden. De callcenterleverancier heeft hierover afspraken gemaakt met uitzendbureaus.

Voor de levering van de door de callcenterleverancier gebruikte applicatie en onderliggende database is een contract afgesloten met een externe partij. Hierin is ondermeer voorzien in de bewaking van de capaciteit. Over het gebruik heeft in 2009 rapportage plaatsgevonden aan de callcenterleverancier.

De capaciteit en de uitputting daarvan worden maandelijks in een Service Niveau Rapportage (SNR) ter beschikking gesteld aan Logius en vervolgens besproken tussen Logius en de callcenterleverancier. Als er aanleiding toe is, vindt bijstelling van de ingezette capaciteit plaats.

Continuity Management

De callcenterleverancier beschikt over een risk assessment en calamiteitenplan dat medio 2008 is vastgesteld. Er is hierin onder andere

aandacht voor de uitval van telefoons, databases en intranet. Alle relevante geledingen van de callcenterleverancier zijn bij de risico-inventarisatie betrokken geweest.

Ten behoeve van de registratie van het primaire proces maken medewerkers gebruik van een softwaretool, danwel applicatie. In 2009 hebben zich rondom de applicatie op de werkvloer geen verstoringen voorgedaan.

Back-ups worden weggeschreven naar een andere productielocatie. De kopie van de data staat derhalve continu off-site. De telecomleverancier garandeert een 99,98% beschikbaarheid van de keten. Indien een locatie onverhoopt mocht uitvallen, kunnen de diensten worden doorgeschakeld naar een andere locatie. In oktober 2009 heeft zich een ernstige verstoring met betrekking tot deze dienstverlening voorgedaan in een aantal vestigingen van de callcenterleverancier. Deze verstoring, die ongeveer zes uur duurde, is na het volgen van een noodprocedure verholpen.

Over 2009 wordt met betrekking tot de door de callcenterleverancier aan een externe leverancier uitbestede ICT-beheerprocessen slechts globaal inzicht geboden inzake de continuïteit/uitwijk en back-up & recovery van de centrale applicatie. Dit is inclusief database en kennisbank, waarmee eerstelijns vragen over DigiD worden beantwoord. De callcenterleverancier heeft dit onderkend en stelt zich tot doel over geheel 2010 volledig inzicht te bieden in deze onderwerpen. Begin 2010 zullen hierover nadere afspraken worden gemaakt met de externe leverancier.

Access Management

De externe leverancier heeft richtlijnen voor toegang van gebruikers tot systemen en applicaties. Wanneer een medewerker de eerste keer toegang krijgt, dient een nieuw wachtwoord te worden ingevoerd. Een medewerker krijgt toegang tot het netwerk wanneer hij/zij is geregistreerd in het gebruikte Enterprise Resource Planning (ERP)systeem. Vervolgens wordt de medewerker, afhankelijk van zijn functie, geautoriseerd voor diverse applicaties. Medewerkers (onder andere teamleiders en agents) hebben op basis van hun functie afgestemde toegangsrechten. Medewerkers (behalve agents) hebben persoonlijke accounts met een persoonlijk wachtwoord. Voor agents is er een collectief account. Hun activiteiten worden op de werkvloer echter tot op de minuut gelogd. Ook is er direct oogtoezicht door de teamleiders. Zowel teamleiders als agents hebben alleen raadpleegrechten in de centrale applicatie.

Wanneer een medewerker uit dienst gaat wordt dit geregistreerd in het ERP-systeem. Dit leidt tot het blokkeren van het netwerkaccount van betreffende medewerker. Maandelijks worden de accounts van de agents die uit dienst zijn getreden verwijderd.

Over 2009 wordt beperkt inzicht geboden in de interne ICT-beheerprocessen, met name inzake toegangsbeveiliging/autorisaties van de applicatie, inclusief de database waarmee de DigiD-dienstverlening plaatsvindt en de kennisbank. Dit wordt door de callcenterleverancier onderkend en in 2010 zullen gepaste acties worden ondernomen. De callcenterleverancier stelt zich tot doel over heel 2010 aan te tonen dat toegangsbeveiliging/ autorisaties met betrekking tot de applicatie,

inclusief bijbehorende database waarmee de DigiD-dienstverlening plaatsvindt en de DigiD kennisbank (FAQ) zijn geïmplementeerd en uitgevoerd.

Incident Management

Alle calls worden gelogd. Agents classificeren een melding naar vraag, klacht of incident. Dit wordt vastgelegd in de betreffende applicatie. Wanneer een vraag niet kan worden beantwoord op basis van de FAQ database, wordt de melding door middel van een genormaliseerde e-mail als incident doorgezet naar het servicecentrum van Logius voor afhandeling door de tweede lijn. Het servicecentrum bevestigt de ontvangst van de melding middels doorgifte van een meldingsnummer, waarna de melding door de callcenterleverancier als afgehandeld wordt beschouwd. Deze meldingen (incidenten) worden maandelijks gerapporteerd in de Service Niveau Rapportage (SNR) aan Logius en besproken in het serviceniveau overleg. De procedure voor de genormaliseerde e-mail wordt overigens als niet praktisch ervaren en zal in 2010 worden geëvalueerd.

4.3.5 *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 voorzieningen waarmee deze functionaliteit wordt gerealiseerd, is een overeenkomst afgesloten tussen Logius en een SMS dienstverlener. 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 uitgevoerd naar het SMS dienstverleningsproces. De conclusie is dat het SMS dienstverleningsproces en de daaraan gerelateerde beheerprocessen bij de SMS dienstverlener in voldoende mate invulling geven aan de daaraan gestelde eisen met betrekking tot de kwaliteit. Uit het onderzoek komen de volgende punten naar voren.

Verzendverzoek afkomstig van een bevoegde instantie

Met behulp van twee maatregelen wordt vastgesteld dat het verzendverzoek afkomstig is van een bevoegde instantie. Dit betreft een toegangslijst op de webserver met IP-adressen via welke de te verzenden

SMS berichten aangeboden mogen worden (cliënt authenticatie) en certificaten die door Logius aan de SMS dienstverlener ter beschikking zijn gesteld en waarmee wordt vastgesteld dat de ontvangende partij een bevoegde ontvanger is (server authenticatie). Deze certificaten, die niet door Logius en ook niet door de SMS-dienstverlener kunnen worden gewijzigd, voorzien door middel van een 128-bits encryptie in een versleuteling van de berichten.

Afhandelen van verzendverzoeken

SMS berichten die door Logius aan de SMS dienstverlener worden aangeboden, worden door de SMS dienstverlener volledig aan de provider verstrekt. Om dit te realiseren zijn beheerprocessen beschreven in de Service Niveau Overeenkomst voor SMS Gateway Service DigiD en zijn beheerprocessen ingericht.

Verstoringen in de afhandeling van verzendverzoeken worden opgemerkt en leiden tot een incidentmelding. De tijdige afhandeling van incidenten wordt door de SMS-dienstverlener bewaakt. De SMS dienstverlener beschikt over een verzendcapaciteit van minimaal 1.200 SMS berichten per minuut. Dit betreft een limiet op de verzendfaciliteit, niet op de ontvangstfaciliteit. Op verzoek van Logius kan de capaciteit van de verzendfaciliteit worden verhoogd naar 5.000 SMS berichten per minuut. De capaciteit van de verzendfaciliteit is in de verantwoordingsperiode toereikend geweest.

De belasting van de infrastructuurcomponenten wordt doorlopend aan de hand van monitoringsystemen bewaakt en de beschikbaarheid wordt doorlopend getest in de productieomgeving. De ontvangstfaciliteit is redundant uitgevoerd. De primaire ontvangstfaciliteit betreft een platform welke exclusief voor DigiD in gebruik is. De secundaire ontvangstfaciliteit betreft een uitwijkmogelijkheid naar een platform dat voor meerdere klanten van de onderaannemer in gebruik is.

De beide ontvangstfaciliteiten zijn naar een primaire verzendfaciliteit ontsloten van de SMS dienstverlener. Indien de primaire verzendfaciliteit niet beschikbaar is dan kan voor DigiD verkeer gebruik worden gemaakt van een uitwijkmogelijkheid. Het DigiD verkeer kan voor uitwijk worden gerouteerd naar de SMS centrale (secundaire verzendfaciliteit) van een tweede operator. In de verantwoordingsperiode hebben zich verschillende verstoringen, danwel incidenten voorgedaan met betrekking tot de beschikbaarheid van de primaire verzendfaciliteit. In alle gevallen is er met succes en binnen de daarvoor gestelde norm uitgeweken naar de secundaire verzendfaciliteit. Over een jaar gemeten is de beschikbaarheid van de verzendfaciliteiten inclusief de verbinding met internet op 99,9% vastgesteld.

In de verantwoordingsperiode hebben zich geen verstoringen, danwel incidenten voorgedaan met betrekking tot de beschikbaarheid van de ontvangstfaciliteiten. Over een jaar gemeten is de beschikbaarheid van de ontvangstfaciliteit inclusief koppelingen naar internet op 100% vastgesteld. Dit is ruim boven de norm van 99,5% (gemeten over een jaar).

De geïmplementeerde toegangsrechten voor de componenten van de ontvangstfaciliteit komen overeen met de door het management vastgestelde autorisatiematrix. Alleen geautoriseerde beheerders kunnen

de SMS-codes benaderen. Toegangsrechten worden ingetrokken nadat van deze rechten gedurende een vastgestelde periode geen gebruik is gemaakt.

Verantwoordingsrapportage

Bij de SMS dienstverlener zijn de gegevens beschikbaar om end-to-end rapportages op te stellen. Zo beschikt de SMS-dienstverlener over registraties van incidenten die betrekking hebben op de SMS-dienstverlening. Tevens beschikt de SMS dienstverlener over een actueel overzicht van de infrastructuur die ten behoeve van de SMS dienstverlening in gebruik is. In dit overzicht wordt onder andere per onderdeel van de infrastructuur de gerealiseerde beschikbaarheid aangegeven. De gerealiseerde dienstverlening wordt periodiek beoordeeld in relatie tot de afgesproken dienstverlening en de uitkomsten worden maandelijks door de SMS dienstverlener aan Logius gerapporteerd.

Voor de door ons geselecteerde dagen komt het aantal SMS berichten dat door de Serviceorganisatie aan de SMS dienstverlener ter behandeling is aangeboden overeen met het aantal door de SMS dienstverlener doorgezette SMS berichten. Voor enkele dagen zijn niet-noemenswaardige verschillen geconstateerd. Deze verschillen waren al eerder door de SMS dienstverlener opgemerkt en verklaard.

4.4 Dienstspectifieke beheersingsmaatregelen DigiD voor Burgers

Inrichting dienstspectifieke maatregelen DigiD

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

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) of SVB register (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.

Het functioneren van deze dienstspectifieke maatregelen in en rondom DigiD is onderzocht en voldoet voor de meeste onderdelen aan het normenkader. Voor een drietal onderdelen heeft Logius vastgesteld dat er onvoldoende invulling is gegeven aan de norm c.q. dat er risicopunten aanwezig zijn. In de volgende alinea's wordt ingegaan op deze onderwerpen:

- analyse logbestanden DigiD;
- geprogrammeerde webapplicatie controles;
- verzending authenticatiecodes voor DigiD niveau midden.

Verder wordt ingegaan op de cryptografische beheersingsmaatregelen en een inherent restrisico in DigiD.

Analyse logbestanden DigiD

In DigiD is een voorziening op applicatieniveau ('applicatielogging') ingericht voor het vastleggen van handelingen van gebruikers en beheerders. Hierbij is rekening gehouden met privacyaspecten. De vastlegging wordt bijvoorbeeld gebruikt voor de analyse van incidentmeldingen die via de DigiD helpdesk binnenkomen. De vastlegging wordt gedurende een langere periode bewaard met onder andere als doel om later ook nog incidenten te kunnen analyseren. In samenhang met de vastlegging van gebeurtenissen in de onderliggende ICT-infrastructuur ('infrastructuurlogging', paragraaf 4.3.2) kan de applicatielogging worden ingezet om het gebruik van DigiD te monitoren.

Logius beschouwt de aanwezige applicatielogging als toereikend voor de beantwoording van de reguliere gebruikersvragen. Op onderdelen is de applicatielogging verbeterd in vergelijking met 2008:

- het internetadres van een gebruiker van DigiD wordt sinds medio 2009 vastgelegd in de applicatielogging wat het ondernemen van actie in het geval van een incident eenvoudiger maakt;
- proactieve analyse van de applicatielogging op een aantal aspecten vindt sinds medio 2009 ieder kwartaal plaats en op de uitkomsten van deze analyse wordt actie ondernomen.

Belangrijke aandachtspunten die nog aanwezig zijn:

- realtime analyse van de applicatielog op basis van statistiek en specifieke meldingen, bijvoorbeeld voor de detectie van ongebruikelijke gebeurtenissen, vindt niet aantoonbaar plaats. Procedures en geautomatiseerde ondersteuning hiervoor ontbreken;
- het detailniveau van de vastlegging van (beheer)acties in de applicatielogging is (te) beperkt. Hierdoor is het niet eenvoudig onderzoek uit te voeren naar handelingen die zijn uitgevoerd door beheerders van DigiD. Ook bleek het in het geval van een recent in een technisch beveiligingsonderzoek ontdekte kwetsbaarheid niet mogelijk om aan de hand van de applicatielogging na te gaan of dit in 2009 daadwerkelijk was opgetreden.

Het risico van deze punten is dat misbruik van of tekortkomingen in DigiD later dan gewenst worden gedetecteerd. Wel is het beter dan in 2008 mogelijk om een sluitende audittrail te construeren voor eventueel forensisch onderzoek, bijvoorbeeld na een beveiligingsincident.

Op het niveau van de IT-infrastructuur waren in 2009 compenserende maatregelen aanwezig in de vorm van een Intrusion Detection Systeem (IDS) en geautomatiseerde analyse van de infrastructuurlogging. Een duidelijke visie op de samenhang tussen de monitoring op IT-infrastructuur en applicatieniveau met een uitwerking in procedures en andere maatregelen is echter niet vastgelegd.

De conclusie is dat de analyse van de logbestanden van DigiD in 2009 aanzienlijk is verbeterd maar nog niet voldoende invulling geeft aan de daaraan door Logius gestelde normen. Logius heeft op dit moment de indruk dat dit geen negatieve gevolgen voor de DigiD voorziening heeft gehad. Uit doelmatigheidsoverwegingen wordt dit risico pas bij nieuwbouw van de DigiD applicatie volledig weggenomen. Wel heeft Logius het voornemen in 2010 de analyse van de applicatielogging stapsgewijs te

verbeteren door ondermeer de leverancier hierover meer te laten rapporteren.

Geprogrammeerde webapplicatie controles

Geprogrammeerde webapplicatie controles zijn van groot belang voor de correcte werking van de DigiD applicatie en het voorkomen van aanvallen op webapplicaties. In 2009 is op DigiD tweemaal een technisch beveiligingsonderzoek uitgevoerd dat ondermeer is gericht op deze webapplicatie controles.

Uit het onderzoek in februari 2009 kwam de aanwezigheid van een niet eerder ontdekte kwetsbaarheid in de DigiD applicatie naar voren. In het tweede technisch beveiligingsonderzoek dat in december 2009 is uitgevoerd is wederom een (andere) kwetsbaarheid van dezelfde soort aangetroffen. Uit dit onderzoek is ook een aandachtspunt naar voren gekomen dat verband houdt met de naleving van de aansluitvoorwaarden voor DigiD door (webdiensten van) klanten. Het aandachtspunt is door Logius gekwalificeerd op niveau 'midden'. Begin 2010 heeft Logius aan de ontwikkelaar voor DigiD de opdracht gegeven om een impactanalyse voor de oplossing van het probleem uit te voeren. Logius gaat er van uit in het probleem in 2010 definitief op te lossen.

De leverancier van ontwikkeldiensten heeft in 2009 in opdracht van Logius de huidige DigiD applicatie volledig doorgelicht op veel voorkomende webapplicatie kwetsbaarheden. De aanpassingen aan de DigiD applicatie die hier uit voortkomen worden in 2010 in productie genomen. De precieze datum voor de in productie name is bepaald op basis van een integrale risicoafweging.

De conclusie is dat de geprogrammeerde webapplicatie controles in 2009 niet op alle punten voldoende invulling hebben gegeven aan de daarvoor geldende normen.

DigiD niveau midden - verzending authenticatiecodes

Voor het DigiD niveau midden worden via SMS authenticatiecodes verzonden. In een publicatie van december 2009 (bijgewerkte publicatie in februari 2010) geeft Govcert.nl aan dat afluisteren van GSM-communicatie, waaronder SMS verkeer, zeer waarschijnlijk op korte termijn mogelijk wordt met relatief eenvoudige middelen. Dit heeft ook gevolgen voor het gebruik van DigiD authenticatiecodes middels SMS. Govcert.nl beveelt onder meer aan: 'Aanbieders van bestaande sms-authenticatiediensten moeten op korte termijn bepalen hoe zij met de veranderende risico's van sms-berichten omgaan. Voer bijvoorbeeld een risicoanalyse uit en overweeg de implementatie van aanvullende preventieve, detectieve of correctieve maatregelen. Denk hierbij ook aan de mogelijkheden die aanvallers hebben om gericht iemand af te luisteren. Ontwikkel geen nieuwe sms-authenticatietoepassingen die afhankelijk zijn van de versleuteling tussen BTS en mobiele telefoon. Logius volgt deze aanbeveling op. Voor de korte termijn heeft Logius vastgesteld dat het risico dat samenhangt met het mogelijk afluisteren van GSM-communicatie beperkt is. Voor de wat langere termijn onderzoekt Logius in overleg met de opdrachtgever voor DigiD de eventueel te treffen maatregelen.

Cryptografische beheersingsmaatregelen

In het DigiD systeem wordt op een aantal plaatsen gebruik gemaakt van encryptie om te voldoen aan de betrouwbaarheidseisen die aan DigiD worden gesteld, bijvoorbeeld vanuit het oogpunt van de Wet Bescherming Persoonsgegevens. Een voorbeeld is dat voor onderdelen van de centrale database van DigiD uitgebreid gebruik wordt gemaakt van encryptie. Ook in het authenticatieprotocol van DigiD wordt gebruik gemaakt van encryptie en aanverwante technieken. De details van de toepassing van encryptie zijn minder duidelijk gedocumenteerd. Er is wel vastgesteld dat in de broncode encryptiemaatregelen daadwerkelijk aanwezig zijn.

Inherent restrisico

De in deze verantwoording beschouwde zekerheidsniveaus van DigiD 'basis' en 'midden' kennen ieder een bepaalde zekerheid van authenticatie. Deze niveaus hebben ieder een geaccepteerd restrisico welke expliciet bekend wordt gemaakt aan en geaccepteerd door de klanten van DigiD. Het bewust geen gebruik maken van persoonlijke identificatie aan een loket bij de aanvraagprocedure voor DigiD om het gebruik van DigiD laagdrempelig te houden, is bijvoorbeeld mede bepalend voor dit geaccepteerde restrisico.

4.5 Naleving wet- en regelgeving

Logius vindt de naleving van wet- en regelgeving voor de in beheer zijnde producten vanzelfsprekend. Activiteiten op dit gebied worden zo veel mogelijk geïntegreerd in de tactische processen zoals beschreven in paragraaf 4.2.

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 Juridische Zaken van Logius in 2009 voor DigiD voor Burgers en de andere producten die in deze verantwoording zijn opgenomen 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;
- Voorschrift Informatiebeveiliging Rijksdienst (VIR).

De uitkomsten van deze analyse zijn aan het management van Logius gerapporteerd. Logius is voornemens in 2010 deze juridische analyse te actualiseren. Voor de periode 1 januari 2009 tot en met 31 december 2009 stelt Logius op basis van de juridische analyse en de inhoud van de voorgaande paragrafen vast dat voor DigiD voor Burgers op hoofdlijnen voldoende invulling is gegeven aan de eisen die voortkomen uit wet- en regelgeving. In 2009 zijn aandachtspunten die lateren aan de naleving van wet- en regelgeving geweest:

- een bewerkersovereenkomst (in de zin van de WBP) moet nog worden afgesloten tussen Logius en de call center leverancier respectievelijk de print & mail leverancier voor DigiD voor Burgers. De inhoud van deze bewerkersovereenkomst is overigens al grotendeels terug te vinden in de reguliere contracten;
- implementatie van het informatiebeveiligingsbeleid en -plan (zie paragraaf 4.2);
- logbewaking en -analyse (zie paragraaf 4.4);

- kwetsbaarheden rondom geprogrammeerde webapplicatiecontroles (zie paragraaf 4.4).

4.6 Conclusie

In vergelijking met het controlejaar 2008 wordt gemeld dat de controleerbaarheid van de IT-infrastructuur en de kwaliteit van het ontwikkelproces in 2009 aanzienlijk is verbeterd. Wel is vastgesteld dat met het aanwezige stelsel van beheersingsmaatregelen voor het product DigiD in de periode 1 januari 2009 tot en met 31 december 2009 nog niet voldoende invulling is gegeven aan alle afgesproken normen. Het betreft concreet:

- de wijze waarop logbewaking en -analyse worden ingezet om afwijkingen te detecteren in het gebruik van DigiD, dient te worden verbeterd op de aspecten aantoonbare samenhang van de getroffen maatregelen en de pro-actieve uitvoering hiervan;
- eind 2009 is evenals in 2008 en begin 2009 een beperkt aantal kwetsbaarheden ontdekt op het gebied van geprogrammeerde webapplicatiecontroles; hierop is overigens adequaat gereageerd;
- de implementatie van het informatiebeveiligingsbeleid en -plan heeft niet voldoende aantoonbaar plaatsgevonden.

Logius heeft de indruk dat genoemde punten in de verantwoordingsperiode geen negatieve gevolgen hebben gehad voor de DigiD dienstverlening. Met betrekking tot de beschikbaarheid van DigiD wordt gemeld dat in januari 2010 een nieuwe infrastructuur in productie is genomen die in ieder geval in opzet de beschikbaarheidsproblematiek mitigeert. De leverancier van ontwikkeldiensten heeft in 2009 een integrale analyse van webapplicatiecontroles uitgevoerd waarvan de resultaten in 2010 in de productieomgeving worden doorgevoerd. Rondom het informatiebeveiligingsbeleid en -plan is Logius een project gestart.

5 Bevindingen Digipoort

5.1 Algemeen

De Digipoort (voorheen Overheidstransactiepoort, OTP) is het elektronische postkantoor van de overheid voor bedrijven en burgers. Het verzorgt de gemeenschappelijke infrastructuur voor het berichtenverkeer tussen bedrijven en burgers enerzijds en overheden anderzijds. Digipoort maakt het uitwisselen van deze gegevens eenvoudiger, omdat bedrijven één elektronische ingang hebben bij de overheid om hun gegevens voor verschillende overheidsinstanties aan te leveren.

Digipoort draagt zorg voor gegarandeerde aflevering van berichten aan overheidsinstellingen. Na ontvangst van een bericht wordt een ontvangstbevestiging naar aanleveraars (bedrijven en burgers) gestuurd waarna Digipoort de aflevering aan de overheidsinstelling bewaakt. In de loop van 2009 is tevens het koppelvlak FTP aan Digipoort toegevoegd waarmee het mogelijk is geworden om grote bestanden via Digipoort uit te wisselen. Andere koppelvlakken van Digipoort zijn SMTP en X.400.

Het gebruik van de Digipoort is afgelopen jaar verder toegenomen met een stijging van 15 miljoen berichten in 2008 tot 22 miljoen berichten in 2009.

Logius is verantwoordelijk voor het tactische beheer en voor onderdelen van het operationeel beheer van Digipoort en wordt hierbij ondersteund door een externe leverancier voor infrastructuur- en applicatiebeheer.

5.2 Tactisch beheer

Logius maakt voor het tactisch beheer van de Digipoort dienstverlening gebruik van dezelfde beheerprocessen als voor DigiD voor Burgers. De in paragraaf 4.2 opgenomen beschrijving inclusief doelstelling en conclusie geldt op hoofdlijnen ook voor Digipoort.

Aanvullend wordt opgemerkt dat de conclusie op het gebied van het proces tactisch security management voor Digipoort minder gewicht heeft dan voor DigiD. De reden hiervoor is onder andere dat er voor Digipoort meer gebruik wordt gemaakt van standaard componenten.

5.3 Operationeel beheer

5.3.1 Context

De kwaliteit van het operationeel beheer van de dienst Digipoort wordt geborgd in de beheerprocessen van Logius Apeldoorn en de externe leverancier. Logius Apeldoorn verzorgt het servicebeheer en de eerstelijnsupport. De externe leverancier levert de technische infrastructuur voor Digipoort en draagt zorg voor het operationeel- en beveiligingsbeheer.

Begin 2009 is de dienstverlening die is belegd bij de externe leverancier voor Digipoort opnieuw aanbesteed. In 2009 heeft de bouw van de nieuwe Digipoort omgeving plaatsgevonden, als resultaat van de uitgevoerde aanbesteding. Oorspronkelijk was het de bedoeling in december 2009 over te gaan van de oude Digipoort naar de nieuwe Digipoort. Dit plan is

niet gehaald en de overgang vindt in het tweede kwartaal van 2010 plaats.

5.3.2 *Mededeling externe leverancier Digipoort*

De normen die gesteld zijn aan het stelsel van beheersingsmaatregelen bij de externe leverancier, zijn tussen de externe leverancier en de Belastingdienst in het verleden overeengekomen. Jaarlijks toetst een externe partij deze normen bij de leverancier. Resultaten van deze toetsing worden door de externe partij gerapporteerd in de Third Party Mededeling (TPM) OB2000 en OTP. In de TPM over het jaar 2009 is geconcludeerd dat de opzet van het stelsel van beheers- en beveiligingsmaatregelen voor de kwaliteitscriteria beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid voldoet aan de daaraan gestelde normen. Ook is vastgesteld dat deze beheers- en beveiligingsmaatregelen gedurende het jaar 2009 conform de opzet hebben bestaan en hebben gewerkt. Het oordeel heeft betrekking op de volgende onderwerpen:

Beveiligingsorganisatie	Wijzigingsbeheer
Personeel	Capaciteits- en beschikbaarheidsbeheer
Fysieke toegangsbeveiliging	Kostenbeheer
Configuratiebeheer	Continuïteitsbeheer
Incidentbeheer	Beveiligingsbeheer
Probleembeheer	Dienstenniveaubeheer
Afscherming derden	

Uit de TPM blijkt dat een aantal bevindingen uit voorgaande jaren in 2009 niet is opgelost. Aangegeven is dat de openstaande bevindingen zijn ingebracht bij het projectteam voor de nieuwe Digipoort. Bij de totstandkoming van de verantwoording over 2010 zal de status van deze openstaande bevindingen een belangrijk aandachtspunt zijn.

5.3.3 *Logius Apeldoorn*

Voor het operationeel beheer van de Digipoort dienstverlening heeft Logius Apeldoorn grotendeels gebruik gemaakt van dezelfde beheerprocessen als voor DigiD voor Burgers. De in paragraaf 4.3.1 opgenomen informatie geldt op hoofdlijnen ook voor Digipoort.

5.4 **Dienstspecifieke beheersingsmaatregelen Digipoort**

Onderzoek beheerprocessen

Naast de generieke operationele beheerprocessen voert Logius Apeldoorn een aantal specifieke processen uit die gericht zijn op het beheer van berichtenstromen en het beheer van aansluitingen van de dienst Digipoort. Conclusie is dat deze beheerprocessen voor de dienst Digipoort voldoen aan de eisen uit het normenkader. Uit het onderzoek naar de beheerprocessen bij Logius Apeldoorn komt een aantal onderwerpen naar voren. Deze worden hierna ter informatie besproken.

Beheer van aansluitingen

Logius Apeldoorn beheert functioneel de aansluitingen op de bestaande berichtenstromen die door de dienst Digipoort worden ondersteund. Dit

proces is binnen Logius Apeldoorn gestandaardiseerd en maakt gebruik van een geautomatiseerd systeem. Dit systeem bewaakt tevens de voortgang van de realisatie van nieuwe aansluitingen. Ook de wijzigingen van bepaalde instellingen (bijvoorbeeld het IP-adres) en gegevens van contactpersonen worden in dit systeem bewaakt. Vanaf het jaar 2010 zal Logius Apeldoorn bij verzoeken om dergelijke wijzigingen contact opnemen met de betrokken organisatie om vast te stellen dat het om een authentieke aanvraag gaat. Nieuwe aansluitingen van overheidsdeelnemers aan Digipoort worden uitgevoerd onder regie van Logius.

Herinjectie berichtenstromen

Bij berichtverlies bij één van de klanten van Digipoort heeft Logius Apeldoorn de mogelijkheid herinjectie van berichten uit te voeren. Aangezien dit een proces is met risico's voor de integriteit van data in klantsystemen is hiervoor een werkinstructie opgesteld. Deze werkinstructie waarborgt dat herinjecties pas na een schriftelijke opdracht en na akkoord van betrokken partijen worden uitgevoerd. In de praktijk hebben, evenals voorgaande jaren, nog geen herinjecties plaatsgevonden.

Uitwijk Digipoort

Voor de ICT-infrastructuur van de dienst Digipoort, zoals geleverd door de externe leverancier, was in 2009 geen uitwijkfaciliteit beschikbaar. Bij een calamiteit op de locatie van de externe leverancier zal de dienst Digipoort als geheel (tijdelijk) niet te gebruiken zijn. In de dienst Digipoort nieuw is in opzet wel een continuïteitsvoorziening opgenomen.

5.5 Naleving wet- en regelgeving

Voor de naleving van wet- en regelgeving geldt in hoofdlijnen hetgeen gesteld is in paragraaf 4.5. Aanvullend wordt gemeld dat het informatiebeveiligingsbeleid en -plan van Logius als eis in het contract voor de nieuwe Digipoort voorziening zijn opgenomen zodat de implementatie in opzet is geborgd. Voor de verantwoording 2010 zal de naleving van het informatiebeveiligingsbeleid en -plan een belangrijk aandachtspunt zijn.

5.6 Conclusie

Het stelsel van beheersingsmaatregelen voor de dienst Digipoort heeft in de verantwoordingsperiode een voldoende invulling aan het normenkader gegeven. De in dit hoofdstuk gesignaleerde verbeterpunten worden onder regie van Logius opgepakt.

6 Bevindingen Haagse Ring

6.1 Algemeen

De Haagse Ring (onderdeel van Diginetwerk, voorheen KPS) 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.

Met 'aangesloten organisaties' worden in deze context de op de Haagse Ring aangesloten ministeries bedoeld. In de praktijk wordt gebruik gemaakt van virtuele netwerken (VPN's) op de Haagse Ring waarmee naar wens verbindingen tussen aangesloten netwerken kunnen worden gerealiseerd. In december 2009 waren 22 VPN's op de Haagse Ring gerealiseerd waarvan het Rijksweb VPN een algemeen bekend voorbeeld is. Voor de goede orde: dit VPN verzorgt het datatransport voor het Rijksweb. De (web)servers van Rijksweb maken geen onderdeel uit van de Haagse Ring dienstverlening.

In dit hoofdstuk wordt ingegaan op de uitvoering van de taken van Logius met betrekking tot Haagse Ring naar de stand van 31 december 2009.

6.2 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. De programmaraad van Logius vormt het bestuur van Haagse Ring. Het bestuur vervult de rol van strategisch beheerder en van gedelegeerd opdrachtgever. Het ministerie van BZK is de bestuurlijke opdrachtgever van de 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, vragen te stellen. 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.

In de paragraaf 6.3 'Informatiebeveiliging Haagse Ring' wordt op het tactisch security management ingegaan. Op het aansluitingen-beheerproces wordt in paragraaf 6.4 ingegaan.

6.3 Informatiebeveiliging Haagse Ring

In de afspraken voor Haagse Ring met Ivent is opgenomen dat het standaard beveiligingsniveau van de Haagse Ring 'departementaal vertrouwelijk' is, zoals bedoeld in het VIR-BI. Voor de realisatie hiervan wordt vertrouwd op Ivent. Er is niet afgesproken dat Ivent 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 aansluitingen-beheerproces van Logius waarbij het foutief doorgeven van wijzigingen kan leiden tot onbedoelde verbindingen of verstoringen.

In het Referentiekader Informatiebeveiliging Haagse Ring versie 1.1 d.d. 11 oktober 2006 is de tweejaarlijkse evaluatie van dit kader en van de onderliggende documenten belegd bij Logius. Het uitgangspunt van Logius is dat deze taak in voldoende mate wordt ingevuld door deel te nemen aan het 'Informatiebeveiligingsberaad'. Dit is een interdepartementaal gremium met als onderwerp informatiebeveiliging. Hieraan nemen ondermeer de aangesloten departementen en de bestuurlijke opdrachtgever deel. Het oorspronkelijk referentiekader is hier ook besproken. Aangezien uit het Informatiebeveiligingsberaad geen signaal naar voren is gekomen dat het Referentiekader Informatiebeveiliging HR niet meer voldoende actueel is, heeft Logius het in 2009 niet noodzakelijk gevonden het kader te evalueren.

In het referentiekader is opgenomen dat bij de realisatie van een nieuwe aansluiting op de Haagse Ring de beveiligingsambtenaar van het betrokken departement schriftelijk aangeeft dat wordt voldaan aan de aansluitvoorwaarden voor Haagse Ring. Overigens is bij de start van Haagse Ring (voor inbeheername door Logius) deze procedure niet gevolgd. Voor nieuwe aansluitingen wordt deze procedure wel gevolgd. Eind 2009 heeft Logius vastgesteld dat aansluitvoorwaarde 6 voor Haagse Ring niet wordt nageleefd. Hierin is opgenomen dat aangesloten organisaties jaarlijks een mededeling verstrekken van de departementale auditdienst of een onafhankelijke derde waaruit blijkt dat het beheer en de beveiliging van de eigen netwerkinfrastructuur adequaat zijn en derhalve geen bedreiging vormen voor de overige Haagse Ring partijen. Logius is voornemens om in de eerste helft van 2010 het referentiekader voor te leggen aan het Informatiebeveiligingsberaad met de vraag of met het huidige gebruik van dit kader de belangrijkste risico's in voldoende mate worden afgedekt.

6.4 Aansluitingenbeheer

Logius heeft een specifiek aansluitingenbeheerproces gerealiseerd, met name gericht op het vertalen van wijzigingsverzoeken van klanten van Haagse Ring naar opdrachten voor Ivent inclusief de afhandeling van financiële, juridische en communicatieve aspecten. Hierbij wordt gebruik gemaakt van de standaard wijzigingenregistratie van Logius. Een onderdeel hiervan is een impliciete toetsing van wijzigingen aan de aansluitvoorwaarden Haagse Ring. Deze stap is echter nog niet expliciet in het proces opgenomen.

Voor 2010 voorziet Logius de volgende verbeteringen rondom het aansluitingenbeheerproces voor Haagse Ring:

- integratie van het specifieke aansluitingenbeheerproces voor Haagse Ring in de generieke processen van Logius;
- expliciet zichtbaar maken van de toetsing van een wijziging aan de aansluitvoorwaarden voor Haagse Ring.

6.5

Conclusie

Het beeld op hoofdlijnen is dat de beheersmaatregelen voor Haagse Ring bij Logius voldoende conform de normen zijn ingevuld naar de stand van 31 december 2009. Een belangrijk voornemen is om in de eerste helft van 2010 het Referentiekader Informatiebeveiliging Haagse Ring voor te leggen aan het Informatiebeveiligingsberaad met de vraag of met het huidige gebruik van dit kader de belangrijkste risico's van Haagse Ring in voldoende mate worden afgedekt.

7 Bevindingen PKIoverheid

7.1 Algemeen

Public Key Infrastructure voor de overheid, kortweg PKIoverheid is een stelsel van afspraken dat generiek en grootschalig gebruik mogelijk maakt van de rechtsgeldige elektronische handtekening en dat identificatie op afstand en vertrouwelijke elektronische communicatie binnen en met de Staat der Nederlanden faciliteert. Overheidsorganisaties kunnen PKI certificaten bijvoorbeeld gebruiken voor het beveiligen van websites en versleuteling van berichtenverkeer. PKIoverheid is te gebruiken voor digitaal berichtenverkeer tussen overheid en overheid, overheid en burgers en overheid en bedrijven.

De zogenaamde 'Policy Authority' (PA) ondersteunt de minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer van PKIoverheid. Logius vult de rol van de PA voor PKIoverheid in. De doelstelling van de PA voor PKIoverheid is: 'Het handhaven van een werkbaar en betrouwbaar normenkader voor PKI-diensten dat voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en dat transparant is voor de gebruikers.

De taken van de PA voor PKIoverheid zijn:

- het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader dat aan de PKI voor de overheid ten grondslag ligt, het zogeheten Programma van Eisen (PvE);
- het proces van toetreding door Certification Service Providers (CSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

7.2 Certificaatautoriteit en -dienstverleners

De basis voor het gehele PKIoverheid afsprakenstelsel wordt gevormd door de certificaatautoriteit (CA) die het beheer over het root certificaat (dit is de 'moedersleutel' voor de gehele PKIoverheid) en het domein certificaat uitvoert. Daarnaast zijn de CSP's die de PKIoverheid-certificaten uitgeven onderdeel van het afsprakenstelsel.

De taken van de CA PKIoverheid zijn:

- de inrichting en beheer en beschikbaarstelling van de Beveiligde Omgeving met daarin het Systeem;
- de inrichting en het beheer van een Overheids Certificatie Autoriteit die het Root certificaat produceert en beheert, en de productie en het beheer van Domein certificaten voor de Domein Certificatie Autoriteiten;
- de inrichting en het beheer van verschillende Domein Certificatie Autoriteiten, die in de onderscheiden domeinen certificaten uitgeven aan certificatie-dienstverleners, en die deze certificaten beheren;
- de inrichting en het beheer van een Directory Service om aangemaakte Certificaten en CRL's benaderbaar te maken via internet;

- de productie in opdracht van de PA van CA-certificaten voor CSP's en het intrekken in opdracht van de PA van CA-certificaten voor CSP's, inclusief de daarbij behorende administratieve handelingen zoals het bijwerken van de CRL (Certificate Revocation List);
- het beheer namens Logius binnen de specifieke, door de Logius vastgestelde beveiligingseisen voor diverse CA's. Hierbij wordt opgemerkt dat een CSP fungeert als een CA voor de door haar uitgegeven certificaten.

De taken van de CA PKIoverheid worden uitgevoerd door een externe certificaatautoriteit. Meerdere CSP's zijn tot de hiërarchie van PKIoverheid toegetroten die toestemming hebben om PKIoverheid-certificaten uit te geven.

Op de dienstverlening van de CA PKIoverheid vindt jaarlijks een audit plaats in opdracht van Logius. Deze audit heeft ook betrekking op een groot deel van de werkzaamheden van de PA PKIoverheid. In de volgende paragraaf wordt nader op deze audit ingegaan. Ook de CSP's zijn contractueel verplicht om jaarlijks een audit uit te laten voeren op basis van de hiervoor geldende standaard Etsi 101456. De CSP's kunnen hierbij kiezen uit twee partijen en verstrekken de uitkomsten van deze audits aan Logius in haar rol van PA. Logius neemt kennis van deze rapportages en reageert indien nodig. Logius onderzoekt in 2010 of de juridische basis voor het ondernemen van actie richting de CSP in het geval van negatieve auditbevindingen versterking behoeft.

7.3 Audit certificaatautoriteit

Het American Institute of Certified Public Accountants (AICPA) heeft een normenkader ontwikkeld om zekerheid te verschaffen over de werkwijze en de beheersmaatregelen met betrekking tot de operationele activiteiten van de certificaatautoriteit (CA). Het "AICPA/CICA WebTrust Program for Certification Authorities" normenkader heeft betrekking op de aanvraag, distributie, melding over aantasting, intrekking en vernieuwing van certificaten, registratie van certificaathouders en verwerking van informatie over de status van het certificaat.

Drie principes in het normenkader zijn belangrijk:

1. CA Business Practices Disclosure – de CA maakt afspraken openbaar over sleutel- en certificaat procedures en levert diensten conform die afspraken;
2. Service Integrity – de CA heeft effectieve maatregelen getroffen om de integriteit en de authenticiteit van haar diensten te waarborgen;
3. CA Environmental Controls – de CA heeft effectieve maatregelen getroffen ten aanzien van autorisatie, continuïteit van sleutel en certificaat en de integriteit van haar systemen.

Het normenkader wordt gebruikt voor de jaarlijkse beoordeling van de CA. Deze beoordeling vindt plaats door een onafhankelijke partij. Bij de CA zijn over 2009 geen materiële afwijkingen van de normen geconstateerd.

7.4 Conclusie

De conclusie van Logius is dat de beheersmaatregelen bij de certificaatautoriteit in de periode 1 januari 2009 tot en met 31 december 2009 in voldoende mate invulling hebben gegeven aan het normenkader.

Bijlage I Lijst met afkortingen

AICPA	American Institute of Certified Public Accountants
BiSL	Business Information Services Library
BTS	Base Tranceiver Station (onderdeel GSM infrastructuur)
CA	Certification Authority
CICA	Canadian Institute of Chartered Accountants
CMDB	Configuration Management Database
CRL	Certificate Revocation List
CSP	Certification Service Provider
DAP	Dossier Afspraken en Procedures
DigiD	Digitale Identiteit
FAQ	Frequently Asked Questions
ICT	Informatie- en Communicatietechnologie
IT	Informatietechnologie
GBA	Gemeenschappelijke Basis Administratie
GBA-V	Gemeentelijke Basis Administratie Verstrekkingen
OTP	Overheidstransactiepoort (Nu: Digipoort)
PA	Policy Authority
PvE	Programma van Eisen
PKI	Public Key Infrastructure
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNO	Service Niveau Overeenkomst
TPM	Third Party Mededeling
VIR	Voorschrift Informatiebeveiliging Rijksoverheid
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens