



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

2011-2000484307

> Retouradres Postbus 20011 2500 EA Den Haag

[Redacted]

DG Organisatie en
Bedrijfsvoering Rijk
Logius, Bedrijfsvoering

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.minbzk.nl

Contactpersoon

[Redacted]

Datum 16 november 2011
Betreft Uw verzoek om informatie

Kenmerk
2011-2000484307

Bijlagen
1

Geachte heer [Redacted]

Bij e-mailbericht van 21 oktober 2011 heeft u bij mijn ministerie een verzoek ingediend, als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna: Wob) en een feitelijke vraag gesteld.

Op 25 oktober 2011 is uw feitelijke vraag telefonisch beantwoord.

Uw verzoek heeft betrekking op het calamiteitenplan van Logius, de Dienst Digitale Overheid van mijn ministerie.

Op 27 oktober 2011 is de ontvangst van uw verzoek schriftelijk bevestigd.

Met betrekking tot uw verzoek om informatie bericht ik u als volgt.

Ik verstrek u hierbij het calamiteitenplan van Logius, getiteld 'Handboek incident-calamiteitenbeheer'.

U zult zien dat op enkele plaatsen in de tekst gegevens onleesbaar zijn gemaakt. Dit betreft op de pagina's 2, 20, 26, 28, 41, 88, 89 en 95 de namen van functionarissen en andere individuele personen, en hun contactgegevens zoals directe (mobiele) telefoonnummers. Deze gegevens maak ik niet openbaar in verband met de eerbiediging van de persoonlijke levenssfeer van betrokkenen, welk belang wordt vermeld in artikel 10, tweede lid, aanhef en onder e, van de Wob. Dit belang afwegende tegen het belang van openbaarmaking van deze gegevens, acht ik het belang genoemd in artikel 10, tweede lid, aanhef en onder e, van de Wob zwaarwegender.

Verder zijn op pagina 90 enkele URL's naar beheerpagina's onleesbaar gemaakt. Deze maak ik evenmin openbaar. Deze beheerlinks maken toegang mogelijk tot de beheeromgeving van DigiD. De links zijn door hun opbouw specifiek en vormen aldus een beveiligingsmaatregel voor DigiD. Openbaarmaking ervan vergroot de kans op misbruik van DigiD door kwaadwillenden. Dit moet worden voorkomen. DigiD is immers het nationale authenticatiemiddel waarmee honderden overheidsorganisaties hun communicatie beveiligen. Ik beroep mij hierbij op het belang van inspectie, controle en toezicht door de Rijksoverheid en op het belang

Pagina 1 van 2

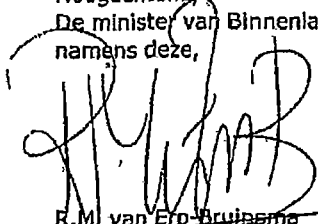
1711201109024

van het voorkomen van onevenredige benadeling van bij de aangelegenheid betrokken andere overheidsorganisaties die met DigiD hun communicatie beveiligen. Het belang van openbaarmaking van de URL's weegt naar mijn overtuiging niet op tegen deze in artikel 10, tweede lid, aanhef en onder d en g, van de Wob genoemde belangen.

Datum
16 november 2011
Kenmerk
2011-2000484307

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend
De minister van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,



R.M. van Erp-Bruinsema
Secretaris-generaal

Bijlage: Handboek incident-calamiteitenbeheer

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit daartegen per brief bezwaar maken bij de minister van Binnenlandse Zaken en Koninkrijksrelaties, DG OBR/Logius, Postbus 20011, 2500 EA Den Haag. Het bezwaarschrift moet zijn ondertekend, voorzien zijn van een datum alsmede de naam en het adres van de indiener en dient vergezeld te gaan van de gronden waarop het bezwaar berust en, zo mogelijk, een afschrift van het besluit waartegen het bezwaar is gericht.



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Handboek incident-calamiteitenbeheer

Versie 2.8

Datum	7 juni 2011
Status	definitief

Colofon

Projectnaam	Handboek P1
Versienummer	2.7
Contactpersoon	
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Gerelateerde documenten	Quick Reference Cards I:\Logius\ServiceManagement\Incidentbeheer Werkinstructie MailPlus I:\Logius\ServiceManagement\Incidentbeheer

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
01-04-2010	2.0	[REDACTED]	Gewijzigde opzet i.v.m. aangescherpt Incidentbeheer
02-04-2010	2.1	[REDACTED]	Contactgegevens leveranciers uitgebreid met management, rol standby manager beschreven, lijst mogelijke leden calamiteitenteam up-to-date gebracht
06-04-2010	2.11	[REDACTED]	Mobiele nummers van medewerkers Dienstverlening toegevoegd
03-05-2010	2.2	[REDACTED]	Diverse aanpassingen n.a.v. reviews door Tjeerd Bosgraaf, servicebeheerders en MT-leden. Scope uitgebreid naar incident- en calamiteitenbeheer (waaronder de standby dienst)
09-08-2010	2.3	[REDACTED]	Diverse aanpassingen n.a.v. evaluaties met servicebeheerders en de afdeling Dienstverlening. Betreft vooral communicatie
17-09-2010	2.4	[REDACTED]	Aanpassingen nav MT, P1 droog oefeningen en opmerkingen-Functioneel beheerders.
14-01-2011	2.5	[REDACTED]	DigiD-Machtigen, Manifestgroep, Zoekdienst & aanpassing 4.5.3.2
16-06-2011	2.6	[REDACTED]	DigiD voor bedrijven verwijderen. Diagnoses stellen 3.3.2.3. Evaluatie 3.3.10 Typo3 URL's Handboek typo3 URL toegevoegd DigiD Machtigen toevoegingen Splitsing Werkinstructie MailPlus
6-9-2011	2.7	[REDACTED]	SMS naar MT leden ten alle tijden. 5.4.1 workflow toegevoegd

3.3.6 communicatie

3.3.10 incidentmanager bepaald evaluatie

ja of nee / evaluatie versturen

Nieuwe organisatiestructuur is doorgevoerd

Inhoud

Colofon	2
Inhoud	4
Inleiding	8
1.1 Doel van document.....	8
1.2 Doelgroep.....	8
1.3 Leeswijzer	8
1.4 Documentbeheer	8
1.5 Gerelateerde documenten.....	8
1.6 Distributie.....	9
2 Kaderstelling	10
2.1 Logius organisatie.....	10
2.2 Logius dienstverlening.....	10
2.2.1 Vormen van dienstverlening	10
2.2.2 Elektronische dienstverlening.....	10
2.2.3 Gebruikersondersteuning	11
2.3 Product- en supportdomein.....	12
2.4 Definities	13
2.4.1 Incident	13
2.4.2 Calamiteit	14
3 Processen incidentbeheer en calamiteitenbeheer.....	15
3.1 Doel.....	15
3.2 Proces op hoofdlijnen	15
3.3 Proces in detail.....	18
3.3.1 Intake	18
3.3.2 Analyse.....	18
3.3.3 Herstellen	19
3.3.4 Afsluiten	19
3.3.5 Bewaking	19
3.3.6 Communicatie.....	19
3.3.7 Escaleren (optioneel).....	22
3.3.8 Formeren calamiteitenteam (bij calamiteit)	23
3.3.9 Formeren herstelteam (bij calamiteit).....	24
3.3.10 Evalueren/verbeteren (bij P1 incident of calamiteit).....	24
3.3.11 Afleggen bestuurlijke verantwoording (bij calamiteit).....	24
4 Organisatie.....	25
4.1 Relevante Logius partijen.....	25
4.2 Bereikbaarheid	25
4.2.1 Algemeen.....	25
4.2.2 Tijdens kantooruren	26
4.2.3 Buiten kantooruren (standby dienst)	26

4.3	<i>Standby dienst</i>	27
4.3.1	Standby team	27
4.3.2	Bereikbaarheid standby team	27
4.3.3	Afspraken rondom standby dienst	28
4.3.4	Standby rooster	28
4.4	<i>Calamiteitenteam</i>	28
4.5	<i>Rollen, taken en verantwoordelijkheden</i>	29
4.5.1	Directeur Logius.....	30
4.5.2	Standby manager.....	30
4.5.3	Incidentmanager.....	31
4.5.4	Woordvoerder Logius.....	32
5	Communicatie	33
5.1	<i>Algemene uitgangspunten bij communicatie</i>	33
5.2	<i>Woordvoerder in calamiteitenteam</i>	33
5.3	<i>Interne communicatie</i>	34
5.4	<i>Media</i>	34
5.4.1	Geen storing, maar wel in de media	35
5.5	<i>Klanten</i>	35
5.6	<i>Politiek en opdrachtgevers</i>	36
5.7	<i>Communicatiemiddelen</i>	36
6	Producten	37
6.1	<i>DigiD voor burgers</i>	37
6.1.1	Globale werking	37
6.1.2	Systeemlandschap	38
6.1.3	Dienstverlening.....	38
6.1.4	Prioriteiten & oplostijden	40
6.1.5	Leverancier(s)	42
6.1.6	Oplostijden leveranciers.....	42
6.2	<i>Eenmalig inloggen</i>	45
6.2.1	Globale werking	45
6.2.2	Systeemlandschap	45
6.2.3	Dienstverlening.....	46
6.2.4	Prioriteiten & oplostijden	46
6.2.5	Leverancier(s)	46
6.2.6	Oplostijden leveranciers.....	46
6.3	<i>DigiD Machtigen</i>	48
6.3.1	Globale werking	48
6.3.2	Dienstverlening.....	48
6.3.3	Prioriteiten & oplostijden	51
6.3.4	Leverancier(s)	53
6.3.5	Oplostijden leveranciers.....	53
6.4	<i>PKIoverheid</i>	57
6.4.1	Globale werking	57
6.4.2	Dienstverlening.....	57
6.4.3	Prioriteiten & oplostijden	57
6.4.4	Leverancier(s)	57
6.5	<i>Digipoort X.400/SMTP/FTP/POP3/SOAP</i>	59

6.5.1	Globale werking	59
6.5.2	Dienstverlening	59
6.5.3	Prioriteiten & oplostijden	60
6.5.4	Leveranciers	61
6.5.5	Calamiteitenbeheer	61
6.6	<i>Berichtenspiegel</i>	63
6.6.1	Werking	63
6.6.2	Dienstverlening	63
6.6.3	Prioriteiten & oplostijden	63
6.6.4	Leveranciers	64
6.7	<i>Digikoppeling</i>	65
6.7.1	Werking	65
6.7.2	Dienstverlening	65
6.7.3	Prioriteiten & oplostijden	66
6.7.4	Leveranciers	67
6.8	<i>Stelselcatalogus</i>	68
6.8.1	Werking	68
6.8.2	Dienstverlening	68
6.8.3	Prioriteiten & oplostijden	68
6.8.4	Leveranciers	68
6.9	<i>Digimelding</i>	69
6.9.1	Werking	69
6.9.2	Dienstverlening	69
6.9.3	Prioriteiten & oplostijden	69
6.9.4	Leveranciers	69
6.10	<i>Inspectieruimte BRZO</i>	70
6.10.1	Werking	70
6.10.2	Dienstverlening	70
6.10.3	Prioriteiten & oplostijden	72
6.10.4	Leveranciers	73
6.11	<i>Manifestgroep</i>	74
6.11.1	Werking	74
6.11.2	Dienstverlening	74
6.11.3	Classificatie en prioritering van de incidenten	76
6.11.4	Betrokken leveranciers	77
6.11.5	Prioriteiten & oplostijden	77
6.11.6	Leveranciers	77
6.12	<i>Inspectieview bedrijven</i>	78
6.12.1	Werking	78
6.12.2	Dienstverlening	78
6.12.3	Prioriteiten & oplostijden	80
6.12.4	Leveranciers	81
6.13	<i>Zoekdienst</i>	83
6.13.1	Werking	83
6.13.2	Dienstverlening	83
6.13.3	Prioriteiten & oplostijden	84
6.13.4	Leveranciers	86
7	Beheermiddelen	88
7.1	<i>Mobiele telefoon</i>	88
7.1.1	Tactisch beheer	Fout! Bladwijzer niet gedefinieerd.
7.1.2	Servicecentrum	88

7.1.3	MT-leden.....	89
7.2	Laptop.....	89
7.2.1	Inrichting laptop	89
7.2.2	Gebruik laptop op kantoor.....	90
7.2.3	Gebruik laptop thuis	90
7.3	Beheeromgevingen	90
7.3.1	DigiD voor burger.....	90
7.3.2	DigiD voor bedrijven.....	90
7.4	Watchmouse	91
7.4.1	Achtergrond	91
7.4.2	Website DigiD.....	91
7.4.3	Authenticatieserver voor burgers	91
7.4.4	Authenticatieserver voor klanten.....	92
7.4.5	Applicatieserver voor DigiD	92
7.4.6	DigiD voor bedrijven.....	92
7.4.7	Digipoort (SOAP).....	92
7.5	MailPlus.....	93
7.5.1	Communicatie.....	93
7.6	Handboek incident- en calamiteitenbeheer.....	93
7.7	Quick Reference kaart	94
8	Contactgegevens	95
8.1	Logius	95
8.2	Klanten	95
8.2.1	Belastingdienst	95
8.2.2	Digipoort klanten	95
8.3	Leveranciers	96
BIJLAGE A: Bekende fouten		97

Inleiding

1.1 Doel van document

Dit document is bedoeld als naslagwerk voor het afhandelen van incidenten en calamiteiten binnen Logius. Elke Logius medewerker die hierbij potentieel betrokken is, dient dit document in hardcopy beschikbaar te hebben.

Naast dit document bestaan er twee 'quick references' kaarten (een voor incidentbeheer en een voor calamiteitenbeheer) waarop de belangrijkste informatie staat. Daarnaast is er een lijst met contactgegevens.

1.2 Doelgroep

Dit document is uitsluitend bestemd voor gebruik binnen Logius. De beoogde gebruikers zijn de Logius medewerkers die betrokken zijn bij de uitvoering van incident- en calamiteitenbeheer:

- Medewerkers Tactisch beheer
- Medewerkers Servicecentrum
- MT-leden
- Woordvoerder

1.3 Leeswijzer

Hoofdstuk 2 beschrijft het kader voor de organisatorische en procesmatige inrichting van incident- en calamiteitenbeheer. Hoofdstuk 3 gaat in op het proces voor incident- en calamiteitenbeheer. De organisatie voor incident- en calamiteitenbeheer wordt in hoofdstuk 4 behandeld. Communicatie tijdens de afhandeling van een incident of calamiteit wordt besproken in hoofdstuk 5. De Logius producten en de dienstverlening rondom deze producten wordt besproken in hoofdstuk 6. Hoofdstuk 7 gaat tenslotte in op de aanwezige middelen, die kunnen worden gebruikt bij de uitvoering van incident- en calamiteitenbeheer.

1.4 Documentbeheer

Dit document wordt up-to-date gehouden en beheerd door afdeling Tactisch beheer.

1.5 Gerelateerde documenten

Naam document	Datum	Versie	In beheer bij
Continuïteitsplan	03-05-2009	0.1	Informatiebeveiliging
Quick Reference Card Incidentbeheer	03-10-2010		Tactisch beheer
Quick Reference Card Calamiteitenbeheer	03-10-2010		Tactisch beheer
Standby rooster			Tactisch beheer
Logboek incident/calamiteit	02-04-2010		Tactisch beheer
Registratieformulier incident/calamiteit	02-04-2010		Tactisch beheer
Plaatsen serviceberichten CMS DigiD v01	6-1-2009	0.1	Communicatie
Plaatsen serviceberichten CMS Logius			Communicatie

1.6

Distributie

Afdeling Tactisch beheer ziet erop toe dat dit document wordt gedistribueerd naar alle Logius medewerkers die een rol hebben in incident- en calamiteitenbeheer (zie paragraaf 1.2).

2 Kaderstelling

2.1 Logius organisatie

Logius is de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Logius beheert overheidsbrede ICT-oplossingen en gemeenschappelijke standaarden, die de communicatie tussen overheden, burgers en bedrijven vereenvoudigen. Met oog voor de samenhang in de infrastructuur van de e-overheid.

2.2 Logius dienstverlening

2.2.1 Vormen van dienstverlening

Logius kent twee vormen van dienstverlening:

<i>vorm</i>	<i>beschrijving</i>
Elektronische dienstverlening	Dit zijn de producten (overheidsbrede ICT oplossingen en standaarden, zie 2.1) die Logius levert aan overheidsorganisaties en eindgebruikers (burgers, bedrijven). Deze producten worden in operationele zin geëxploiteerd door leveranciers van Logius.
Gebruikersondersteuning	Logius biedt overheidsorganisaties en eindgebruikers ondersteuning aan bij het gebruik van en aansluiting op producten. Burgers kunnen zich hiervoor melden bij de Helpdesk. Overheidsorganisaties en bedrijven melden zich bij het Servicecentrum.

De beide vormen van dienstverlening aan burgers, bedrijven en overheidsorganisaties zijn vastgelegd in gebruiksvoorwaarden (burger, bedrijven) en aansluitvoorwaarden/serviceniveau overeenkomsten (overheidsorganisaties).

2.2.2 Elektronische dienstverlening

Logius levert onderstaande producten als elektronische dienstverlening:

<i>Productlijn</i>	<i>Producten</i>
Toegang	DigiD burgers
	Eenmalig inloggen
	DigiD Machtigen
	PKIoverheid
Gegevensuitwisseling	Digipoort
	Digikoppeling

	Diginetwerk
	Digimelding
	Stelselcatalogus
	Inspectieview bedrijven
	Inspectieruimte BRZO
Informatiebeveiliging*	GOVCERT.NL
	Waarschuwingsdienst.nl
Standaardisatie*	Forum Standaardisatie
	College Standaardisatie
	Bureau Forum Standaardisatie

*voor deze producten geldt de incidenten/calamiteitenprocedure niet.

De producten (elektronische dienstverlening) worden in operationele zin geëxploiteerd door leveranciers van Logius. Met deze leveranciers zijn door Logius overeenkomsten, serviceniveau overeenkomsten (SNO) en operationele afspraken (DAP) overeengekomen om de elektronische dienstverlening aan burgers, bedrijven en overheidsorganisaties te waarborgen.

Zie hoofdstuk 3 voor de overeengekomen dienstverlening aan burgers/klanten t.a.v. de producten en die door de Logius leveranciers.

Indien er een (dreigende) verstoring is in bovenstaande dienstverlening, is er sprake van een incident of calamiteit.

2.2.3

Gebruikersondersteuning

Ten behoeve van de ondersteuning op Logius producten is onderstaande gebruikersondersteuning ingericht.

Doelgroep	Ondersteuning door	voor producten
Burgers	Helpdesk (extern callcenter)	DigiD voor burgers, Eenmalig Inloggen, DigiD Machtigen ¹
Bedrijven	Servicecentrum	Digipoort
Overheidsorganisaties	Servicecentrum	DigiD voor burgers, Eenmalig Inloggen, DigiD Machtigen, PKIoverheid, Mijnoverheid.nl, Digipoort,

¹ Logius voert 'werk in opdracht' uit voor ICTU. DigiD Machtigen is nog niet in beheer bij Logius.

		Digikoppeling, Diginetwerk, Digimelding, Inspectievlew bedrijven, Inspectieruimte BRZO, Stelselcatalogus.
--	--	--

De dienstverlening door de Helpdesk is als volgt:

Bereikbaarheid	Telefoon: 0800-0230435 E-mail: info@digid.nl
Openstelling	Werkdagen van 08:00 – 22:00 uur
Beschikbaarheid	Telefoon: 99,5% E-mail: 99,5%

De dienstverlening door het Servicecentrum is als volgt:

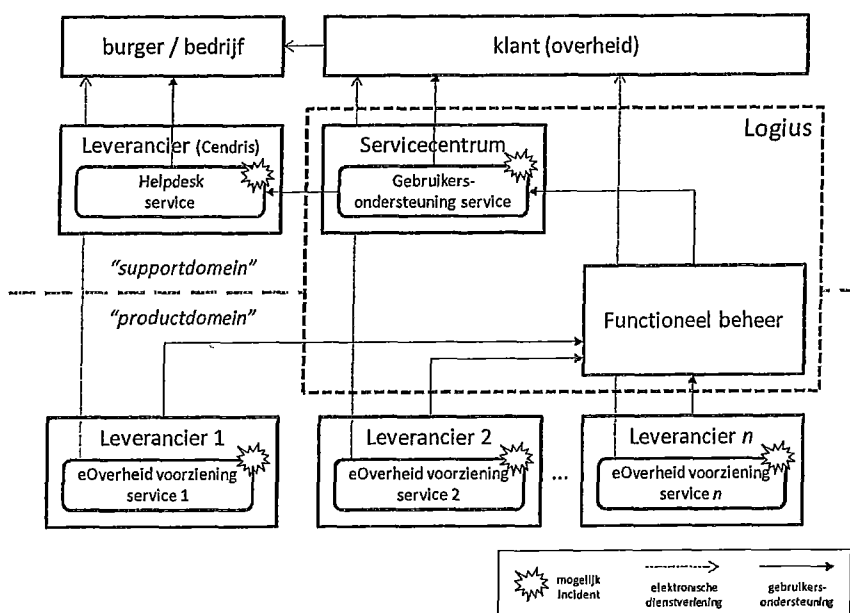
Bereikbaarheid	Telefoon: 0900-5554555 E-mail: servicecentrum@logius.nl
Openstelling	Werkdagen van 08:00 – 17:00 uur
Beschikbaarheid	Telefoon: 99,5% E-mail: 99,5%

Indien bovenstaande dienstverlening niet (volledig) wordt geboden, is er sprake van een incident of calamiteit.

2.3

Product- en supportdomein

Een verstoring kan zich voordoen in het 'productdomein' (de elektronische dienstverlening) of het 'supportdomein' (het Servicecentrum en Helpdesk die support/ondersteuning bieden aan gebruikers van de producten). Zie onderstaande figuur.



Figuur 1: support- en productdomein

Voorbeeld: het niet telefonisch bereikbaar zijn van DigiD Helpdesk of het Servicecentrum is een voorbeeld van een incident in het *supportdomein*. Het niet beschikbaar zijn van DigiD of Digipoort is een voorbeeld van een incident in het *productdomein*.

Dit onderscheid is van belang, omdat dit bepaalt welke afdeling verantwoordelijk is bij een verstoring van de dienstverlening. Bij een verstoring van de dienstverlening in het supportdomein (onbereikbaarheid/onbeschikbaarheid van Helpdesk en/of Servicecentrum) is gedurende de kantooruren de afdeling Dienstverlening verantwoordelijk. Na kantooruren is de Incidentmanager van Servicemanagement het aanspreekpunt. De Incidentmanager plaatst in dit geval een mededeling op de website en informeert het management. Verder actie is niet noodzakelijk. Het Servicecentrum pakt de volgende dag de vervolgacties op.

Bij een verstoring in het productdomein is afdeling Servicemanagement verantwoordelijk.

2.4 Definities

2.4.1 Incident

Een 'incident' is een (dreigende) verstoring van de dienstverlening van Logius. De dienstverlening van Logius bestaat uit:

- elektronische dienstverlening (e-overheid voorziening), veelal door leveranciers. Zie paragraaf 2.2.2.
- gebruikersondersteuning op elektronische dienstverlening (vragen/verzoeken/klachten, aansluiten). Zie paragraaf 2.2.3.

Een incident met prioriteit 1 (hoogste prioriteit), waarvan de oplostijd is overschreden of dreigt te worden overschreden en waarvan geen oplossing in zicht is, wordt een calamiteit (zie paragraaf 2.4.2).

N.B.: veiligheidsincidenten hebben altijd de hoogste prioriteit (=P1)

2.4.2

Calamiteit

Een 'calamiteit' is:

- een gebeurtenis die de algehele dienstverlening van Logius in gevaar brengt (bv. bommelding, brand, overstroming)
- een gebeurtenis die de goede naam/imago van Logius in gevaar brengt of leidt tot politieke schade (bv. mediabericht, fraude met Logius product, journalist meldt zich)
- een prio 1 incident waarvan de oplostijd wordt overschreden of dreigt te worden overschreden en waarvan geen oplossing in zicht is
- ter beoordeling aan het dienstdoende afdelingshoofd

3 Processen incidentbeheer en calamiteitenbeheer

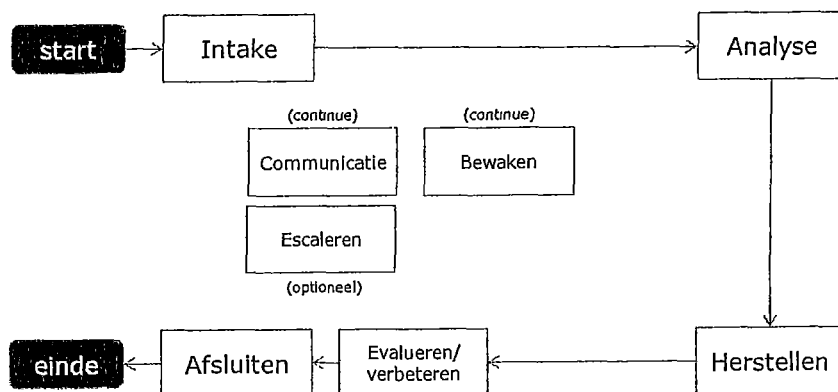
3.1 Doel

Het proces incidentbeheer heeft tot doel het wegnemen of verminderen van de gevolgen van (dreigende) verstoringen van de dienstverlening (zie paragraaf 2.2 voor de definitie van dienstverlening) en ervoor zorgen dat de dienstverlening zo snel mogelijk weer op het overeengekomen niveau komt.

Het doel van calamiteitenbeheer is de omvang en de gevolgen van een calamiteit zoveel als mogelijk te beperken.

3.2 Proces op hoofdlijnen

De processen voor incidentbeheer en calamiteitenbeheer komen op hoofdlijnen overeen. Hieronder een weergave van het incidentbeheerproces.



Figuur 2: incidentbeheerproces

Voor incidentbeheer is sprake van onderstaande volgordelijke activiteiten:

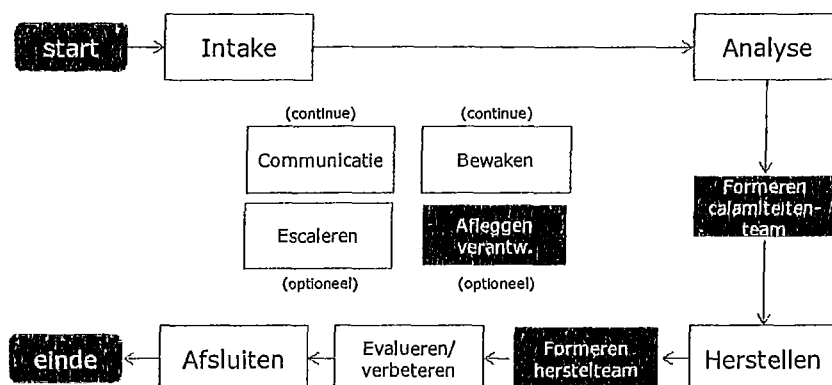
1. Intake: ontvangst of constatering van gebeurtenis, registratie
2. Analyse: classificatie, prioritering, diagnose stellen, communicatie
3. Herstellen: dienstverlening herstellen, communicatie
4. Evalueren/verbeteren (bij een P1 incident)
5. Afsluiten: registratie

Continue activiteiten voor incident- als calamiteitenbeheer zijn:

- Communicatie: over ontstaan, status en afmelding
- Bewaken: monitoren van oplostijd

Tijdens het incidentbeheer proces kan optioneel worden geëscaleerd: horizontaal, verticaal of van een incident naar een calamiteit.

Hieronder is het calamiteitenbeheerproces weergegeven.



Figuur 3: calamiteitenbeheer proces

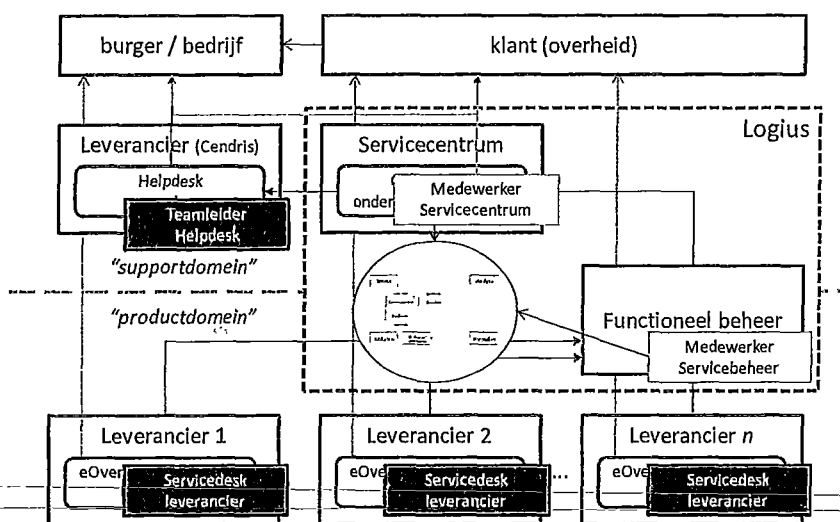
Voor calamiteitenbeheer worden ten opzichte van Incidentbeheer onderstaande extra activiteiten uitgevoerd:

- Formeren calamiteitenteam
- Formeren herstelteam
- Afleggen bestuurlijke verantwoording (optioneel)

De activiteiten worden in paragraaf 3.3 verder in detail beschreven.

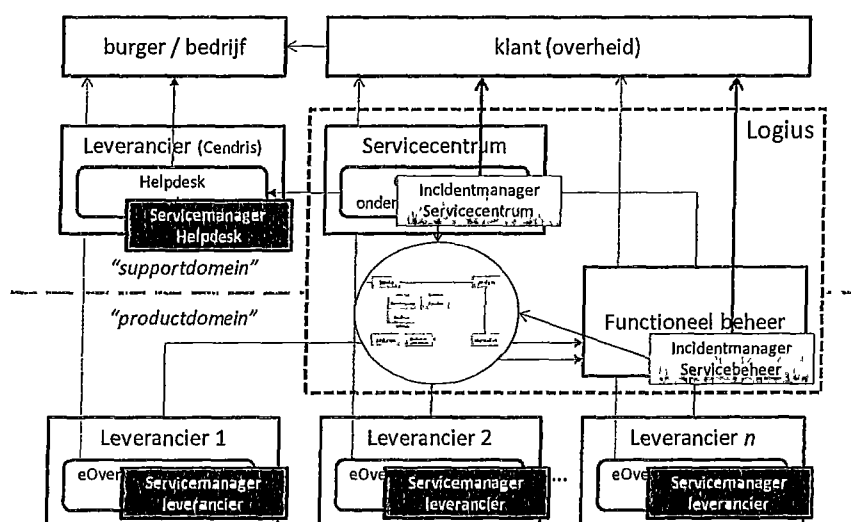
Hoewel de processen voor incident- en calamiteitenbeheer op hoofdlijnen overeenkomen, zijn de actoren verschillend.

Onderstaande figuren laten dit zien.



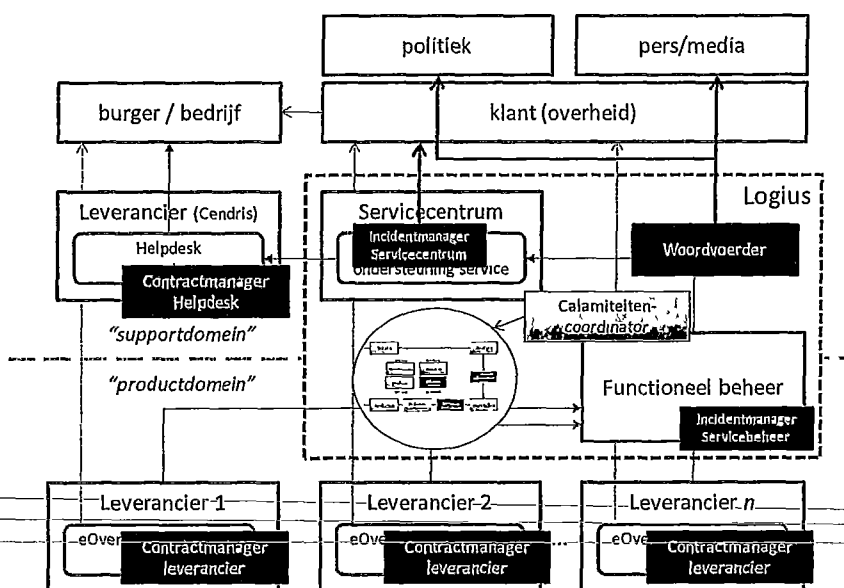
Figuur 4: incidentbeheer (prio < 1)

In **Figuur 4: incidentbeheer (prio < 1)** is te zien dat medewerkers van het Servicecentrum verantwoordelijk zijn voor de afhandeling van incidenten (prio < 1) in het supportdomein en medewerkers van Servicemanagement voor de afhandeling van incidenten in het productdomein. Standaardcommunicatie over het incident vindt plaats via mailplus door de Incidentmanager.



Figuur 5: Incidentbeheer (prio 1)

Figuur 5: incidentbeheer (prio 1) laat de situatie zien bij een P1 incident. De actoren zijn hier veranderd: de incidentmanager van het Servicecentrum is verantwoordelijk voor de afhandeling van incidenten in het supportdomein en de incidentmanager van Servicemanagement is voor de afhandeling van incidenten in het productdomein verantwoordelijk. Standaardcommunicatie over het Incident vindt grootschaliger plaats via mailplus door de Incidentmanager .



Figuur 6: calamiteitenbeheer

Bij een calamiteit, weergegeven in **Figuur 6: calamiteitenbeheer**, neemt de calamiteitencoördinator de regie over van de Incidentmanager. Tevens krijgt de woordvoerder van Logius een rol in de communicatie naar de politiek en de pers/media. De incidentmanagers kunnen een inhoudelijke rol spelen bij de oplossing van de calamiteit.

3.3 Proces in detail

3.3.1 Intake

3.3.1.1 Ontvangst

Een incident/calamiteit kan op diverse manieren ontstaan:

- het Servicecentrum wordt door klanten op de hoogte gesteld van een verstoring
- Tactisch beheer of Servicecentrum constateert zelf een verstoring van de dienstverlening (bv. middels Watchmouse)
- een Logius leverancier meldt een verstoring
- Helpdesk (Cendris) meldt bij het Servicecentrum een sterke toename in het aantal meldingen door burgers
- er meldt zich een journalist (bij de persvoorlichter)
- er staat een bericht in de media
- een Logius medewerker neemt kennis van een gebeurtenis.

De gebeurtenis wordt ten alle tijden gemeld bij het Servicecentrum of Servicemanagement, zodat de afhandeling op een correcte wijze kan starten.

3.3.1.2 Registratie

De gebeurtenis wordt geregistreerd (zie hiervoor de werkinstructie Servicecentrum – Loket of Servicemanagement – Loket). Tijdens kantoortijden gebeurt dit direct in Clientèle door de betreffende medewerker van het Servicecentrum of Servicemanagement.

Buiten kantoortijden vraagt de incidentmanager om de volgende gegevens en noteert deze (in het geval van een P1 incident of calamiteit) in het incident registratieformulier:

- tijdstip inkomende telefoongesprek
- naam, organisatie en telefoonnummer van de beller
- korte omschrijving van het probleem
- tijdstip begin van het probleem of de ontdekking van het probleem
- prioriteit (indien deze al kan worden vastgesteld)
- hoe men het probleem heeft gevonden
- eventueel de mogelijke oorzaak van het probleem
- vervolgstappen af (bijvoorbeeld laten uitzoeken van het probleem en terugbellen).

De gegevens worden op een later tijdstip (maar wel zo snel als mogelijk) geregistreerd in Clientèle.

3.3.2 Analyse

3.3.2.1 Classificeren

Stel vast op welk onderdeel van de dienstverlening de melding betrekking heeft (zie paragraaf 2.2). Bepaal of een soortgelijk incident en herstelactie bekend is. Registreer de bevindingen.

3.3.2.2 Prioriteren

Aan elk incident wordt een prioriteit toegekend. De wijze van prioritering hangt af van het product waarop het incident betrekking heeft. In hoofdstuk 5 is voor elk Logius product aangegeven welke prioriteiten

worden onderkend en welke oplostijden hierbij horen. Ook is beschreven welke oplostijden gelden voor Logius leveranciers.

Registreer de bevindingen.

- 3.3.2.3 *Diagnose stellen*
Analyseren van het incident in het geval er nog geen herstelactie bekend is en vaststellen waar welke mogelijke acties zouden kunnen liggen.

Let op: Informeer het MT altijd via MailPlus, ook als je besluit niet naar klanten te communiceren.

Registreer de bevindingen.

- 3.3.3 *Herstellen*
Herstel zelf de verstoring of schakel een of meerdere leveranciers in om de verstoring te verhelpen.

Zie bijlage B voor een overzicht met bekende fouten ('known errors').

Verstuur indien nodig (in overleg met standby manager) op regelmatige basis met MailPlus email/sms-berichten met een update van de status van de verstoring.

Registreer de uitgevoerde activiteiten.

- 3.3.4 *Afsluiten*
Registreer (bij een P1 incident op het incidentregistratieformulier) het tijdstip dat de dienstverlening weer is hersteld.

Verstuur met MailPlus een email/sms-bericht met een afmelding van de storing aan alle doelgroepen die eerder op de hoogte waren gesteld van de verstoring.

- 3.3.5 *Bewaking*
Tijdens de afhandeling van een incident vindt een continue bewaking plaats van de oplostijd. Indien nodig wordt horizontaal of verticaal geëscaleerd.

In geval van een P1 incident wordt geëscaleerd naar een calamiteit als de oplostijd (die bij de P1 prioriteit hoort) is verstreken of dreigt te verstrijken.

- 3.3.6 *Communicatie*

In het geval van een P1 incident tijdens en buiten kantooruren is de incidentmanager verantwoordelijk voor de uitvoering en coördinatie van de communicatie naar klanten en intern. Uitgangspunt is dat de Incidentmanagersnel de communicatie start. Snel is: de Incidentmanager informeert de externe doelgroep binnen 30 minuten nadat de Incidentmanager tot de conclusie komt dat er sprake is van een P1. Hij verstuurt een standaard bericht via Mailplus en zet een standaardbericht op de website van Interne medewerkers informeert de incidentmanager binnen 10 minuten via Mailplus.

Let op: bovenstaande geldt voor productieverstorende incidenten. Als er sprake is van een niet-productieverstorend incident bijv. fraude of andere

imago schade dan beslist de standbymanager over wel of niet externe communicatie, en wanneer. De Incidentmanager verzorgt ook de berichtgeving over de voortgang en afsluiting van een P1 met Mailplus en via de website van Logius dan wel DigiD.nl. Communicatie naar klanten en Logius medewerkers verloopt per e-mail en/of sms-bericht via MailPlus. Daarnaast wordt er gecommuniceerd via de website van Logius dan wel DigiD.

Indien het nodig is afwijkende berichten te versturen (bijvoorbeeld naar speciale doelgroepen van klanten of als specifieke informatie die voor alle klanten van belang is moet worden verstrekt) of een ander medium (bijv. de website of een brief) in te zetten, dan overlegt de Incidentmanager dit met het team Marketing en Communicatie (woordvoerder) (). De uitvoering hiervan ligt bij Marketing-communicatie. In dit geval coördineert de Incidentmanager de communicatie. Indien noodzakelijk en ter beoordeling van de incidentmanager kan ook Servicecentrum worden ingezet bij de uitvoering.

Communicatie buiten kantooruren

Als er in de nachtelijke uren een P1 voorkomt waarbij bovenstaande niet volstaat, zal de Incidentmanager contact opnemen met de calamiteitenmanager, die vervolgens de woordvoerder van Logius inschakelt om te bepalen welke communicatie nodig is. De incidentmanager verstuurt vervolgens berichten via Mailplus en zet berichten op de website.

In geval van een calamiteit overlegt de standby manager met de woordvoerder en de incidentmanager of, hoe en wat er naar klanten wordt gecommuniceerd.

Bij een calamiteit stelt de calamiteitencoördinator de directeur van Logius en de beleidsopdrachtgever(s)² op de hoogte. Zie de Quick Reference Card Calamiteitenbeheer voor de contactgegevens.

De directeur Logius informeert bij een calamiteiten de ambtelijke staf (DG en SG).

Bij een calamiteit is de woordvoerder/persvoorlichter verantwoordelijk voor de externe communicatie naar pers/media. De wijze en inhoud van externe communicatie wordt hierbij afgestemd met de betreffende contactpersonen van beleidsopdrachtgever(s).

De woordvoerder informeert bij een calamiteit indien noodzakelijk het afdelingshoofd van Dienstverlening. Deze zorgt voor verdere interne communicatie of wijst een contactpersoon voor de woordvoerder aan.

Zie voor meer informatie over de rol van de woordvoerder: hoofdstuk 5.

Doelgroepen voor communicatie

Als er moet worden gecommuniceerd, stel dan vast welke doelgroepen moeten worden geïnformeerd over de verstoring van de dienstverlening.

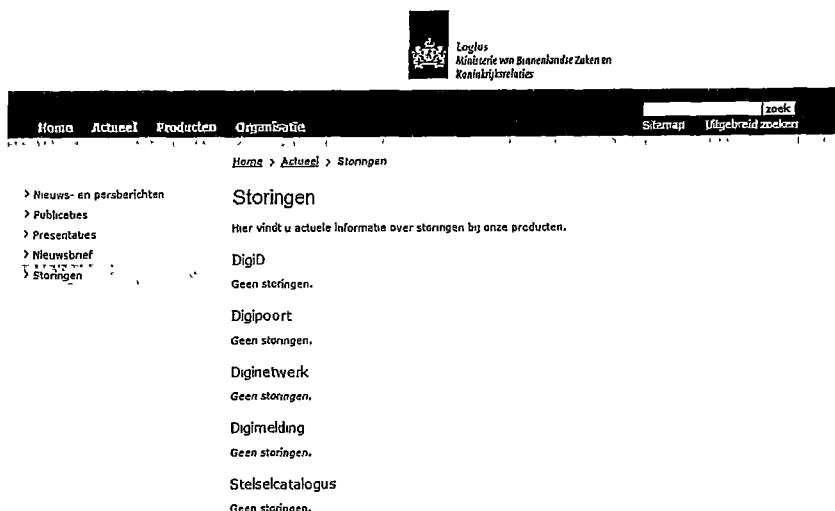
² Dat zijn de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (Programma Dienstverlening, Regeldruk en Informatiebeleid), Economische Zaken, Volksgezondheid, Welzijn en Sport en Onderwijs, Cultuur en Wetenschap.

Mogelijke keuzen zijn:

- alleen intern
- alleen extern
- zowel intern als extern

Daarnaast moet worden vastgesteld of er alleen wordt gecommuniceerd naar de contactpersonen voor een specifiek Logius product of voor alle Logius producten. Alle mogelijke doelgroepen bevinden zich in MailPlus.

NB: Zie werkinstructie Servicecentrum en Tactisch beheer voor



communicatie tijdens een incident met een prioriteit lager dan 1. Deze is te vinden op:
I:\Logius\Ondersteunende_staf\Communicatie\Logius\Website\Handleidingen Handleiding Storingenberichten.

E-mail/sms

Raadpleeg Handleiding MailPlus voor het versturen van e-mail en sms-berichten aan de vastgestelde doelgroepen.

Bij een P1 moet het MT te allen tijden worden ingelicht via Mailplus, per SMS.

Logius website

Op de Logius website (www.logius.nl/actueel/storingen) wordt een servicebericht geplaatst. Zie hieronder.

In de verstuurde e-mail/sms-berichten wordt hiernaar verwezen. Het plaatsen van het bericht verloopt middels het Content Management Systeem (CMS) van de website.

Het CMS kan worden benaderd via de URL:

<http://www.logius.nl/typo3/>

De werkinstructie voor het plaatsen van een bericht is als apart document bijgevoegd.

DigiD website

Op de DigiD website (www.digid.nl) kan een servicebericht worden geplaatst. Het plaatsen van het bericht verloopt middels het Content Management Systeem (CMS) van de website.

Het CMS kan worden benaderd via de URL:

<https://www.digid.nl/typo3/index.php>

N.B. In verband met een IP-restrictie kan deze URL alleen worden benaderd vanuit kantoor (Den Haag, Apeldoorn) of via een VPN-verbinding (middels de laptop).

De werkinstructie voor het plaatsen van een bericht is als apart document bijgevoegd.

DigiD applicatie

Op de schermen in de DigiD applicatie (aanvragen, activeren, authenticeren, Mijn gegevens) kunnen ook meldingen worden geplaatst. Alleen Atos Origin is hiertoe in staat. Neem contact op met Atos Origin voor het plaatsen van meldingen op een of meerdere DigiD applicatie schermen.

3.3.7 Escaleren (optioneel)

Tijdens de uitvoering van incident- en calamiteitenbeheer kan er sprake zijn van meerdere (eventueel gelijktijdige) vormen van escalatie. De escalatievormen worden in de onderstaande paragrafen behandeld.

3.3.7.1 Horizontale escalatie

Deze vorm van escalatie betreft:

- inschakelen van specialisme (materiedeskundigheid)
- als incident niet snel genoeg kan worden opgelost in de huidige lijn

Domein	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Support	Medewerker Servicecentrum	Logius oplosgroep(en) van Servicecentrum	Leverancier	
Product	Functioneel beheerder	Logius oplosgroep(en) van Functioneel beheer	Servicedesk (Leverancier)	Specialist (Leverancier)

Figuur 7: horizontale escalatie

N.B. De verantwoordelijkheid voor het afhandelen van het incident of de calamiteit wordt bij horizontale escalatie niet verplaatst naar andere actoren.

3.3.7.2 Verticale escalatie

Verticale escalatie wordt ingezet:

- voor verkrijgen (extra) autoriteit of resources
- voor verkrijgen (extra) mandaat
- indien overeenkomst met leverancier niet lijkt te worden nagekomen

Domein	Support	Support	Product	Product
--------	---------	---------	---------	---------

	(Logius)	(Cendris)	(Logius)	(Leverancier)
Niveau 4	Directeur	Directeur Cendris	Directeur	Directeur
Niveau 3	Hoofd Dienstverlening	Contractmanager Cendris	Hoofd management	Contractmanagement
Niveau 2	Tactisch coördinator	Servicemanager Cendris	Servicemanager	Servicemanager
Niveau 1	Medewerker Servicecentrum	Teamleider Cendris	Functioneel beheerder	Servicedesk medewerker

Figuur 8: verticale escalatie

N.B. De verantwoordelijkheid voor het afhandelen van het incident of de calamiteit wordt bij verticale escalatie niet verplaatst naar andere actoren.

N.B. Bij deze vorm van escalatie hoeft er geen sprake te zijn van een calamiteit!

3.3.7.3

Escalatie van incident naar calamiteit

Tijdens de uitvoering van incidentbeheer kan het voorkomen dat een incident een calamiteit wordt. Redenen hiervoor kunnen zijn:

- de oplostijd van een P1 incident wordt overschreden
- de oplostijd van een P1 incident dreigt te worden overschreden
- een gebeurtenis is bij nader inzien ernstiger dan eerder vastgesteld en brengt de algehele dienstverlening van Logius in gevaar
- een gebeurtenis is bij nader inzien ernstiger dan eerder vastgesteld en brengt de goede naam/imago van Logius in gevaar of leidt tot politieke schade (bv. mediabericht, fraude met Logius product, journalist meldt zich).

Het is de verantwoordelijkheid van de standby manager om vast te stellen of er sprake is van een escalatie naar een calamiteit.

Indien er sprake is van een calamiteit wijzigen de actoren. Zie paragraaf 3.2.

3.3.8

Formeren calamiteitenteam (bij calamiteit)

Als er sprake is van een calamiteit (door standby manager vast te stellen), formeert de standby manager een calamiteitenteam. De standby manager is de voorzitter van het calamiteitenteam.

De calamiteitencoördinator informeert de contactperso(n)en van de beleidsopdrachtgever(s) indien er sprake is van een calamiteit. Indien nodig leveren deze capaciteit (teamlid) om een bijdrage te leveren aan het zo snel mogelijk oplossen van de calamiteit.

De teamleden van de beleidsopdrachtgevers informeren als lid van het calamiteitenteam, de beleidsopdrachtgevers intern.

3.3.9 *Formeren herstelteam (bij calamiteit)*

De calamiteitencoördinator kan besluiten om een herstelteam te formeren. Hiervoor wijst hij/zij een voorzitter aan. Het herstelteam houdt zich bezig met het herstel van de schade die door de calamiteit is ontstaan.

3.3.10 *Evalueren/verbeteren (bij P1 incident of calamiteit)*

Na afronding van de herstelwerkzaamheden van een P1 incident of calamiteit wordt er altijd een evaluatie uitgevoerd.

Binnen 5 werkdagen na oplossing van het incident moet er een evaluatie gemaakt worden en deze moet op de g-schijf worden geplaatst. De evaluatie is afgestemd met betrokkenen bij de P1. Als het incident langer dan een week openstaat, maak dan alvast een voorlopige evaluatie. Bij een incident mag de incidentmanager zelf bepalen of hij een evaluatieoverleg organiseert met interne medewerkers die direct betrokken waren bij de P1 of niet. Bij calamiteiten wordt altijd een overleg met direct betrokkenen gepland.

Bij calamiteiten is de calamiteitencoördinator verantwoordelijk voor de evaluatie. Hij of zij wordt hierbij ondersteund door de incident manager. De registratie in Clientèle en de monitoring van de verbeterpunten kan hij delegeren aan de incidentmanager.

De evaluatie gaat in op:

- de gekozen oplossing
- werking van incident- en/of calamiteitenbeheer

Vul de evaluatie in op het incidentregistratieformulier, sla het formulier op op de g-schijf, De Incidentmanager stuurt de evaluatie altijd rond naar de direct betrokken medewerkers/MT-lid.

De incidentmanager belegt actiepunten uit de evaluatie bij zijn collega's, via Clientèle.

Indien nodig wordt het incidentbeheerproces of calamiteitenbeheerproces aangepast. De incidentmanager zorgt ervoor dat deze verbeteracties in de lijn worden belegd via reguliere processen.

De incidentmanager neemt de evaluatie op in Clientèle, inclusief de verbeterpunten. De incidentmanager houdt de voortgang van de verbeterpunten bij.

Het evaluatierapport kan ook weer worden gebruikt als input voor communicatie naar klanten in de nazorg.

3.3.11 *Afleggen bestuurlijke verantwoording (bij calamiteit)*

Bij een calamiteit wordt in overleg met de Programmaraad van Logius en de voorzitter van het calamiteitenteam bepaald op welke wijze en aan wie verantwoording dient afgelegd te worden.

4 Organisatie

4.1 Relevante Logius partijen

De relevante Logius partijen voor incident- en calamiteitenbeheer zijn:

Supportdomein:

afdeling	rol
Incidentbeheer	
Dienstverlening	Medewerker Servicecentrum
	Incidentmanager Servicecentrum
Calamiteitbeheer	
MT	Calamiteiten coördinator (MT-lid)
Dienstverlening	Incidentmanager Servicecentrum
Marketing-communicatie	Woordvoerder

Productdomein:

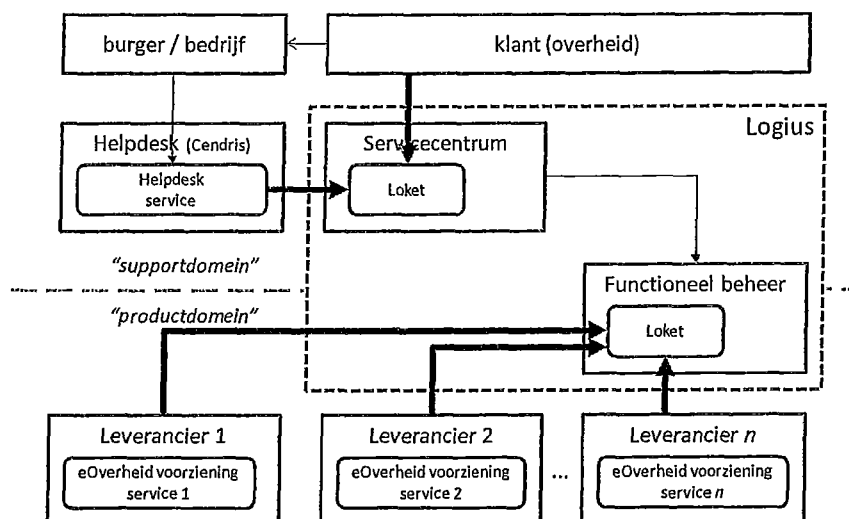
afdeling	rol
Incidentbeheer	
Tactisch beheer	Medewerkers Tactisch beheer
	Incidentmanager Tactisch beheer
Calamiteitbeheer	
MT	Calamiteiten coördinator (MT-lid)
Tactisch beheer	Incidentmanager Servicemanagement
Communicatie	Woordvoerder

4.2 Bereikbaarheid

4.2.1 Algemeen

Voor het supportdomein en het productdomein is elk één loket ingericht: klanten melden zich aan het loket van het Servicecentrum, leveranciers melden zich aan het loket van Tactisch beheer.

Hierbij wordt voor één leverancier een uitzondering gemaakt, namelijk voor Cendris. De contacten tussen Cendris en het Servicecentrum verlopen via het Servicecentrum. Zie onderstaande figuur.



Servicecentrum is verantwoordelijk voor het bewaken van de meldingen in het supportdomein (van klanten en van Cendris). Tactisch beheer is verantwoordelijk voor het bewaken van de meldingen in het productdomein (van/naar leveranciers).

4.2.2

Tijdens kantooruren

Klanten kunnen het Servicecentrum tijdens kantoortijden als volgt bereiken:

Bereikbaarheid	Telefoon: 0900-5554555 E-mail: servicecentrum@logius.nl
Openstelling	Werkdagen van 08:00 – 17:00 uur

Leveranciers kunnen Tactisch beheer tijdens kantoortijden als volgt bereiken:

Bereikbaarheid	[REDACTED]
Openstelling	Werkdagen van 08:00 – 17:00 uur

4.2.3

Buiten kantooruren (standby dienst)

Om storingen in de dienstverlening ook buiten kantooruren af te handelen is de standby dienst ingesteld. Zie paragraaf 4.3.

De standby dienst geldt buiten kantooruren, dus op maandag t/m vrijdag van 17:00 – 08:00 uur, in weekenden en op nationaal erkende feestdagen.

4.3 Standby dienst

4.3.1 Standby team

Elke week wordt er een standby team geformeerd. Dit team bestaat uit:

teamlid	rol
Medewerker Tactisch beheer	Incidentmanager productdomen
Medewerker Tactisch beheer	Backup van Incidentmanager
Medewerker F&G	Backup voor Incidentmanager (vrijwillig ³)
Medewerker Servicecentrum	Incidentmanager supportdomein
MT-lid	Calamiteiten coördinator (tevens voorzitter calamiteitenteam)

Het team bestaat elke week uit andere medewerkers.

De teamleden van het standby team zijn op hun standby mobiele toestellen voor elkaar bereikbaar. Zie hiervoor de Quick Reference Incidentbeheer en Quick Reference Calamiteitenbeheer.

N.B. De incidentmanager van het Servicecentrum staat uitsluitend standby op werkdagen van 17:00 – 22:00 uur, aangezien het servicevenster van de Helpdesk op werkdagen eindigt op 22:00 uur en de Helpdesk in het weekend en feestdagen niet geopend is.

4.3.2 Bereikbaarheid standby team

Buiten kantooruren kan het Servicecentrum door klanten worden benaderd in geval van een ernstige technische storing van Logius producten.

Bereikbaarheid	Telefoon: 0900-5554555 E-mail: servicecentrum@logius.nl
Openstelling	Alle dagen van het jaar, 24 uur per dag

Een oproep naar 0900-5554555 wordt buiten kantooruren doorgeschakeld naar de incidentmanager (standby Servicebeheerder).

Buiten kantooruren kan Tactisch beheer door leveranciers worden benaderd in geval van een ernstige technische storing van Logius producten.

³ Op dit moment levert een medewerker F&G alleen op vrijwillige basis een bijdrage aan de standby dienst. Het ligt in de bedoeling dat medewerkers F&G ook volledig standby diensten gaan draaien. De rechtspositionele gevolgen hiervan worden onderzocht.

Bereikbaarheid	[REDACTED]
Openstelling	Alle dagen van het jaar, 24 uur per dag

4.3.3

Afspraken rondom standby dienst

Elke standby Tactisch beheer medewerker zorgt er voor dat in de week dat hij/zij standby dienst heeft:

- hij/zij de standby mobiele telefoon altijd bij zich heeft en dat deze telefoon aan staat en voldoende opgeladen is
- hij/zij een telefonische oproep op de standby mobiele telefoon binnen 30 seconden aanneemt en de melder te woord staat
- hij/zij eventuele ontvangen voicemail binnen 10 minuten na ontvangst beantwoordt (terugbelt).
- binnen 30 minuten na de telefonische oproep op de standby mobiele telefoon beschikbaar is voor het afhandelen van incidenten/calamiteiten
- hij/zij beschikt over zijn/haar laptop
- de laptop naar behoren werkt en verbinding heeft met alle Logius voorzieningen t.b.v. standby dienst (middels vaste/draadloze netwerkverbinding)
- hij/zij het standby handboek, inclusief gerelateerde documenten, bij zich heeft
- hij/zij incident registratieformulieren (P1) bij zich heeft
- hij/zij geen verdovende middelen of alcohol nuttigt.

4.3.4

Standby rooster

Voor elke week van het jaar wordt er vastgesteld welke medewerkers zich in het standby team bevinden. De verantwoordelijkheid voor het opstellen van het rooster is als volgt:

medewerker	verantwoordelijk voor inroosteren van
Secretariaat Logius	Calamiteiten coördinatoren (standby managers)
Teamleider Tactisch beheer	Incidentmanagers Tactisch beheer
Tactisch coördinator Servicecentrum	Incidentmanagers Servicecentrum

Het inroosteren van medewerkers gebeurt door het plaatsen van items in de agenda's (Exchange) van de betreffende medewerkers.

Als een toegewezen teamlid op een of meerdere dagen niet kan (bv. tijdens vakantie of vrije dag), zorgt hij/zij zelf voor vervanging en draagt de mobiele telefoon over aan een collega.

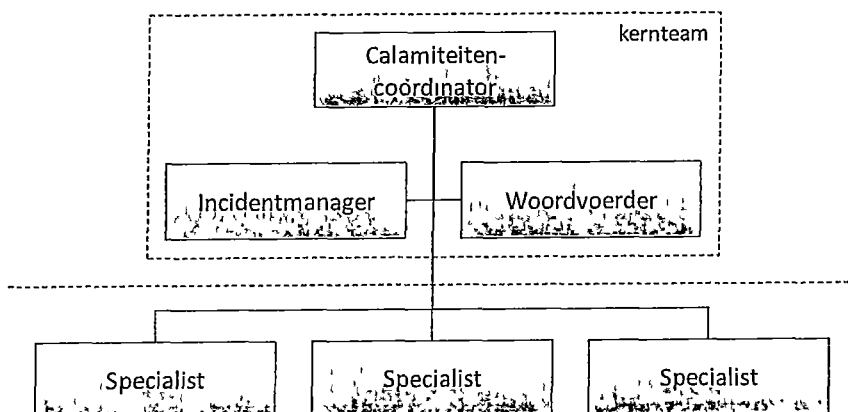
De incidentmanager Tactisch beheer, incidentmanager Servicecentrum en calamiteiten coördinator (standby-manager) dragen allen een standby mobiele telefoon bij zich. Zie paragraaf 7.1.

4.4

Calamiteitenteam

Wanneer zich een calamiteit voordoet die Logius als organisatie of de politiek raakt, dan zal het Calamiteitenteam de regie voeren over de stappen die extern en intern gezet moeten worden om de schade zo

beperkt mogelijk te houden en het probleem zo snel mogelijk op te lossen.



Figuur 9: organisatie calamiteitenteam

Het Calamiteitenteam is een tijdelijke organisatie en verzorgt de centrale coördinatie van alles wat met de calamiteit te maken heeft. De behoefte aan coördinatie zal per calamiteit verschillen. Bij een calamiteit komt echter minimaal het zogenaamde kernteam bijeen. Het kernteam bestaat uit:

1. calamiteitencoördinator (voorzitter)
2. woordvoerder Logius
3. incidentmanager

De calamiteitencoördinator is de dienstdoende manager in het standby team. De incidentmanager is de dienstdoende servicebeheerder en dienstdoende coördinator van het Servicecentrum.

Afhankelijk van de aard en omvang van de gebeurtenis wordt het kernteam van het Calamiteitenteam, op aanwijzing van de voorzitter, uitgebreid met vertegenwoordigers afdelingen van Logius en de beleidsopdrachtgever(s).

De leden van het Calamiteitenteam adviseren de voorzitter over het te voeren beleid, de te ondernemen acties, communicatie en over de te stellen prioriteiten. De leden van het Calamiteitenteam geven gevraagd en ongevraagd (onderling afgestemde) adviezen aan de voorzitter en collega Calamiteitenteamleden. Daarnaast zijn de leden van het Calamiteitenteam individueel verantwoordelijk voor de juiste aansturing en coördinatie van de activiteiten die uitgevoerd moeten worden binnen hun eigen verantwoordelijkheidsgebied.

Het Calamiteitenteam beschikt over alle bestuurlijke bevoegdheden die nodig zijn om de calamiteit effectief te bestrijden.

4.5

Rollen, taken en verantwoordelijkheden

Bij de afhandeling van incidenten en calamiteiten worden verschillende rollen onderkend, elk met hun eigen verantwoordelijkheid. Deze worden in onderstaande paragrafen beschreven.

4.5.1 *Directeur Logius*

De directeur is eindverantwoordelijk voor het continuïteitsniveau van de dienstverlening door Logius aan klanten.

4.5.2 *Standby manager*

De incidentmanager schakelt manager van dienst bij een P1 in als het incident dreigt te escaleren naar een calamiteit door het overschrijden van de met de klanten afgesproken oplostijd of bij een dreigende schade van het imago van de politiek of Logius of economische schade. Bij dreigende schade is communicatie met en naar de pers cruciaal.

Tijdens de P1 heeft de incidentmanager de regie over de oplossing en communicatie. De standby-manager treedt op als eerste contactpersoon van de incidentmanager. In overleg met hem bepaalt de incidentmanager op welke wijze escalatie naar leveranciers nodig is en welke besluiten nodig zijn om tot een oplossing van het incident te komen. Tot slot helpt hij waar nodig de incidentmanager in de communicatie.

Het incident kan escaleren tot een calamiteit. De incidentmanager overlegt met de standby-manager stelt of er sprake is van een calamiteit.

Als sprake is van een calamiteit dan neemt hij de regie over van de incidentmanager. Dit betekent dat de standby-manager vanaf dat moment verantwoordelijk is voor de oplossing van de calamiteit en de communicatie. De incidentmanager kan inhoudelijk (o.a. probleem, oorzaak, duur oplossing) hier een bijdrage aan leveren. De standby-manager schakelt meteen de woordvoerder van Logius in om de pers-communicatie voor te bereiden. De standby-manager is ook degene die direct de directeur Logius en de opdrachtgevers informeert over de calamiteit. Verder heeft de standby-manager de taak om alles wat nodig is in gang te zetten om het incident zo snel mogelijk op te lossen en indien nodig op managementniveau naar de leveranciers te escaleren.

Verantwoordelijkheden standby manager (volgens rooster):

- paraat staan voor de incidentmanager t.b.v. besluitvorming (calamiteit ja/nee, extern communiceren ja/nee)
- beoordeelt in overleg met de incidentmanager de calamiteitenmelding en stelt indien nodig het calamiteitenplan in werking. Onder het beoordelen van de melding wordt onder meer verstaan dat er een vertaalslag wordt gemaakt van de opgetreden verstoring(en) in de systemen/applicaties naar de bedrijfsprocessen en (in- en externe) dienstverlening die geraakt wordt
- het nemen van een besluit of er sprake is van een calamiteit
- zit het Calamiteitenteam voor
- inlichten Logius-Directie
- neemt de besluiten die hij nodig acht om de calamiteit op de juiste wijze te bestrijden en laat zich daarbij bijstaan door een door hem samengestelde crisisorganisatie
- draagt er zorg voor dat personen en instanties van buiten Logius op de juiste manier worden geïnformeerd (externe informatievoorziening)
- draagt er zorg voor dat personen binnen Logius op de juiste manier worden geïnformeerd (interne informatievoorziening)
- neemt het besluit tot herstel (beëindiging van de calamiteit)
- draagt na afloop zorg voor een evaluatie van de calamiteit

- verantwoordt de tijdens de calamiteit genomen besluiten naar de beleidsopdrachtgevers
- contact opnemen met woordvoerder ter afstemming perscommunicatie
- verticale escalaties richting leveranciers t.b.v. het in gang zetten van activiteiten die hij/zij nodig acht ter oplossing van een incident/calamiteit.

4.5.3 Incidentmanager

Voor zowel het supportdomein als het productdomein is er een incidentmanager (volgens rooster). Voor het supportdomein is dit de standby operationeel coördinator van het Servicecentrum. Voor het productdomein is dit de standby servicebeheerder.

De Incidentmanager is bevoegd, heeft het mandaat, om collega's te benaderen en uit hun normale werk te halen.

4.5.3.1 Taken

De taken van de incidentmanager zijn:

- coördinatie activiteiten voor verhelpen van verstoring
- interne en externe communicatie
- evaluatie na verhelpen incident
- rapportage (achteraf) aan hoofd Dienstverlening (supportdomein) of hoofd Tactisch beheer (productdomein)

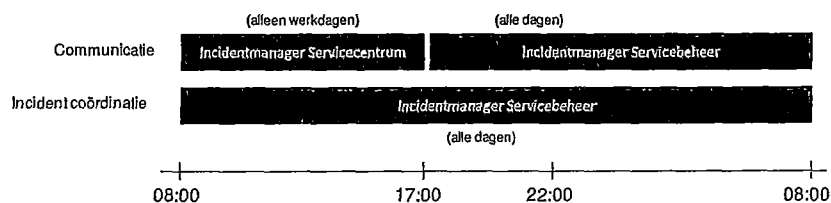
4.5.3.2 Verantwoordelijkheden

De incidentmanager is verantwoordelijk voor:

- De regievoering over het afhandelen van het incident en
- de communicatie over de afhandeling van het incident aan relevante partijen

In onderstaande schema is in de tijd de verantwoordelijkheid weergegeven van het coördineren van de afhandeling van het incident en de communicatie naar betrokkenen hierover.

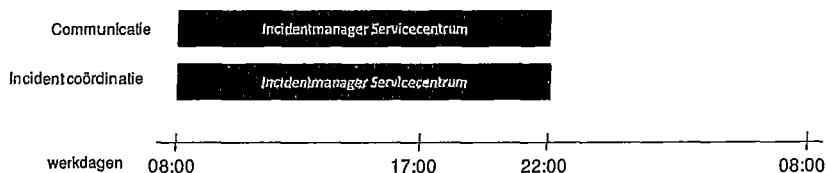
Productdomein



De Incidentmanager van Tactisch beheer is verantwoordelijk voor de afhandeling en communicatie van incidenten die zich gedurende alle dagen (24 x 7) in het productdomein voordoen.

N.B. De gebruikte communicatieteksten (website, e-mail, sms-bericht) worden hierbij zoveel mogelijk gestandaardiseerd en overeengekomen met Marketing-Communicatie en worden verstuurd namens de incidentmanager van Tactisch beheer.

Supportdomein



De Incidentmanager van het Servicecentrum is verantwoordelijk voor de afhandeling van incidenten die zich gedurende werkdagen (08:00 – 22:00 uur) in het supportdomein (Helpdesk, Servicecentrum) voordoen. Dit betekent dat hij/zij verantwoordelijk is voor het herstel van de dienstverlening door het Servicecentrum en de Helpdesk. Ook de communicatie naar klanten/gebruikers over de verstoring valt ook onder de verantwoordelijkheid van de incidentmanager van het Servicecentrum.

4.5.3.3 Bevoegdheden

De Incidentmanager heeft de bevoegdheid tot:

- inschakelen van specialisten (binnen Logius en/of externe partijen)
- contact opnemen met het standby manager

4.5.3.4 Eigenschappen

De eigenschappen van de incidentmanager zijn:

- natuurlijk overwicht
- natuurlijke neiging tot communicatie aan betrokkenen
- weten door te dringen tot de essentie
- goed ontwikkeld klantbesef
- gevoel voor communicatie
- hoofdzaken van bijzaken kunnen onderscheiden (niet verliezen in details)
- ervaring in IT Tactisch beheer (ITIL) omgeving

4.5.4 Woordvoerder Logius

De woordvoerder van Logius is lid van het kernteam van het Calamiteitenteam. De woordvoerder is in samenspraak met de voorzitter van het Calamiteitenteam verantwoordelijk voor een zorgvuldige, duidelijke, eerlijke en tijdige communicatie aan zowel interne als externe partijen (waaronder media en externe klanten).

De woordvoerder Logius:

- adviseert de voorzitter van het Calamiteitenteam gevraagd en ongevraagd over communicatieve onderwerpen
- initieert en coördineert de interne en de externe communicatie
- stuurt het communicatieteam aan (bestaande uit leden van de eenheid Communicatie)
- treedt op als woordvoerder namens het Logius.

5 Communicatie

In dit hoofdstuk worden de taken en verantwoordelijkheden ten aanzien van de uitvoering van communicatie beschreven.

5.1 Algemene uitgangspunten bij communicatie

Zorgvuldige communicatie

Bij de interne en externe communicatie staat zorgvuldige communicatie voorop. Hoewel Logius eerlijk en open wil communiceren, is het niet raadzaam om ten alle tijden alle informatie openbaar te maken. In de volgende paragrafen wordt ingegaan op de communicatie naar de verschillende doelgroepen.

Eerlijke en tijdige communicatie

Om de reputatie en het imago van Logius te bewaken, is het noodzakelijk eerlijk en tijdig te communiceren. Hierdoor kan voorkomen worden dat er naast materiële schade, tevens immateriële schade wordt opgelopen. Bij een slechte begeleiding van de calamiteitenprocedure kan de reputatie en het imago van een organisatie veel schade oplopen. Dit mag bij Logius niet gebeuren.

Interne communicatie vóór externe communicatie

De eigen medewerkers en managers moeten als eerste worden geïnformeerd. Er zijn echter ook calamiteiten denkbaar, waarbij andere stakeholders eerder moeten worden geïnformeerd. Bij iedere calamiteit moet dus goed worden overwogen wie als eerste moet worden geïnformeerd. De Logius woordvoerder adviseert de calamiteitencoördinator daarover.

5.2 Woordvoerder in calamiteitenteam

De Logius woordvoerder is als communicatieadviseur lid van het calamiteitenteam. De woordvoerder wordt door de calamiteitencoördinator geïnformeerd zodra er sprake is van een calamiteit. Hij/zij is, in samenspraak met de calamiteitencoördinator, verantwoordelijk voor een zorgvuldige, duidelijke, eerlijke en tijdige communicatie aan zowel interne als externe stakeholders.

De bevoegdheden en verantwoordelijkheden van de woordvoerder zijn als volgt:

1. Gevraagd en ongevraagd adviseren van de calamiteitencoördinator. De leden van het calamiteitenteam adviseren de voorzitter over het te voeren beleid, de te ondernemen acties en over de te stellen prioriteiten. Zij geven gevraagd en ongevraagd (onderling afgestemde) adviezen aan de voorzitter en collega teamleden. De adviezen van de woordvoerder richten zich op de communicatieve onderwerpen.

2. Initiëren en coördineren van de interne en externe communicatie. De leden van het calamiteitenteam zijn individueel verantwoordelijk voor de juiste aansturing en coördinatie van de activiteiten die uitgevoerd moeten worden binnen hun eigen verantwoordelijkheidsgebied. De woordvoerder is verantwoordelijk voor een eenduidige interne en externe communicatie over de calamiteit.

3. Aansturen van het Communicatieteam

De woordvoerder stelt een communicatieteam samen van leden van het team Communicatie. De woordvoerder stuurt dit team aan en vormt de schakel tussen het communicatieteam en het calamiteitenteam. Tijdens de calamiteit wordt de woordvoerder rechtstreeks over de stand van zaken en eventuele ontwikkelingen geïnformeerd door het calamiteitenteam.

4. Optreden als woordvoerder namens Logius

De woordvoerder wordt als lid van het calamiteitenteam door de calamiteitcoördinator geïnformeerd zodra er sprake is van een calamiteit. De woordvoerder dient tijdig op de hoogte te worden gesteld, zodat hij/zij zich kan voorbereiden op eventuele vragen. De woordvoerder onderhoudt contacten met de media en geeft interviews, of is aanwezig bij door anderen (bijvoorbeeld de voorzitter van het calamiteiten) te geven interviews.

5.3 Interne communicatie

Met het oog op een adequate en gerichte interne communicatie richt de woordvoerder zich op de interne communicatie.

Relevante interne medewerkers zijn:

- MT+ leden
- Productmarketeers Dienstverlening
- Accountmanagers Dienstverlening
- Woordvoerder
- Servicemanagers
- Medewerkers Servicecentrum
- Tactisch beheerders

Tevens is de woordvoerder verantwoordelijk voor de interne contacten en het peilen van de reacties onder de medewerkers.

De woordvoerder heeft, na afstemming met de voorzitter van het calamiteitenteam, tot taak het management te informeren over de calamiteit. De woordvoerder stuurt daarvoor een bericht naar het Logius management. Dit kan via een e-mail of telefonisch. Hierbij kan gebruik worden gemaakt van de e-mail/sms-voorziening (MailPlus). De incidentmanager heeft toegang tot deze voorziening.

De woordvoerder levert de tekst voor het bericht aan bij de incidentmanager zodat hij/zij het kan verspreiden onder de medewerkers. Informatie aan Logius medewerkers kan worden gegeven via het Intranet, per e-mail of sms.

5.4 Media

De taken van de woordvoerder zijn het onderhouden van de contacten met de media en het geven of begeleiden van interviews. Wanneer bijvoorbeeld de voorzitter van het calamiteitenteam wordt geïnterviewd, is de woordvoerder hierbij aanwezig.

Daarnaast gelden de volgende afspraken bij contacten met de media:

- de media worden altijd doorverwezen naar de woordvoerder.
- wanneer blijkt dat medewerkers de media zelf te woord hebben gestaan, zonder dat hierover afspraken zijn gemaakt met de woordvoerder, dan wordt gecontroleerd of de verstrekte informatie

correct is. Wanneer de informatie niet klopt, dan neemt de woordvoerder contact op met de betrokken media. Tevens wordt de betrokken medewerker gewezen op het overtreden van de interne procedures.

- bij afwezigheid van de woordvoerder neemt, afhankelijk van de aard van de calamiteit, de voorzitter van het calamiteitenteam of de plaatsvervangend woordvoerder uit het communicatieteam deze taak over.

De woordvoerder zorgt voor het opstellen van persberichten. Nadat een persbericht is goedgekeurd door de voorzitter van het calamiteitenteam, wordt het bericht per e-mail verstuurd naar (een selectie van) de media afhankelijk van de aard van de calamiteit. Wanneer e-mailverkeer niet mogelijk is, dan wordt gebruik gemaakt van de fax of de telefoon om contact met de relevante media te onderhouden.

Vragen van de media over de calamiteit worden verzameld. Na afstemming met de voorzitter van het calamiteitenteam, beantwoordt de woordvoerder in een eenduidige, heldere boodschap de vragen van de media. De overige leden van het calamiteitenteam worden door de woordvoerder op de hoogte gehouden van verdere ontwikkelingen. De woordvoerder heeft ook als taak om te monitoren wat er in de media over de calamiteit wordt bericht.

5.4.1 *Geen storing, maar wel in de media*

Als een mediabericht/artikel leidt tot imagoschade voor Logius of een bepaald product, zal Communicatie/Woordvoering dit afstemmen met de Calamiteitencoördinator. Deze bepaalt of er een calamiteit van wordt gemaakt en is verantwoordelijk voor de afhandeling, samen met communicatie.

De workflow wordt:

- Meld het 'media-issue' altijd bij de woordvoerder.
- De woordvoerder bepaalt of zij het zelf kan oplossen of dat het incidentenproces gevolgd wordt.
- Zo ja, dan belt de woordvoerder met de incidentmanager of stuurt mail aan servicecentrum.
- De incidentmanager schakelt meteen de calamiteitenmanager/standby manager in, en zorgt voor registratie.
- Daarna is de calamiteitenmanager verantwoordelijk voor oplossen van het media-incident, samen met woordvoerder en incidentmanager.

5.5 Klanten

Bij communicatie richting klanten is tactisch beheer, in samenspraak met de woordvoerder, verantwoordelijk voor een eenduidige berichtgeving over de calamiteit. De woordvoerder stelt hiervoor een bericht op in overleg met de incidentmanager. Wanneer dit bericht is goedgekeurd door de voorzitter van het calamiteitenteam, kan de incidentmanager het bericht verspreiden.

De contactpersonen bij klanten worden door het Servicecentrum bepaald en beheerd in Clientele en MailPlus.

5.6 Politiek en opdrachtgevers

De politiek en opdrachtgevers moeten, als belangrijke stakeholders van Logius, ook worden geïnformeerd wanneer zich een calamiteit voordoet. De communicatie met deze groepen wordt gevoerd door de woordvoerder.

In de Quick Reference Calamiteitenbeheer staan de contactgegevens van deze groepen.

5.7 Communicatiemiddelen

Voor communicatie aan betrokkenen via e-mail en/of sms wordt gebruik gemaakt van MailPlus (zie paragraaf 7.5). In MailPlus worden op basis van klantgegevens in Clientele communicatiedoelgroepen aangemaakt. Deze groepen worden samengesteld op basis van de positie van de contactpersoon (Logius of extern), Logius product waarover de contactpersoon geïnformeerd wenst te worden en de wijze (e-mail en/of sms) waarop de contactpersoon een bericht wil ontvangen.

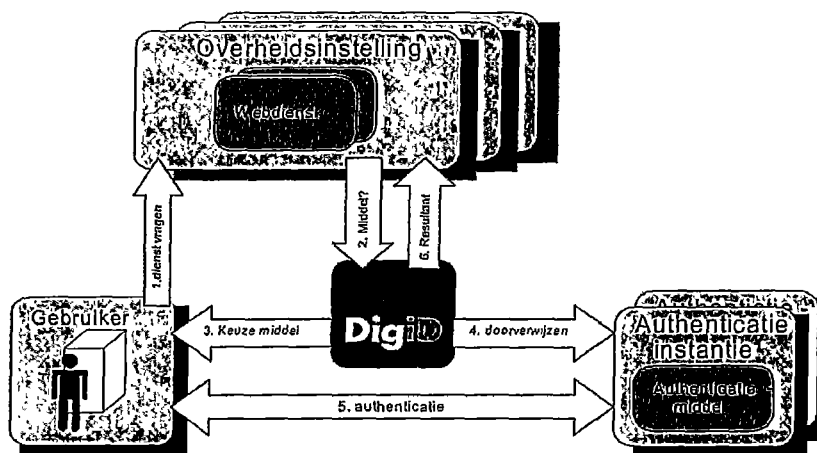
N.B. Vooralsnog is een beperkt aantal contactpersonen bij klanten opgenomen in MailPlus.

6 Producten

6.1 DigiD voor burgers

6.1.1 Globale werking

De DigiD-dienst bestaat uit het authenticeren van eindgebruikers (burgers) voor overheidswebdiensten (klanten van DigiD). De globale werking van DigiD wordt in onderstaande figuur weergegeven.



Figuur 10: globale werking van DigiD

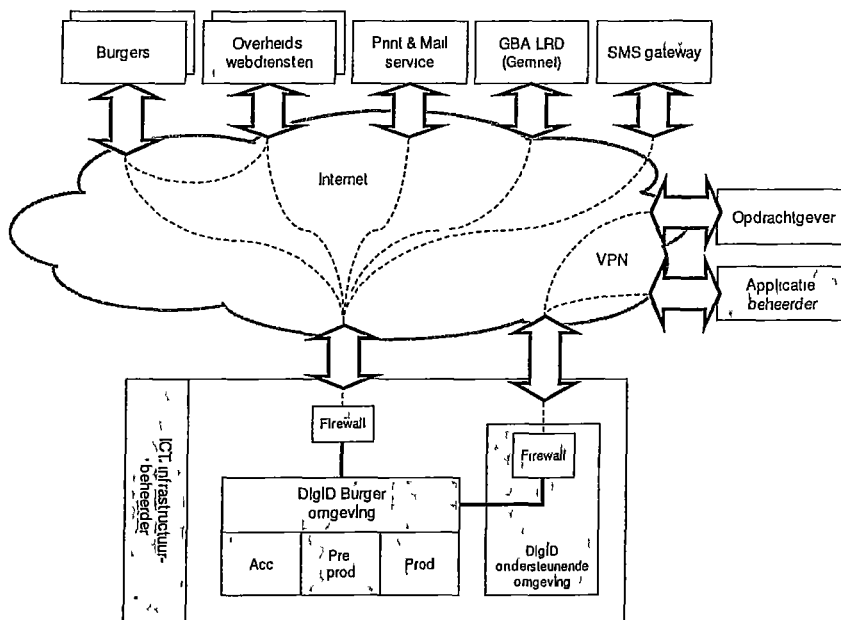
DigiD voor Burgers is bedoeld voor het authenticeren van burgers door overheidswebdiensten. De burger benadert hierbij via Internet een webdienst van een overheidsinstelling die op DigiD is aangesloten. Voor het vaststellen van de identiteit van de burger wordt de burger doorverwezen naar de authenticatievoorziening binnen DigiD. Hier vult de burger zijn/haar gebruikersnaam en wachtwoord (en eventueel sms transactiecode) in. DigiD controleert deze gegevens en - indien correct - sluisst de gebruiker terug naar de webdienst. DigiD communiceert aan de webdienst het burgerservicenummer (BSN) en het betrouwbaarheidsniveau waarmee de burger is geauthenticeerd. De webdienst biedt de burger tenslotte toegang tot (een selectie van) haar diensten.

Voordat een burger gebruik kan maken van DigiD, dient deze zich eerst aan te melden. Na invoer van de persoonsgegevens worden deze door DigiD gecontroleerd bij de Gemeentelijke Basis Administratie Persoonsgegevens (GBA). Indien de gegevens juist zijn, stuurt DigiD via een externe Print & Mail service een brief naar de burger. In deze brief staat een activeringscode. Om het DigiD account te activeren voert de burger deze code in op de DigiD website. De burger kan ervoor kiezen om zich door DigiD op een hoger betrouwbaarheidsniveau te laten authenticeren door middel van het invoeren van een sms transactiecode op de DigiD website. Dit aanvullende wachtwoord stuurt DigiD middels een SMS-bericht dat wordt verstuurd via een externe SMS gateway.

6.1.2

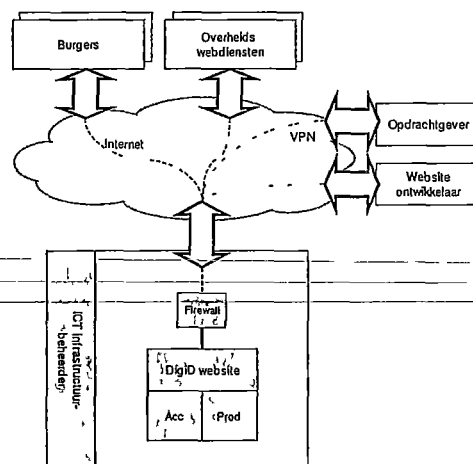
Systeemlandschap

De ICT Infrastructuur voor DigiD voor burgers bevindt zich bij Atos Origin. Het is een zg. twinning concept, waarbij 2 locaties tegelijkertijd actief zijn. Indien een van de locaties deels of geheel uitvalt, dan kan de andere locatie de activiteiten overnemen (grotendeels automatisch).



De "uitwijk" wordt geheel binnen de verantwoordelijkheid van Atos Origin uitgevoerd. Alleen als Atos bepaalde (grote) risico's ziet aan de te ondernemen activiteiten, dan zal contact met Logius worden opgenomen.

De ICT infrastructuur voor de DigiD website bevindt zich ook bij Atos Origin.



6.1.3

Dienstverlening

De dienstverlening bestaat uit de elektronische dienstverlening (de DigiD applicatie die via Internet wordt ontsloten naar de eindgebruikers) en de

gebruikersondersteuning aan burgers (door de Helpdesk) en klanten (door het Servicecentrum).

Zodra er sprake is van een (dreigende) verstoring van de hieronder beschreven dienstverlening, is er sprake van een incident.

Eigenschappen van de elektronische dienstverlening (voor de klant) zijn:

Performance indicatoren voor openstellingswindow		
Soort afspraak	Norm	Minimaal te realiseren
Beschikbaarheid van de dienst voor burgers (productieomgeving)	De productieomgeving van DigiD is 7*24 uur, alle dagen van het jaar, beschikbaar voor: het verwerken van aanmeldingen door burgers; activeren van aangevraagde accounts door middel van een activeringscode; afhandelen van authenticatieverzoeken.	99,5 % beschikbaar.
Beschikbaarheid van de DigiD website: openstelling van de dienst (productie)	De productieomgeving van DigiD website is 7*24 uur, alle dagen van het jaar beschikbaar	99,5% beschikbaar.
Beschikbaarheid van de dienst voor klanten (productieomgeving)	De productieomgeving van DigiD is 7x24 uur, alle dagen van het jaar, beschikbaar voor een operationele Klant.	99,5 % beschikbaar.
Beschikbaarheid van de dienst voor klanten (pré-productieomgeving)	De pré-productieomgeving van DigiD is ma.-vr. van 7:00 – 18:00 uur beschikbaar voor testsituaties voor potentiële Klanten en leveranciers. NB. In deze pré-productieomgeving is een pseudo koppeling met de LRD omgeving voorhanden (i.v.m. privacy aspecten).	99,0 % beschikbaar.

Prestatie-indicatoren voor onderhoudswindow		
	Norm	Norm
	Productieomgeving	Pré-productieomgeving
Structureel gepland onderhoud m.b.t. diensten	Maximaal 1 keer per maand, gedurende maximaal 6 uur.	Buiten het openstellingswindow.
Onderhoud m.b.t. de technische installaties	Maximaal 4 keer per jaar, gedurende maximaal 4 uur.	Maximaal 4 keer per jaar, gedurende maximaal 4 uur.

Performance indicator voor capaciteit en performance DigiD systemen		
Soort afspraak	Norm	Minimaal te realiseren

Verwerkingstijd van DigiD bij authenticatie	Verwerking authenticatie gemiddeld afgehandeld binnen 0,15 sec.	100 %.
Verwerkingstijd bij maximale concurrent sessies	Daar waar 900 concurrent sessies worden gestart, is de verwerkingstijd van minimaal 95% van deze 900 sessies korter dan 30 seconden.	100 %.

Kentallen met betrekking tot capaciteit en performance DigiD systemen		
Soort afspraak	Norm	Minimaal te realiseren
Capaciteit authenticaties	Het aantal authenticaties wordt gegarandeerd voor 300.000 authenticaties per uur (gedurende 24 uur per dag).	Geen.

Eigenschappen van de gebruikersondersteuning (voor de klant) zijn:

Performance indicatoren voor servicewindow		
Beschikbaarheid	Norm	Norm
	Productie-omgeving	Pré-productieomgeving
1 ^e -lijns ondersteuning voor het melden van incidenten door burgers	Werkdagen van 8.00 uur tot 22.00 uur.	
1 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door burgers	Werkdagen van 8.00 uur tot 22.00 uur.	
1 ^e -lijns ondersteuning voor het melden van incidenten door klanten en leveranciers	24 uur per dag, 7 dagen per week, alle dagen van het jaar.	Werkdagen van 8.00 uur tot 17.00 uur.
1 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door klanten en leveranciers	Werkdagen van 8.00 uur tot 17.00 uur.	Werkdagen van 8.00 uur tot 17.00 uur.
1 ^e -lijns ondersteuning voor het aansluiten op de dienst door klanten en leveranciers	Werkdagen van 8.00 uur tot 17.00 uur.	Werkdagen van 8.00 uur tot 17.00 uur.
1 ^e -lijns ondersteuning voor het melden van calamiteiten	24 uur per dag, 7 dagen per week, alle dagen van het jaar.	Werkdagen van 7.00 uur tot 18.00 uur.

6.1.4

Prioriteiten & oplostijden

Om op een juiste wijze om te gaan met de verschillen in aard en aantal bij de afhandeling van incidenten zijn de incidenten als volgt geclassificeerd en geprioriteerd:

DigiD voor burgers productieomgeving:

Functionaliteit	Prioriteit		
	Prio 1	Prio 2	Prio 3
Primaïr			
Authenticatie			
werkt niet meer voor	> 100 gebruikers > 2 klanten een top-5 klant	2-100 gebruikers 1-2 klanten	1 gebruiker
performance wordt niet gehaald	> 5 min	1-5 min	< 1 min
Aanvragen en activeren account			
werkt niet meer voor	> 25 gebruikers	2-25 gebruikers	1 gebruiker
Beheer module			
werkt niet meer voor	> 1 beheerder		1 beheerder
Website DigiD.nl			
werkt niet meer voor	>= 50% van alle gebruikers		< 50% van alle gebruikers
performance wordt niet gehaald	> 5 min	1-5 min	< 1 min
Versturen briefbestand			
wordt niet verstuurd naar Group Joos		1e keer	
Beveiliging			
aanval	alle incidenten		
door Govcert.nl aangegeven risico	Hoog (Govcert)		Midden en laag (Govcert)
Secundair			
Mijn gegevens			
werkt niet meer voor		>= 50% van alle gebruikers	< 50% van alle gebruikers
Beheer module			
performance wordt niet gehaald		>= 30 min	< 30 min
Aansluiten klant			
werkt niet meer voor		> 1 klant	1 klant
Versturen briefbestand			
wordt niet verstuurd naar Group Joos	2e en opvolgende keer		

De prioriteit bepaalt de oplostijd van incidenten binnen het servicewindow.

N.B. Hoog = Prio 1, Midden = Prio 2, Laag = Prio 3.

De severity van P1 meldingen die via mail aan Atos Origin worden verstuurd, moeten via de helpdesk van Atos Origin () opgehoogd worden van 2 naar 1. Via mail is het namelijk alleen mogelijk om een P1 met severity 2 aan te leveren.

Performance indicatoren voor oplossen incidenten in de productieomgeving			
Prioriteit	Oplostijd	Terugkoppeling	Minimaal te realiseren
Hoog	8 uur	Na oplossing van Incident aan melder	15% van het aantal Incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Hoog niet binnen 100% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Midden	1 werkdag	Na oplossing van Incident aan melder	15% van het aantal Incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Midden niet binnen 150% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Laag	2 werkdagen	Na oplossing van Incident aan melder	15% van het aantal Incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Midden niet binnen 150% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.

Performance indicatoren voor oplossen incidenten in de pré-productieomgeving			
Prioriteit	Oplostijd	Terugkoppeling	Minimaal te realiseren
Hoog	1 werkdag	Na oplossing van Incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Hoog niet binnen 100% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Midden	2 werkdagen	Na oplossing van Incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Midden niet binnen 150% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Laag	3 werkdagen	Na oplossing van Incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een incident met prioriteit Midden niet binnen 150% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.

6.1.5

Leverancier(s)

De leveranciers die een rol spelen bij DigiD voor burgers zijn:

leverancier	rol
Atos Origin	Applicatiebeheer en Infrabeheer, webhosting DigiD.nl
Group Joos	Print & mail service
Cendris	Helpdesk
Golden Bytes	SMS gateway
BPR	Gegevensbeheer GBA-V
Gemnet	Verbinding tussen DigiD en GBA-V
DigiNotar	Certificaatverstrekker voor DigiD
Netcreators	Applicatiebeheer DigiD.nl (CMS)

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.1.6

*Oplostijden leveranciers*Atos Origin

DigiD Burger en Bedrijven Productieomgeving					
Nr.	Prestatie-indicator	Vorm	Norm per prioriteit		
			Hoog	Midden	Laag

PI 1.7	Oplostijd binnen de Support-uren ¹	Tijd en %	Binnen 4 uur in minimaal 85% gevallen	Binnen 8 uur in minimaal 85% gevallen	Binnen 16 uur in minimaal 85% gevallen
--------	---	-----------	---------------------------------------	---------------------------------------	--

N.B. Definitie van prioriteiten zijn conform die in paragraaf 6.1.4.

Group Joos

Impact	Omschrijving Incident
Hoog	In de volgende gevallen wordt de impact 'hoog' toegekend aan het Incident: <ul style="list-style-type: none"> het Incident heeft of kan ernstige gevolgen hebben voor het printen en ter verzending aanbieden van brieven; het Incident heeft betrekking op het printen en ter verzending aanbieden van brieven aan een significant deel van de eindgebruikers.
Laag	Overige situaties.

Urgentie	Omschrijving Incident
Hoog	De urgentie 'hoog' toegekend aan een Incident indien de kwaliteit van functionaliteit, prestatie, beschikbaarheid en beveiliging volledig wordt beïnvloed.
Laag	Overige situaties.

Impact/Urgentie	Prioriteit
Hoog/Hoog	Prio 2
Hoog/Laag	Prio 4
Laag/Hoog	
Laag/Laag	Prio 5

Prioriteit	Oplostijd
Prio 2	Minimaal 85% van de Incidenten is binnen 8 uur opgelost
Prio 4	Minimaal 85% van de Incidenten is binnen 24 uur opgelost
Prio 5	Minimaal 85% van de Incidenten is binnen 48 uur opgelost

Cendris

Impact	Omschrijving Incident
Hoog	Impact 'hoog' wordt toegekend aan het Incident indien het incident betrekking heeft op de dienstverlening (m.b.t. helpdesk activiteiten) aan een significant deel van de eindgebruikers.
Laag	Overige situaties.

Urgentie	Omschrijving Incident
Hoog	De urgentie 'hoog' toegekend aan een Incident indien de kwaliteit van functionaliteit van de dienstverlening (m.b.t. helpdesk activiteiten aan eindgebruikers), prestatie, beschikbaarheid en beveiliging volledig wordt beïnvloed.
Laag	Overige situaties.

Impact/Urgentie	Prioriteit
-----------------	------------

Hoog/Hoog	Prio 2
Hoog/Laag	Prio 4
Laag/Hoog	
Laag/Laag	Prio 5

Prioriteit	Oplostijd
Prio 2	Minimaal 85% van de Incidenten is binnen 8 uur opgelost
Prio 4	Minimaal 85% van de Incidenten is binnen 24 uur opgelost
Prio 5	Minimaal 85% van de Incidenten is binnen 48 uur opgelost

Golden Bytes

Incident melding Prioriteit	Vergelijkbaar Serviceorganisatie Melding niveau (1-5)	Omschrijving Incident Opdrachtgever stelt initiële prioriteit.
Hoog	2	In de volgende gevallen kan de prioriteit 'hoog' worden toegekend aan het Incident: <ul style="list-style-type: none"> de gehele dienstverlening of primaire functionaliteit van de dienstverlening is niet beschikbaar; het Incident heeft betrekking op de beveiliging van de dienstverlening.
Midden	3	In de volgende gevallen kan aan de prioriteit 'midden' worden toegekend aan een Incident: <ul style="list-style-type: none"> secundaire functionaliteit van de dienstverlening is niet beschikbaar.
Laag	4	In overige situaties die betrekking hebben op de uitvoering van Exploitatieprocessen (exclusief Exploitatieproces rapportage) kan prioriteit 'laag' worden toegekend aan een Incident.

Onder primaire functionaliteit wordt verstaan:

- de mogelijkheid tot het ontvangen (door Opdrachtnemer) van SMS-verzoeken (interface richting de DigiD applicatie);
- de mogelijkheid tot het verzenden van SMS-berichten (dit betreft de tijd tussen de ontvangst van het verzoek tot verzenden van een SMS in de Ontvangstfaciliteit en de ontvangst van de te verzenden SMS in de Verzendfaciliteit)

Onder secundaire functionaliteit van de dienstverlening kan worden verstaan:

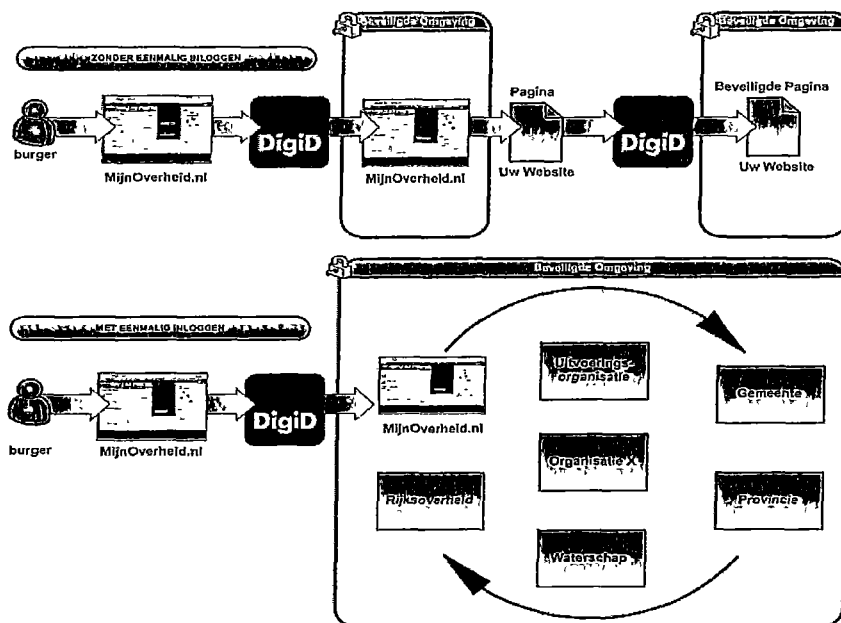
- back-up mogelijkheden voor het ontvangen (door Opdrachtnemer) van SMS-verzoeken (interface richting de DigiD applicatie)

Indicator	Vorm	Norm
Oplostijd	Tijd	<ul style="list-style-type: none"> Incidenten met Prioriteit Hoog: Minimaal 85% van de Incidenten is binnen 8 uur na melding opgelost; Incidenten met Prioriteit Midden: Minimaal 85% van de Incidenten is binnen 24 uur, d.w.z. 1 Werkdag na melding opgelost; Incidenten met Prioriteit Laag: Minimaal 85% van de Incidenten is binnen 48 uur, d.w.z. 2 Werkdagen na melding opgelost.

6.2 Eenmalig inloggen

6.2.1 Globale werking

Een gebruiker logt in via DigiD. Zijn gegevens worden door de server van de federatie gecontroleerd en bijgehouden. Deze authenticatie via DigiD vindt plaats op zekerheidsniveau basis (gebruikersnaam en wachtwoord).

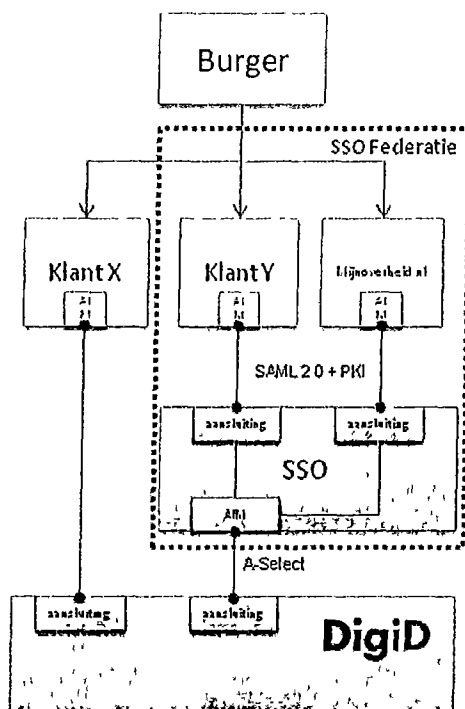


Overheidsorganisaties bepalen zelf welk zekerheidsniveau van DigiD is vereist (niveau Basis of Midden). Indien het zekerheidsniveau hoger is dan waarmee een burger is ingelogd, ontvangt de burger een melding met de mogelijkheid op een hoger niveau in te loggen en wordt in de federatie het hogere inlogniveau geregistreerd.

De URL waaraan Eenmalig inloggen te herkennen is <https://federatie.overheid.nl>

6.2.2 Systeemlandschap

De ICT infrastructuur voor Eenmalig inloggen (SSO in onderstaande figuur) bevindt zich bij ICTU.



6.2.3 Dienstverlening

De dienstverlening is gelijk aan die van DigiD voor burgers. Zie paragraaf 6.1.3.

6.2.4 Prioriteiten & oplostijden

Prioriteiten en oplostijden zijn gelijk aan die voor DigiD voor burgers. Zie paragraaf 6.1.4.

6.2.5 Leverancier(s)

De leveranciers die een rol spelen bij Eenmalig inloggen zijn:

leverancier	rol
ICTU	ICT infra- en applicatiebeheer

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.2.6 Oplostijden leveranciers

ICTU

Prioriteiten:

	Prioriteit		
	Hoog	Midden	Laag
Verkrijgen toegang:			
Website			
Werkt niet meer voor:	> 100 gebruikers	2-100 gebruikers	1 gebruiker

	Prioriteit		
	Hoog	Midden	Laag
	≥ 1 Cat.1 ⁽⁴⁾ > 2 Cat.2 dienstaanbieders	1-2 dienstaanbieders	
Prestatie wordt niet gehaald	> 5 minuten	1-5 minuten	< 1 minuut
Aansluiten dienst aanbieder			
Werkt niet meer voor:	n.v.t.	> 1 dienstaanbieder	1 dienstaanbieder
Aansluiten softwareontwikkelaar			
Werkt niet meer voor:	n.v.t.	> 1 software- ontwikkelaar ⁽⁵⁾	1 software- ontwikkelaar
Werkt niet meer voor:	≥ 50% van alle gebruikers	n.v.t.	< 50% van alle gebruiker
Prestatie wordt niet gehaald	> 5 minuten	1-5 minuten	< 1 minuut
Security incident			
Aanval ⁽⁶⁾	alle incidenten	n.v.t.	n.v.t.
Door GOVCERT.NL ⁽⁷⁾ aangegeven risico	hoog	n.v.t.	medium en laag

"Eenmalig inloggen" Productieomgeving(en)					
Prestatie indicator				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja / Nee	Interval
PI 1.4	Incident Prio hoog	aantal %	85% binnen 4 uur opgelost	Ja	maand
PI 1.5	Incident Prio midden	aantal %	85% binnen 8 uur opgelost	Ja	maand
PI 1.6	Incident Prio laag	aantal %	85% binnen 24 uur opgelost	Ja	maand

⁴ In het DAP is een tabel opgenomen met Dienstaanbieders en de bijbehorende Categorie(1 of 2)

⁵ Als software ontwikkelaar wordt hier bedoeld de software ontwikkelaar van de Dienstaanbieder

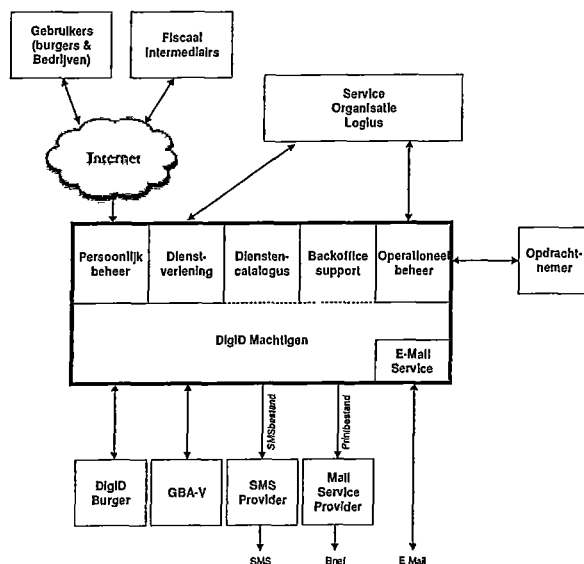
⁶ Met een aanval wordt (het vermoeden van) een aanval van buitenaf bedoeld bijvoorbeeld een (Distributed) Denial-of-Service aanval.

⁷ GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid en ondersteunt overheidsorganisaties in ICT- en informatiebeveiliging met diensten als preventie, waarschuwing, advisering, kennisdeling en monitoring.

6.3 DigiD Machtigen

6.3.1 Globale werking

DigiD Machtigen maakt het mogelijk dat iemand wordt gemachtigd om namens een ander elektronisch zaken te regelen met de overheid. Een burger kan hiermee op een betrouwbare manier bijvoorbeeld een buurvrouw of kennis machtigen om namens hem of haar zaken te doen met de overheid, bv. voor het indienen van de belastingaangifte. Deze machtiging wordt in een register vastgelegd. Op het moment dat de persoon die gemachtigd is zaken doet met de betreffende overheidsorganisatie, raadpleegt de overheidsorganisatie het machtigingsregister. Hierdoor kan de overheidsorganisatie toetsen of iemand anders deze aanvraag mag doen.



6.3.2 Dienstverlening

Vanaf 1 januari 2010 doet Logius standby en de incidenten.

De dienstverlening bestaat uit de elektronische dienstverlening (de DigiD machtigen applicatie die via Internet wordt ontsloten naar de eindgebruikers) en de gebruikersondersteuning aan burgers (door de Helpdesk) en klanten (door het Servicecentrum).

Zodra er sprake is van een (dreigende) verstoring van de hieronder beschreven dienstverlening, is er sprake van een incident.

Eigenschappen van de elektronische dienstverlening zijn:

Performance indicatoren voor Openstellingswindow		
Soort afspraak	Norm	Minimaal te realiseren
Beschikbaarheid van de dienst voor burgers (productieomgeving)	De productieomgeving van DigiD Machtigen is 7*24 uur, alle dagen van het jaar, beschikbaar voor: Het verlenen van machtigingen voor burgers; Activeren van machtigingen d.m.v. een activeringscode; Afhandelen van machtigingsverzoeken.	99,95 % beschikbaar.
Beschikbaarheid van de DigiD website: openstelling van de dienst (productie)	De productieomgeving van DigiD Machtigen is 7*24 uur, alle dagen van het jaar, beschikbaar.	99,95 % beschikbaar.
Beschikbaarheid van de van de dienst voor klanten (productieomgeving)	De productieomgeving van DigiD Machtigen is 7*24 uur, alle dagen van het jaar, beschikbaar voor een operationele klant.	99,95 % beschikbaar.
Beschikbaarheid van de DigiD Machtigen Ketentacceptatieomgeving	De ketentacceptatieomgeving van DigiD Machtigen is van 7:00 tot 19:00 uur, op werkdagen	99,7 % beschikbaar.
Beschikbaarheid van de DigiD Machtigen Acceptatieomgeving	De acceptatieomgeving van DigiD Machtigen is van 7:00 tot 19:00 uur, op werkdagen	99,5 % beschikbaar.

Performance indicatoren voor Onderhoudswindow	
	Norm
Soort afspraak	Productieomgeving
Structureel gepland onderhoud m.b.t. diensten	1 maal per maand. Iedere 2 ^e maandag van de maand van 0:00 tot 06:00 en uitsluitend na overleg met Opdrachtgever. Voor security updates kan uitsluitend in overleg met Opdrachtgever een uitzondering worden gemaakt.
Onderhoud m.b.t. de technische installaties	Maximaal 4 keer per jaar, gedurende maximaal 4 uur.
DigiD-Machtigen Ketentacceptatieomgeving	Op Werkdagen tussen 19:00 uur en 07:00 uur (uitsluitend na overleg met Opdrachtgever).
DigiD Machtigen Acceptatieomgeving	Op Werkdagen tussen 19:00 uur en 07:00 uur (uitsluitend na overleg met Opdrachtgever).

Performance Indicator voor capaciteit en performance DigiD Machtigen systemen		
Soort afspraak	Norm	Minimaal te realiseren
Voorziening	Maximale Verwerkingstijd initiëren machtiging bij	1 seconden in 99,8% van de

	maximaal 200 gelijktijdige verzoeken.	gevallen
	Maximale Verwerkingstijd opvragen keuzeschermbemachtigingsmiddelen bij maximaal 200 gelijktijdige verzoeken.	1,5 seconden in 99,8% van de gevallen
	Maximale Verwerkingstijd redirect naar bemachtigingsmiddelen bij maximaal 200 gelijktijdige verzoeken.	1,5 seconden in 99,8% van de gevallen
	Maximale Verwerkingstijd beschikbaar stellen bemachtigingresultaat bij maximaal 200 gelijktijdige verzoeken.	2 seconden in 99,8% van de gevallen
	Maximale Verwerkingstijd opvragen bemachtigingsgegevens bij maximaal 200 gelijktijdige verzoeken.	2 seconden in 99,8% van de gevallen
	Verwerkingscapaciteit voorziening	Minimaal 900 gelijktijdige sessies
GBAV	Maximale tijd noodzakelijk voor het versturen van een GBAV verzoek bij een continue verzending van 750 GBAV verzoeken per minuut.	0,5 seconde in 99,5% van de gevallen
DigID	Maximale tijd noodzakelijk voor het versturen van een GBAV verzoek bij een continue verzending van 750 DigID verzoeken per minuut.	0,5 seconde in 99,5% van de gevallen
Website	Maximaal aantal transacties per uur	70.000
	Maximale responsetijd per transactie	≤ 0,15 seconde in 97% van de gevallen ≤ 0,2 seconde in 99, 99% van de gevallen

Kentallen met betrekking tot capaciteit en performance DigID systemen		
Soort afspraak	Norm	Minimaal te realiseren
Capaciteit Authenticaties Machtigingen	Het aantal Authenticaties op machtigingen wordt gegarandeerd op ... authenticaties per uur (gedurende 24 uur per dag).	N.v.t.

Eigenschappen van de gebruikersondersteuning zijn:

Performance indicatoren voor servicewindow	
Beschikbaarheid	Norm
	Productie omgeving
1 ^{ste} lijns ondersteuning voor het melden van incidenten door burgers.	Werkdagen van 8.00 uur tot 22.00 uur.

1 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door burgers.	Werkdagen van 8.00 uur tot 22.00 uur.
1 ^e -lijns ondersteuning voor het melden van incidenten door klanten en leveranciers.	24 uur per dag, 7 dagen per week, alle dagen van het jaar.
1 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door klanten en leveranciers.	Werkdagen van 8.00 uur tot 17.00 uur.
1 ^e -lijns ondersteuning voor het aansluiten op de dienst van klanten en leveranciers.	Werkdagen van 8.00 uur tot 17.00 uur.
1 ^e -lijns ondersteuning voor het melden van calamiteiten.	24 uur per dag, 7 dagen per week, alle dagen van het jaar.

6.3.3

Prioriteiten & oplostijden

Om op een juiste wijze om te gaan met de verschillen in aard en aantal bij de afhandeling van incidenten zijn de incidenten als volgt geclassificeerd en geprioriteerd:

DigiD Machtigen productieomgeving:

	Prioriteit		
	Hoog	Midden	Laag
Machtigen			
Werkt niet meer voor:	> 100 gebruikers	2-100 gebruikers	1 gebruiker
	> 2 dienst- aanbieders	1-2 dienst- aanbieders	
	>2 software-ontwikkelaars ⁸	1-2 software-ontwikkelaars	
Performance wordt niet gehaald ⁹	> 5 minuten	1-5 minuten	< 1 minuut
Aanvragen, activeren en intrekken machtiging			
Werkt niet meer voor:	> 25 gebruikers	2-25 gebruikers	1 gebruiker
Overzicht machtigingen inclusief inzien machtiging details			
Werkt niet meer voor:		≥ 50% van alle gebruikers	< 50% van alle gebruiker
Dienstverleningsapplicatie			
Werkt niet meer voor:	> 1 helpdesk-medewerker		1 helpdesk-medewerker

⁸ Met een softwareontwikkelaar wordt hier een partij bedoeld dat externe software (bv boekhoudpakket) ontwikkelt dat samenwerkt met DigiD Machtigen.

⁹ Performance volgens de in paragraaf 6.5.5s gespecificeerde prestatie-indicatoren.

Performance wordt niet gehaald		≥ 30 minuten	< 30 minuten
Beheermodule			
Werkt niet meer voor:	> 1 servicedesk-medewerker		1 servicedesk-medewerker
Performance wordt niet gehaald		≥ 30 minuten	< 30 minuten
Website			
Werkt niet meer voor:	≥ 50% van alle gebruikers		< 50% van alle gebruiker
Performance wordt niet gehaald	> 5 minuten	1-5 minuten	< 1 minuut
Security incident			
Aanval ¹⁰	alle Incidenten		
Door GOVCERT.NL ¹¹ aangegeven risico	hoog		medium en laag
Calamiteit¹²			
	Opdrachtgever bepaald	Opdrachtgever bepaald	Opdrachtgever bepaald
Overige incidenten¹³			
	n.v.t.	n.v.t.	allemaal

De prioriteit bepaalt de oplostijd van incidenten binnen het servicewindow.
N.B. Hoog = Prio 1, Midden = Prio 2, Laag = Prio 3.

De severity van P1 meldingen die via mail aan CAP//Getronics worden verstuurd, moeten via de helpdesk van CAP/Getronics opgehoogd worden van 2 naar 1. Via mail is het namelijk alleen mogelijk om een P1 met severity 2 aan te leveren.

Performance Indicatoren voor oplossen Incidenten in de productieomgeving			
Prioriteit	Oplostijd	Terugkoppeling	Minimaal te realiseren
Hoog	8 uur	Na oplossing van incident aan melder.	85% van de incidenten wordt conform de norm opgelost. Indien voorzienbaar is dat een incident. Indien voorzien wordt dat een incident met prioriteit

¹⁰ Met een aanval wordt een aanval van buitenaf bedoeld bijvoorbeeld een (Distributed) Denial-of-Service aanval.

¹¹ GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid

¹² In geval van een Calamiteit bepaald Opdrachtgever de prioriteit en kunnen prioriteiten worden verhoogd van laag naar midden en van midden naar hoog.

¹³ Als incidenten niet kunnen worden geclassificeerd aan hand van bovenstaande tabel dan krijgen ze automatisch prioriteit laag.

			"Hoog" niet binnen de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Midden	1 werkdag	Na oplossing van Incident aan melder.	85% van de Incidenten wordt conform de norm opgelost. Indien voorzienbaar is dat een Incident . Indien voorzien wordt dat een incident met prioriteit "Hoog" niet binnen 150% van de norm oplostijd kan worden opgelost, wordt geëscaleerd.
Laag	2 werkdagen	Na oplossing van Incident aan melder.	85% van de Incidenten wordt conform de norm opgelost. Indien voorzienbaar is dat een Incident . Indien voorzien wordt dat een incident met prioriteit "Hoog" niet binnen 150% van de norm oplostijd kan worden opgelost, wordt geëscaleerd.

6.3.4

Leverancier(s)

De leveranciers die een rol spelen bij DigiD Machtigen zijn:

Leverancier	Rol
CAP	Applicatiebeheer en infrabeheer, webhosting DigiD.nl
Group Joos	Print & mail service
Cendris	Helpdesk
Golden Bytes	SMS gateway
BPR	Gegevensbeheer GBA-V
Gernnet	Verbinding tussen DigiD en GBA-V
DigiNotar	Certificaatverstrekker voor DigiD
Netcreators	Applicatiebeheer DigiD.nl (CMS)

Zie paragraaf **8.3** voor de contactgegevens van de leveranciers.

6.3.5

*Oplostijden leveranciers*CAP

DigiD Machtigen				
Prestatie Indicator	Vorm	Norm per prioriteit		
		Hoog	Midden	Laag
Oplostijd binnen de supporturen	Tijd en %	Binnen 4 uur in minimaal 85% gevallen	Binnen 8 uur in minimaal 85% gevallen	Binnen 16 uur in minimaal 85% gevallen

N.B. Definitie van prioriteiten zijn conform die in paragraaf **6.1.4**.

Group Joos

Impact	Omschrijving Incident
Hoog	In de volgende gevallen wordt de impact 'hoog' toegekend aan het Incident: het Incident heeft of kan ernstige gevolgen hebben voor het printen en ter verzending aanbieden van brieven; het Incident heeft betrekking op het printen en ter verzending aanbieden van brieven aan een significant deel van de eindgebruikers.
Laag	Overige situaties.

Urgentie	Omschrijving Incident
Hoog	De urgentie 'hoog' toegekend aan een Incident indien de kwaliteit van functionaliteit, prestatie, beschikbaarheid en beveiliging volledig wordt beïnvloed.
Laag	Overige situaties.

Impact/Urgentie	Prioriteit
Hoog/Hoog	Prio 2
Hoog/Laag Laag/Hoog	Prio 4
Laag/Laag	Prio 5

Prioriteit	Oplostijd
Prio 2	Minimaal 85% van de Incidenten is binnen 8 uur opgelost
Prio 4	Minimaal 85% van de Incidenten is binnen 24 uur opgelost
Prio 5	Minimaal 85% van de Incidenten is binnen 48 uur opgelost

Cendris

Impact	Omschrijving Incident
Hoog	Impact 'hoog' wordt toegekend aan het Incident indien het Incident betrekking heeft op de dienstverlening (m.b.t. helpdesk activiteiten) aan een significant deel van de eindgebruikers.
Laag	Overige situaties.

Urgentie	Omschrijving Incident
Hoog	De urgentie 'hoog' toegekend aan een Incident indien de kwaliteit van functionaliteit van de dienstverlening (m.b.t. helpdesk activiteiten aan eindgebruikers), prestatie, beschikbaarheid en beveiliging volledig wordt beïnvloed.
Laag	Overige situaties.

Impact/Urgentie	Prioriteit
Hoog/Hoog	Prio 2
Hoog/Laag Laag/Hoog	Prio 4
Laag/Laag	Prio 5

Prioriteit	Oplostijd
Prio 2	Minimaal 85% van de Incidenten is binnen 8 uur opgelost
Prio 4	Minimaal 85% van de Incidenten is binnen 24 uur opgelost
Prio 5	Minimaal 85% van de Incidenten is binnen 48 uur opgelost

Golden Bytes

Prioriteit Incident-melding	Vergelijkbaar Serviceorganisatie Melding niveau (1-5)	Omschrijving Incident Opdrachtgever stelt initiële prioriteit
Hoog	2	In de volgende gevallen kan de prioriteit "hoog" worden toegekend aan het Incident: De gehele dienstverlening of primaire functionaliteit van de dienstverlening is niet beschikbaar Het Incident heeft betrekking op de beveiliging van de dienstverlening.
Midden	3	In de volgende gevallen kan de prioriteit "midden" worden toegekend aan het Incident: Secundaire functionaliteit van de dienstverlening is niet beschikbaar.
Laag	4	In overige situaties die betrekking hebben op de uitvoering van Exploitatieprocessen (exclusief Exploitatieproces rapportage) kan prioriteit "laag" worden toegekend aan een Incident.

Onder primaire functionaliteit wordt verstaan:

- de mogelijkheid tot het ontvangen (door Opdrachtnemer) van SMS-verzoeken (interface richting de DigiD Machtigen applicatie);

- de mogelijkheid tot het verzenden van SMS-berichten (dit betreft de tijd tussen de ontvangst van het verzoek tot verzenden van een SMS in de Ontvangstfaciliteit en de ontvangst van de te verzenden SMS in de Verzendfaciliteit)

Onder secundaire functionaliteit van de dienstverlening kan worden verstaan:

- back-up mogelijkheden voor het ontvangen (door Opdrachtnemer) van SMS-verzoeken (Interface richting de DigiD Machtigen applicatie)

Indicator	Vorm	Omschrijving Incident <i>Opdrachtgever stelt initiële prioriteit</i>
Oplostijd	Tijd	Incidenten met Prioriteit Hoog: minimaal 85% van de Incidenten is binnen 8 uur na melding opgelost; Incidenten met Prioriteit Midden: Minimaal 85% van de Incidenten is binnen 24 uur, d.w.z. 1 Werkdag, na melding opgelost Incidenten met Prioriteit Laag: Minimaal 85% van de Incidenten is binnen 48 uur, d.w.z. 2 Werkdagen, na melding opgelost

6.4 PKIoverheid

6.4.1 *Globale werking*

Public Key Infrastructure voor de overheid, kortweg PKIoverheid, maakt betrouwbare digitale communicatie mogelijk. Met behulp van PKI-certificaten is de informatie die personen en organisaties over het internet sturen, beveiligd op een hoog niveau van betrouwbaarheid.

PKIoverheid certificaten worden gebruikt bij:

- het zetten van een rechtsgeldige elektronische handtekening
- het beveiligen van websites
- het op afstand authenticeren van personen of services
- het versleutelen van berichten

Zie verder:

<http://www.logius.nl/producten/toegang/pkioverheid/productinformatie/over-pkioverheid/>

6.4.2 *Dienstverlening*

Voor dit product hoeft geen standby dienst te worden uitgevoerd.

6.4.3 *Prioriteiten & oplostijden*

Niet van toepassing tijdens standby dienst.

6.4.4 *Leverancier(s)*

De uitgevers van certificaten binnen PKIoverheid kunnen private of publieke partijen zijn, onder voorwaarde dat zij voldoen aan de gestelde eisen. Hiertoe behoren ook de eisen die zijn gesteld aan de dienstverlener die gekwalificeerde certificaten uitgeeft. Dit zijn eisen aan bijvoorbeeld

- het identificatieproces dat de certificatedienstverlener moet uitvoeren bij uitgifte van een certificaat;
- eisen aan de te bewaren gegevens en de bewaartermijnen en
- eisen aan de continuïteit van de dienstverlening van de certificatedienstverlener.

De certificaatuitgever is verplicht zich te laten registreren bij de OPTA.

De huidige leveranciers van certificaten zijn:

Naam CSP	Domein	Datum toetreding	Bijzonderheden
<u>Getronics PinkRocade Nederland BV</u>	Overheid & Bedrijven	6 oktober 2003	Persoonsgebonden certificaten en services certificaten
<u>Diginotar BV</u>	Overheid & Bedrijven	2 juni 2004	Persoonsgebonden certificaten en services certificaten
<u>CIBG</u>	Overheid & Bedrijven	22 december 2004	Persoonsgebonden certificaten en services certificaten voor de Zorgsector
<u>ESG De electronische signatuur BV</u>	Organisatie	23 augustus 2006	Persoonsgebonden certificaten en services certificaten
<u>Ministerie van Defensie</u>	Overheid & Bedrijven	22 april 2008	Persoonsgebonden certificaten voor de Defensiesector
<u>QuoVadis Trustlink BV</u>	Organisatie	14 juli 2009	Persoonsgebonden certificaten en services certificaten

6.5 Digipoort X.400/SMTP/FTP/POP3/SOAP

6.5.1 Globale werking

Digipoort is hét elektronische postkantoor van de overheid voor bedrijven. Het verzorgt de gemeenschappelijke infrastructuur voor het berichtenverkeer tussen bedrijven enerzijds en overheden anderzijds.

Een bedrijf stuurt een envelop met adresgegevens (elektronisch bericht), waaraan documenten kunnen worden toegevoegd naar Digipoort. Digipoort sorteert de documenten uit het bericht, voert eventuele validaties uit en kijkt voor welke overheidsinstelling ze bestemd zijn. Daarna levert Digipoort het bericht met de juiste documenten af bij de juiste ontvangers.

Van iedere verstuurde envelop wordt bekeken of de afzender wel bekend en geautoriseerd is voor het versturen van gegevens naar de ontvanger. Authenticatie en beveiliging zijn daarom belangrijke aspecten van Digipoort.

Communicatie kan plaatsvinden middels de koppelvlakken OTP Nieuw (X.400, SMTP, POP3, FTP) en PI (SOAP). Dit onderscheid wordt hieronder geëxpliciteerd.

6.5.2 Dienstverlening

De dienstverlening bestaat uit de elektronische dienstverlening (de Digipoort voorziening die via Internet wordt ontsloten naar bedrijven overheden, en de gebruikersondersteuning aan bedrijven en overheden (door het Servicecentrum).

Zodra er sprake is van een (dreigende) verstoring van de hieronder beschreven dienstverlening, is er sprake van een incident.

Eigenschappen van de elektronische dienstverlening voor de klant zijn: OTP Nieuw en PI.

Performance indicatoren voor openstellingswindow		
Beschikbaarheid	Productie	Pre-productie
Openstelling:	24 uur per dag, 7 dagen per week, alle dagen van het jaar.	24 uur per dag, 7 dagen per week, alle dagen van het jaar.
Norm beschikbaarheidspercentage:	99,7 %	99%.

Eigenschappen van de gebruikersondersteuning voor de klant zijn: OTP Nieuw en PI.

Performance indicatoren voor servicewindow		
Voor het melden van:	Beschikbaarheid:	Via:

Incidenten	Werkdagen van 8.00 uur tot 17.00 uur.	E-Mail en telefoon
Klachten en het stellen van vragen	Werkdagen van 8.00 uur tot 17.00 uur.	E-Mail en telefoon
X Calamiteiten	24 uur per dag, 7 dagen per week, alle dagen van het jaar.	E-mail tussen 8 – 17:00 Telefoon 7 * 24
X Storingen ¹⁴ aan de kant van de Afnemer	24 uur per dag, 7 dagen per week, alle dagen van het jaar.	E-mail tussen 8 – 17:00 Telefoon 7 * 24

Let op:

Calamiteiten en Storingen gelden alleen voor Digipoort X.400/SMTP/FTP/POP3. Deze worden bewaakt door KPN/Getronics. Indien er door KPN een incident gesignaleerd wordt zal de stand-by dienst van Tactisch beheer Logius gebeld worden. Bedrijfsdeelnemers en overheidsdeelnemers die geen berichten ontvangen kunnen dit melden bij de stand-by dienst.

Tijdens kantooruren (werkdagen, 08.00- 17.00 uur), worden incidenten rondom Digipoort X.400/SMTP/FTP/POP3 gemeld door KPN/Getronics en afgehandeld door Logius.

Buiten kantooruren kunnen bedrijfsdeelnemers en overheidsdeelnemers die geen berichten ontvangen dit melden bij de stand-by dienst. Deze zal dan KPN/Getronics inschakelen.

6.5.3**Prioriteiten & oplostijden**

Om op een juiste wijze om te gaan met de verschillen in aard en aantal bij de afhandeling van incidenten zijn de incidenten als voor de klant volgt geclassificeerd en geprioriteerd.

OTP Nieuw en PI

Impact	Omschrijving incident
Hoog	In de volgende gevallen kan de Impact 'hoog' worden toegekend aan het Incident: het incident heeft of kan ernstige gevolgen hebben voor het proces van de Gebruikers en / of Afnemers; het Incident heeft betrekking op een significant deel van de Gebruikers en / of Afnemers.
Laag	Overige-situaties.

¹⁴ Waarbij een storing getypeerd wordt als een incident of calamiteit bij de Afnemer, waardoor de keten dienstverlening (tijdelijk) niet beschikbaar is.

Urgentie	Omschrijving incident
Hoog	In de volgende gevallen kan aan de urgentie 'hoog' worden toegekend aan een incident: de werking, functionaliteit, performance, beschikbaarheid en / of beveiliging wordt volledig beïnvloed; directe communicatie tussen Logius en de Afnemers is verstoord.
Laag	Overige situaties.

Impact en urgentie bepalen de prioriteit voor het oplossen van incidenten binnen het servicewindow voor de klant.

OTP Nieuw en PI

Prestatie-indicatoren oplostijd van incidenten en terugkoppeling aan Afnemer			
Impact/Urgentie		Oplostijd (in uren na melding)	Terugkoppeling aan Afnemer
Hoog/Hoog	Prio 1	4	Binnen een uur (24 uur per dag, alle dagen van het jaar) en daarna afstemming in overleg.
Hoog/Laag, Laag/Hoog	Prio 2	8	binnen een uur(alle dagen van het jaar, tussen 08:00 – 22:00 uur) en daarna afstemming in overleg
Laag/Laag	Prio 3	1 werkdag	geen
	Norm	85 %.	100 %.

6.5.4

Leveranciers

De leveranciers die een rol spelen bij Digipoort zijn:

leverancier	rol
KPN/Getronics	Applicatie- en infrabeheer OTP Nieuw koppelvlak (X.400, SMTP, FTP en POP3)
EBPI	Applicatiebeheer PI koppelvlak (SOAP)
Equinix	ICT Infrabeheer PI koppelvlak (SOAP)

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.5.5

Calamiteitenbeheer

Een calamiteit is een verstoring (zie ook 6.6.2.1 e.v.) van de dienstverlening waarbij verwacht wordt, dat de vastgestelde servicetijden overschreven zullen worden. Daarnaast kan dit type verstoring leiden tot imagoschade voor één of meer partijen.

OTP Nieuw

Samenstellen calamiteitenteam	Servicecentrum Logius escaleert de calamiteit direct, uiterlijk binnen 1 uur, naar Logius. Logius en Servicecentrum Logius bepalen of een gebeurtenis definitief is aan te merken als een calamiteit en stellen de
-------------------------------	--

	leden van het calamiteitenteam vast.
Afnemers melden van calamiteit	Binnen 1 uur na constatering
Oplossen calamiteit	Afhankelijk van grootte en impact van calamiteit

PI

Samenstellen calamiteitenteam	Servicecentrum Logius escaleert de calamiteit direct, uiterlijk binnen 2 uur, naar Logius. Logius en Servicecentrum Logius bepalen of een gebeurtenis definitief is aan te merken als een calamiteit en stellen de leden van het calamiteitenteam vast.
Afnemers melden van calamiteit	Binnen 2 uur na constatering
Oplossen calamiteit	Afhankelijk van grootte en impact van calamiteit

6.6 Berichtenspiegel

Digipoort maakt uitwisseling van verantwoordingsinformatie mogelijk. Denk aan aangiften, jaarverslagen, balansen enzovoort: informatie die is ingedeeld volgens een vaste taxonomie (Nederlandse taxonomie) en wordt aangeleverd in XBRL-formaat.

Met de Berichtenspiegel kunnen bedrijven en organisaties XBRL-berichten leesbaar maken. Zo draagt Logius bij aan een nog efficiëntere Digipoort.

6.6.1 Werking

Digipoort maakt uitwisseling van verantwoordingsinformatie mogelijk. Denk aan aangiften, jaarverslagen, balansen enzovoort: informatie die is ingedeeld volgens een vaste taxonomie (Nederlandse taxonomie) en wordt aangeleverd in XBRL-formaat.

Met de Berichtenspiegel kunnen bedrijven en organisaties XBRL-berichten leesbaar maken. Zo draagt Logius bij aan een nog efficiëntere Digipoort.

6.6.2 Dienstverlening

De dienstverlening bestaat uit het via Internet beschikbaar stellen van de 'Berichtenspiegel' applicatie (elektronische dienstverlening) en het gedurende kantooruren bieden van gebruikersondersteuning aan klanten.

Logius levert een inspanningsverplichting voor het beschikbaar houden van de Berichtenspiegel.

Voor dit product wordt geen standby dienst uitgevoerd.

6.6.3 Prioriteiten & oplostijden

Prioriteitenmatrix Incidenten:

Prioriteit	Omschrijving Melding
Hoog	In de volgende gevallen wordt de prioriteit 'hoog' toegekend aan het Incident: Indien de gehele dienst niet beschikbaar is; Indien het Incident (een vermoedelijke) betrekking heeft op de beveiliging van de dienst.
Midden	In de volgende gevallen wordt de prioriteit 'midden' toegekend aan een Incident: Indien de dienst gedeeltelijk niet beschikbaar is.
Laag	Bij overige incidenten en vragen wordt de prioriteit 'laag' toegekend.

De prioriteit van een Melding wordt volgens onderstaande matrix ingedeeld.

Prioriteit	Productieomgeving	Acceptatieomgeving
Hoog	Prio 1	Prio 2
Midden	Prio 2	Prio 3
Laag	Prio 3	Prio 4

Indicator	Vorm	Norm
Oplostijd	tijd	Meldingen met Prio 1: Minimaal 90% van de Meldingen is binnen 4 uur opgelost; Meldingen met Prio 2: Minimaal 85% van de Meldingen is binnen 1 werkdag opgelost; Meldingen met Prio 3: Minimaal 85 % is binnen 2 werkdagen opgelost Meldingen met Prio 4: Minimaal 85% van de Meldingen is binnen 3 dagen opgelost.
Oplossen Meldingen gedurende:	tijd	Meldingen met Prio 1 t/m 4: werkdagen, 08:00 – 17:00 uur
Terugkoppeling aan Opdrachtgever tijdens afhandeling Melding	tijd / frequentie	Meldingen met Prio 1: binnen een uur (werkdagen, 08:00 – 17:00 uur) en daarna afstemming in overleg Overige Meldingen: geen rapportage.

In 'Oplostijd' is uitgezonderd de reactietijd die Opdrachtgever gebruikt om op een afmelding van een Melding te reageren.

6.6.4

Leveranciers

De leveranciers die een rol spelen bij Berichtenspiegel zijn:

leverancier	rol
Atos Origin (Groningen)	Applicatie- en infra-beheer

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.7 Digikoppeling

6.7.1 Werking

Digikoppeling is de 'interne postbode' voor de overheid. Digikoppeling bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties. Als deze standaarden worden geïmplementeerd in software van organisaties, dan kunnen deze eenvoudig digitaal berichten uitwisselen met collega-overheidsorganisaties. Via connectiviteit van Diginetwerk, internet of een andere verbinding. Digikoppeling is een NUP-bouwsteen.

6.7.2 Dienstverlening

De dienstverlening bestaat uit de elektronische dienstverlening (de Compliance voorziening, Serviceregister en Digimelding applicatie die via Internet wordt ontsloten naar de gebruikers) en de gebruikers-ondersteuning aan klanten (door het Servicecentrum).

Zodra er sprake is van een (dreigende) verstoring van de hieronder beschreven dienstverlening, is er sprake van een incident.

Eigenschappen van de elektronische dienstverlening voor de klant ¹⁵zijn:

Performance indicatoren voor openstellingswindow		
Soort afspraak	Norm	Minimaal te realiseren
Beschikbaarheid van de Digikoppeling Compliance voorziening	24 uur per dag, 7 dagen per week, alle dagen van het jaar	99,5 % beschikbaar
Beschikbaarheid van Digikoppeling Service Register	24 uur per dag, 7 dagen per week, alle dagen van het jaar	99,5 % beschikbaar
Beschikbaarheid van Digimelding	24 uur per dag, 7 dagen per week, alle dagen van het jaar	99,5 % beschikbaar

Prestatie-indicatoren voor onderhoudswindow	
	Norm
Structureel gepland onderhoud m.b.t. diensten en onderhoud m.b.t. de technische installaties	Maximaal 1 keer per maand, gedurende maximaal 6 uur (van 0:00 tot 6:00 van zondag nacht op maandag ochtend).

Performance Indicator voor capaciteit en performance		
Soort afspraak	Norm	Minimaal te realiseren
Capaciteit	Een bericht per seconde	99,5%
Performance	Antwoord binnen 3 seconde	99,5%

¹⁵ Uit SNO Digikoppeling en Digimelding (Publicatieplein, 15-01-2010)

Eigenschappen van de gebruikersondersteuning voor de klant zijn:

Performance Indicatoren voor servicewindow	
Beschikbaarheid	Norm
Ondersteuning bij het melden van Incidenten	Werkdagen van 8.00 uur tot 17.00 uur.
Ondersteuning bij het melden van klachten en het stellen van vragen	Werkdagen van 8.00 uur tot 17.00 uur.
Ondersteunen bij het registreren van calamiteiten	24 uur per dag, 7 dagen per week, alle dagen van het jaar.

Voor dit product hoeft geen standby dienst te worden uitgevoerd.

6.7.3

Prioriteiten & oplostijden

Om op een juiste wijze om te gaan met de verschillen in aard en aantal bij de afhandeling van incidenten zijn de incidenten voor de klant als volgt geclassificeerd en geprioriteerd:

Prioriteit Hoog

1. de gehele dienstverlening of primaire functionaliteit van de dienstverlening is niet beschikbaar;
2. het incident heeft betrekking op de beveiliging van de dienstverlening.

Prioriteit Midden

1. secundaire functionaliteit van de dienstverlening is niet beschikbaar;

Prioriteit Laag

1. Overige situaties.

De prioriteit bepaalt de oplostijd van incidenten binnen het servicewindow voor de klant.

Performance Indicatoren voor oplossen Incidenten en terugkoppeling aan afnemer			
Prioriteit	Oplostijd	Terugkoppeling	Minimaal te realiseren
Hoog	6 uur	Na oplossing van incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost. Indien voorzienbaar is dat een Incident met prioriteit Hoog niet binnen 100% van de norm-oplostijd kan worden opgelost, wordt geëscaleerd.
Midden	12 uren	Na oplossing van incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost.
Laag	3 werkdagen	Na oplossing van incident aan melder	15% van het aantal incidenten wordt niet conform de norm opgelost.

6.7.4

Leveranciers

De leveranciers die een rol spelen bij Digikoppeling zijn:

leverancier	rol
Ordina	applicatiebeheerder
NXS	ICT Infrabeheerder

Zie paragraaf **8.3** voor de contactgegevens van de leveranciers.

6.8 Stelselcatalogus

6.8.1 *Werking*

Gebruikers van basisregistraties - zoals overheden en instellingen - moeten weten welke gegevens ze precies in handen hebben. De Stelselcatalogus is een online catalogus die de structuur van het stelsel van basisregistraties en de definities van soorten objecten, gegevens en berichten beschrijft. Met die informatie kunnen gebruikers gegevens uit de basisregistratie(s) makkelijk inpassen in hun eigen werkprocessen.

De definities in de Stelselcatalogus zijn overgenomen uit de verschillende basisregistraties. De beheerders van de basisregistraties onderhouden de definities zelf.

De Stelselcatalogus verschaft inzicht in de gegevenshuishouding van het Nederlandse stelsel van Basisregistraties. Het is daarmee een belangrijke bouwsteen voor de e-overheid.

6.8.2 *Dienstverlening*

Voor dit product hoeft geen standby dienst te worden uitgevoerd. Wel worden incidenten tijdens kantooruren opgelost.

6.8.3 *Prioriteiten & oplostijden*

Is gelijk aan Digikoppeling.

6.8.4 *Leveranciers*

Zijn gelijk aan Digikoppeling

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.9 Digimelding

6.9.1 *Werking*

Bij basisregistraties draait het om betrouwbaarheid en om juiste, actuele en eenduidige gegevens. De meeste gegevens staan goed in de basisregistraties. Maar er kan altijd iets misgaan. Daarom is er Digimelding. Via dit webportaal kan een ambtenaar die vermoedt dat gegevens niet kloppen, daarvan melding maken. Die melding komt automatisch bij de juiste instantie terecht. Zijn de gegevens inderdaad onjuist, dan worden ze aangepast.

Digimelding bevat een aantal functionaliteiten die hieronder in het kort worden beschreven.

- Terugmelden: het doorgeven van een vermoedelijk onjuist gegeven in een basisregistratie.
- Intrekken: een eerder gedane melding kan worden ingetrokken als later blijkt dat het gegeven toch juist is.
- Registreren: het vastleggen van (meta)gegevens voor de administratie van de meldingen.
- Administratie: het beschikbaar stellen van de administratieve gegevens voor zowel afnemer als de houder van de basisregistratie.
- Status bijhouden: het mogelijk maken dat een afnemer de status van een melding kan inzien.

6.9.2 *Dienstverlening*

De dienstverlening is gelijk aan die voor Digikoppeling. Zie paragraaf 6.7.2.

6.9.3 *Prioriteiten & oplostijden*

De prioriteiten en oplostijden zijn gelijk aan die voor Digikoppeling. Zie paragraaf 6.7.3.

6.9.4 *Leveranciers*

De leveranciers die een rol spelen bij Digimelding zijn:

leverancier	rol
Ordina	ICT Infra- en applicatiebeheerder

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

6.10 Inspectieruimte BRZO

6.10.1 Werking

De Inspectieruimte BRZO is een online inspectiedatabase. De Inspectieruimte stelt BRZO inspectieteams in staat om gezamenlijk een inspectie voor te bereiden en af te ronden. Iedere inspectiedeelneemer heeft vanaf de eigen werkplek toegang tot het inspectiedossier en kan hier informatie in opslaan.

Voor wie is het?

De Inspectieruimte BRZO is bestemd voor BRZO-toezichthouders, -coördinatoren, -managers en -ondersteuners. Zij hebben de volgende toegangsrechten:

- Regiocoördinatoren hebben wijzigrechten om inrichtingen te kunnen toevoegen en inspecties te kunnen aanmaken.
- BRZO-Inspecteurs -werkzaam bij maatlatorganisaties*- hebben wijzigrechten om inspecties voor te bereiden en resultaten te verwerken, en leesrechten op alle inrichtingeninformatie.
- BRZO-managers -werkzaam bij maatlatorganisaties*- hebben leesrechten zodat zij kwaliteitstoetsen kunnen uitvoeren.
- BRZO-ondersteunenden hebben dezelfde rechten als de regiocoördinatoren.
- Overige betrokken medewerkers van gemeenten of provincies, niet zijnde 'maatlatinspecteurs'*, hebben leesrechten op inrichting informatie en op inspecties die worden uitgevoerd binnen hun werkgebied.

6.10.2 Dienstverlening

Onderwerp	Service level afspraak	Opmerkingen
Beschikbaarheid Prio hoog	Werkdagen 08:00 – 18:00	
Beschikbaarheid Prio midden	Werkdagen 08:00 – 18:00	
Beschikbaarheid Prio laag	Werkdagen 08:00 – 18:00	
Service verzoeken	Werkdagen 08:00 – 18:00	
Registratie van meldingen	100% registreren	Zowel Meldingen van Opdrachtgever als Opdrachtnemer

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met de Terugkoppeltijd en servicedesk van Opdrachtnemer.

Geldigend voor alle omgeving(en)					
Prestatie indicator incidentbeheer - terugkoppeltijd				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.1	Melding per telefoon	aantal %	80 % binnen 20 seconden	Nee	

			een deskmedewerker aan de telefoon, overige 20% binnen 2 minuten		
PI 1.2	Melding per E-mail	aantal %	80% binnen 15 min na E-mail ontvangst ticketnummer retour overige 20% binnen 1 uur	Nee	
PI 1.3	Hoeveelheid meldingen	aantal	Registratie van alle meldingen	Ja	Maand

Opdrachtnemer doet eenmaal per maand een rapportage van de kwaliteit van de servicedesk. Indien Opdrachtgever tussentijds een verminderde performance van de servicedesk vermoedt, zal Opdrachtgever dit in het SNR overleg ter sprake brengen. Daartoe verzocht, zal Opdrachtnemer verslag doen van de onderstaande indicatoren.

Incidenten

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met het oplossen van Incidenten door Opdrachtnemer:

Productieomgeving					
Prestatie indicator incidentbeheer - oplostijd				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.4	Incident Prio hoog	aantal %	90% binnen 8 uur opgelost 95% binnen 16 uur opgelost	Ja	maand
PI 1.5	Incident Prio midden	aantal %	90% binnen 16 uur opgelost 95% binnen 40 uur opgelost	Ja	maand
PI 1.6	Incident Prio laag	aantal %	90% binnen 40 uur opgelost 95% binnen 80 uur opgelost	Ja	maand

Serviceverzoeken

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met afhandelen van Serviceverzoeken door Opdrachtnemer.

Geldend voor alle omgeving(en)					
Prestatie indicator afhandeltijd serviceverzoeken				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.9	Afhandeling standaard service verzoeken	aantal %	90% binnen overeengekomen tijd	Ja	Maand
PI 1.10	Afhandeling niet stnd. Serviceverzoeken	Aantal %	90% binnen overeengekomen tijd	Ja	Maand

6.10.3

Prioriteiten & oplostijden

Voor Incidenten met betrekking tot de **Productieomgeving** is de volgende prioriteitenmatrix van toepassing, (indien een van de zaken onder een Prioriteit optreedt, zal het incident in overeenstemming met deze prioriteit worden geregistreerd en behandeld):

	Prioriteit		
	Hoog	Midden	Laag
Verkrijgen toegang:			
Website			
Werkt niet meer voor:	> 1 gebruiker	1 gebruiker	
Performance wordt niet gehaald	> 5 minuten	1 - 5 minuten	< 1 minuut
Beheermodule			
Werkt niet meer voor:	> 1 beheerder		1 beheerder
Performance wordt niet gehaald		≥ 30 minuten	< 30 minuten
Connectiviteit met bronleverancier			
Werkt niet meer voor:		> 1 bronleverancier	1 bronleverancier
Security incident			
Aanval ¹⁶	alle Incidenten		
Door GOVCERT.NL ¹⁷ aangegeven risico	hoog		medium en laag
Calamiteit			
	door Opdrachtgever bepaald	door Opdrachtgever bepaald	door Opdrachtgever bepaald
Overige incidenten			
			allemaal

Een Melding wordt door Opdrachtgever op de volgende manier aangemeld

¹⁶ Met een aanval wordt (het vermoeden van) een aanval van buitenaf bedoeld bijvoorbeeld een (Distributed) Denial-of-Service aanval.

¹⁷ GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid en ondersteunt overheidsorganisaties in ICT- en informatiebeveiliging met diensten als preventie, waarschuwing, advisering, kennisdeling en monitoring.

bij de servicedesk van Opdrachtnemer:

Type Melding	Prioriteit	Manier van melden door Opdrachtgever
Incident	Hoog	Eerst telefonisch en vervolgens bevestigen per email
	Midden	Per email
	Laag	Per email
Serviceverzoek		Per email

Opdrachtnemer informeert Opdrachtgever over de status van de door Opdrachtgever aan Opdrachtnemer gedane Meldingen en de door Opdrachtnemer geconstateerde Incidenten volgens volgende tabellen:

Productieomgeving¹⁸:

Type Melding	Prioriteit	Eerste Informatie moment	Volgende informatie moment	Support-uren
Incident	Hoog	Binnen 2 uur nadat Incident is geconstateerd / aangemeld	Iedere 2 uur totdat Incident is opgelost	Werkdagen van 08:00-18:00, aangemeld voor 18:00, dan verruimde openstelling tot 23:00
	Midden	Binnen 2 uur nadat Incident is geconstateerd / aangemeld	Aan het einde van iedere werkdag	Werkdagen van 08:00-18:00
	Laag	Binnen 4 uur nadat Incident is geconstateerd / aangemeld	Aan het einde van iedere Werkweek, of aan het eind van iedere werkdag bij overschrijding	Werkdagen van 08:00-18:00
Serviceverzoek		Zie DAP	Zie DAP	Zie DAP

6.10.4

Leveranciers

De leveranciers die een rol spelen bij Inspectieruimte BRZO zijn:

leverancier	rol
Ordina	Applicatiebeheerder en hosting

Zie paragraaf 8.3 voor de contactgegevens van de leveranciers.

¹⁸ Dienstverlening niveau conform de Ordina norm is voor de productieomgeving qua Applicatiebeheer "Zilver" en qua Technisch beheer "Zilver".

6.11 Manifestgroep

6.11.1 Werking

De Manifestgroep is een initiatief van twaalf uitvoeringsinstellingen van de Nederlandse overheid (o.a. Belastingdienst, UWV, SVB, DUO, IND). Zij willen burgers en bedrijven alle overheidsbrede informatie en diensten aanbieden die relevant is voor hun vraag en/of situatie. Belangrijke aspecten hierbij zijn vraagsturing (vanuit life-events en behoeften) en het op maat aanbieden van een samenhangende relevante combinatie van producten en diensten.

De bezoeker krijgt op de genoemde portals informatie-op-maat die past bij de persoonlijke informatie-behoefte. Na het beantwoorden van enkele vragen krijgt de bezoeker een gericht overzicht van relevante informatie en diensten die belangrijk zijn. De portals maken het de bezoeker makkelijk: minder zoeken op internet, snel een helder overzicht door de gecombineerde informatie en zekerheid over de relevantie van de onderwerpen.

De portals zijn ontwikkeld door Be Informed en worden via hen gehost bij Betagraphics. Er wordt gebruik gemaakt van Hippo als content management systeem.

Hierbij wordt gebruik gemaakt van onderstaande portalen.

<http://onderwijsbijverdienen.overheid.nl>
<http://vertreknaarhetbuitenland.overheid.nl>
<http://overlijden-overheid.nl>
<http://www.newtoholland.nl>

6.11.2 Dienstverlening

Vanaf 17 januari 2011 doet Logius het beheer. (geen stand-by)

De dienstverlening bestaat uit de elektronische dienstverlening (de Manifestgroep portalen, die via Internet worden ontsloten naar de eindgebruikers) en de gebruikersondersteuning aan burgers (door het Servicecentrum) en klanten (door Tactisch beheer functioneel beheer). Klant heeft de mogelijkheid om via het Servicecentrum een Serviceaanvraag te doen voor het aanmaken van nieuwe gebruikers m.b.t. het contentbeheer. Deze gebruikers zullen belast zijn met het beheren van de aan hun toegekende content op een van de vier portals. Hiervoor heeft Tactisch beheer de beschikking over een webbased applicatie waarmee ingelogd kan worden op het CMS.

<http://87.249.114.169>

Een uitgebreide handleiding is te vinden op

I:\Logius\Service management\Manifestgroep\3_Beheerhandleiding\Hippo
CMSWerkinstructie gebruik Hippo 6 CMS Manifest Groep.doc

Zodra er sprake is van een (dreigende) verstoring van de hieronder beschreven dienstverlening, is er sprake van een incident.

Eigenschappen van de elektronische dienstverlening zijn:

Performance Indicatoren voor Openstellingswindow		
Soort afspraak	Norm	Minimaal te realiseren
Beschikbaarheid van de dienst voor burgers (productieomgeving)	De productieomgeving van de Manifestgroep portalen is 7*24 uur, alle dagen van het jaar, beschikbaar voor: Het verstrekken van informatie voor burgers;	Best Effort.
Beschikbaarheid van de DigiD website: openstelling van de dienst (productie)	De productieomgeving van de Manifestgroep portalen is 7*24 uur, alle dagen van het jaar, beschikbaar.	Best Effort.
Beschikbaarheid van de dienst voor klanten (productieomgeving)	De productieomgeving van de Manifestgroep portalen is 7*24 uur, alle dagen van het jaar, beschikbaar voor een operationele klant.	Best Effort.

Performance Indicatoren voor Onderhoudswindow	
	Norm
Soort afspraak	Productieomgeving
Structureel gepland onderhoud m.b.t. diensten	1 maal per maand. Iedere 2 ^e maandag van de maand van 0:00 tot 06:00 en uitsluitend na overleg met Opdrachtgever. Voor security updates kan uitsluitend in overleg met Opdrachtgever een uitzondering worden gemaakt.
Onderhoud m.b.t. de technische installaties	Maximaal 4 keer per jaar, gedurende maximaal 4 uur.

Eigenschappen van de gebruikersondersteuning zijn:

Performance Indicatoren voor servicewindow	
Beschikbaarheid	Norm
	Productie omgeving
1 ^e -lijns ondersteuning voor het melden van incidenten door burgers.	Werkdagen van 8:00 uur tot 17:00 uur.
1 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door burgers.	Werkdagen van 8.00 uur tot 17.00 uur.
2 ^e -lijns ondersteuning voor het melden van incidenten door klanten en leveranciers.	Werkdagen van 8.00 uur tot 17.00 uur.
2 ^e -lijns ondersteuning voor het melden van klachten en het stellen van vragen door klanten en leveranciers.	Werkdagen van 8.00 uur tot 17.00 uur.

2 ^e -lijns ondersteuning voor het melden van calamiteiten.	Werkdagen van 8.00 uur tot 17.00 uur.
---	---------------------------------------

6.11.3 Classificatie en prioritering van de incidenten

Om op een juiste wijze om te gaan met de verschillen in aard en aantal bij de afhandeling van incidenten zijn de incidenten als volgt geclassificeerd en geprioriteerd:

Manifestgroep portalen productieomgeving:

	Prioriteit		
	Hoog	Midden	Laag
Manifestgroep portalen			
	Defects die de beschikbaarheid en functionaliteit van de applicatie verstoren.	Defects die in overleg met de Opdrachtgever belangrijker of gelijk belangrijk zijn dan de andere openstaande defects.	Defects die in overleg met de Opdrachtgever minder belangrijk zijn dan de andere openstaande defects.
Aanval ¹⁹	alle incidenten		
Door GOVCERT.NL ²⁰ aangegeven risico	hoog		medium en laag
Calamiteit²¹			
	Opdrachtgever bepaald	Opdrachtgever bepaald	Opdrachtgever bepaald
Overige incidenten²²			
	n.v.t.	n.v.t.	allemaal

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met de Terugkoppeltijd en servicedesk van Opdrachtnemer.

Geldend voor alle omgeving(en) voor Manifestgroep meldingen (geen burgervragen)					
Prestatie indicator				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
Hoog	Melding per telefoon	aantal %	95 % binnen 10 min een deskmedewerker aan de telefoon	Ja	maand
Midden	Melding per E-mail	aantal %	95% binnen 1 uur na E-mail ontvangst ticketnummer retour	Ja	maand
laag	Hoeveelheid meldingen	aantal	Registratie van alle meldingen	Ja	maand

Geldend voor burgervragen				
Prestatie indicator			Rapportage	
Omschrijving	Vorm	Norm	Ja/Nee	Interval
Meldingen gedaan door burger per mail	aantal	Registratie van alle meldingen binnen Clientèle en doorsturen naar landelijk aanspreekpunt Manifestgroep.	Ja	maand

6.11.4

Betrokken leveranciers

De leveranciers die een rol spelen bij de Manifestgroep portalen zijn:

Leverancier	Rol
Be Informed	Applicatiebeheer
Beta Graphics	Infrastructuur, webhosting

6.11.5

Prioriteiten & oplostijden

Niet van toepassing tijdens stand-by dienst. (**Geen stand-by**)

6.11.6

Leveranciers

Leverancier	Rol
Be Informed	Applicatiebeheer
Beta Graphics	Hosting, Infra

6.12 Inspectieview bedrijven

6.12.1 *Werking*

Inspectieview Bedrijven is in opdracht van de Arbeidsinspectie (AI) door het ICTU programma e-inspecties ontwikkeld. Aan Inspectieview Bedrijven is het bronsysteem (i-net) van de AI gekoppeld waardoor AI inspectiegegevens real-time bevraagd kunnen worden.

Inspectieview Bedrijven is een digitaal dossier wat tot doel heeft het delen van informatie tussen de toezichthouders van inspectiediensten eenvoudiger te maken.

Doelgroep van Inspectieview Bedrijven zijn de medewerkers van Rijksinspecties, gemeenten, provincies en andere organen met een wettelijke inspectietaak.

Inspectieview bedrijven kent de volgende functionaliteiten:

- Aanmeldfaciliteit: geautoriseerde toegang tot de voorziening;
- Zoeken: presentatieapplicatie;
- Samenvoegen: dienstenapplicatie;
- Documentatiegeneratie: samengesteld document;
- Informatie over de applicatie.

6.12.2 *Dienstverlening*

Onderwerp	Service level afspraak	Opmerkingen
Beschikbaarheid Prio hoog	Werkdagen 08:00 – 18:00	
Beschikbaarheid Prio midden	Werkdagen 08:00 – 18:00	
Beschikbaarheid Prio laag	Werkdagen 08:00 – 18:00	
Service verzoeken	Werkdagen 08:00 – 18:00	
Registratie van meldingen	100% registreren	Zowel Meldingen van Opdrachtgever als Opdrachtnemer

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met de Terugkoppeltijd en servicedesk van Opdrachtnemer.

Geldend voor alle omgeving(en)					
Prestatie Indicator Incidentbeheer - terugkoppeltijd				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.1	Melding per telefoon	aantal %	80 % binnen 20 seconden een deskmedewerker aan de telefoon, overige 20% binnen 2 minuten	Nee	
PI 1.2	Melding per E-mail	aantal %	80% binnen 15 min na E-mail ontvangst ticketnummer retour overige 20% binnen 1 uur	Nee	
PI 1.3	Hoeveelheid meldingen	aantal	Registratie van alle meldingen	Ja	Maand

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met het oplossen van Incidenten door Opdrachtnemer:

Productieomgeving					
Prestatie Indicator Incidentbeheer - oplostijd				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.4	Incident Prio hoog	aantal %	90% binnen 8 uur opgelost 95% binnen 16 uur opgelost	Ja	maand
PI 1.5	Incident Prio midden	aantal %	90% binnen 16 uur opgelost 95% binnen 40 uur opgelost	Ja	maand
PI 1.6	Incident Prio laag	aantal %	90% binnen 40 uur opgelost 95% binnen 80 uur opgelost	Ja	maand

Serviceverzoeken

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met afhandelen van Serviceverzoeken door Opdrachtnemer.

Geldend voor alle omgeving(en)					
Prestatie Indicator afhandeltijd serviceverzoeken				Rapportage	
Nr	Omschrijving	Vorm	Norm	Ja/Nee	Interval
PI 1.9	Afhandeling standaard service	aantal %	90% binnen	Ja	Maand

	verzoeken		overeengekomen tijd		
PI 1.10	Afhandeling niet stnd. Serviceverzoeken	Aantal %	90% binnen overeengekomen tijd	Ja	Maand

6.12.3

Prioriteiten & oplostijden

Voor Incidenten met betrekking tot de **Productieomgeving** is de volgende prioriteitenmatrix van toepassing, (indien een van de zaken onder een Prioriteit optreedt, zal het incident in overeenstemming met deze prioriteit worden geregistreerd en behandeld):

	Prioriteit		
	Hoog	Midden	Laag
Verkrijgen toegang:			
Website			
Werkt niet meer voor:	> 1 gebruiker	1 gebruiker	
Performance wordt niet gehaald	> 5 minuten	1 - 5 minuten	< 1 minuut
Beheermodule			
Werkt niet meer voor:	> 1 beheerder		1 beheerder
Performance wordt niet gehaald		≥ 30 minuten	< 30 minuten
Connectiviteit met bronleverancier			
Werkt niet meer voor:		> 1 bronleverancier	1 bronleverancier
Security incident			
Aanval ²³	alle incidenten		
Door GOVCERT.NL ²⁴ aangegeven risico	hoog		medium en laag
Calamiteit			
	door Opdrachtgever bepaald	door Opdrachtgever bepaald	door Opdrachtgever bepaald

²³ Met een aanval wordt (het vermoeden van) een aanval van buitenaf bedoeld bijvoorbeeld een (Distributed) Denial-of-Service aanval.

²⁴ GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid en ondersteunt overheidsorganisaties in ICT- en informatiebeveiliging met diensten als preventie, waarschuwing, advisering, kennisdeling en monitoring.

Overige incidenten			
			allemaal

Een Melding wordt door Opdrachtgever op de volgende manier aangemeld bij de servicedesk van Opdrachtnemer:

Type Melding	Prioriteit	Manier van melden door Opdrachtgever
Incident	Hoog	Eerst telefonisch en vervolgens bevestigen per email
	Midden	Per email
	Laag	Per email
Serviceverzoek		Per email

Opdrachtnemer informeert Opdrachtgever over de status van de door Opdrachtgever aan Opdrachtnemer gedane Meldingen en de door Opdrachtnemer geconstateerde Incidenten volgens volgende tabellen:

Productieomgeving²⁵:

Type Melding	Prioriteit	Eerste informatie moment	Volgende informatie moment	Support-uren
Incident	Hoog	Binnen 2 uur nadat Incident is geconstateerd / aangemeld	Iedere 2 uur totdat Incident is opgelost	Werkdagen van 08:00-18:00, aangemeld voor 18:00, dan verruimde openstelling tot 23:00
	Midden	Binnen 2 uur nadat Incident is geconstateerd / aangemeld	Aan het einde van iedere werkdag	Werkdagen van 08:00-18:00
	Laag	Binnen 4 uur nadat Incident is geconstateerd / aangemeld	Aan het einde van iedere Werkweek, of aan het eind van iedere werkdag bij overschrijding	Werkdagen van 08:00-18:00
Serviceverzoek		Zie DAP	Zie DAP	Zie DAP

6.12.4

Leveranciers

De leveranciers die een rol spelen bij Inspectieview Bedrijven zijn:

²⁵ Dienstverlening niveau conform de Ordina norm is voor de productieomgeving qua Applicatiebeheer "Zilver" en qua Technisch beheer "Zilver".

leverancier	rol
Ordina	Applicatiebeheerder en hosting

Zie paragraaf **8.3** voor de contactgegevens van de leveranciers.

6.13 Zoekdienst

6.13.1

Werking

De zoekdienst is een initiatief van ICTU samen met een negental departementen. Het initiatief is gestart in 2005 en had als doel de gezamenlijke inkoop van zoekfunctionaliteit ten behoeve van de ontsluiting van publieksinformatie op het internet. Daarnaast bestond er de gezamenlijke ambitie een 'overheidsbrede zoekdienst' op te zetten die door en over organisatiegrenzen heen informatie ontsluit in een voor de gebruiker relevante context. In 2006 is er een overeenkomst gesloten met Be Value voor de realisatie en exploitatie van de zoekdienst, als gevolg van gunningbesluit in een Europese aanbesteding. Sinds medio 2006 is de zoekdienst in gebruik. De zoekdienst wordt beheerd en geëxploiteerd als een dienst.

Zoekdienst heeft functioneel gezien interfaces met :

- Dienstaanbieders (zie bedrijfsarchitectuur)
- Publiekscontacten (zie bedrijfsarchitectuur)
- Hulpcollecties en Kennismodellen

De informatiesystemen van de Dienstaanbieders en Publiekscontacten vormen geen onderdeel van Zoekdienst.

De volgende omgevingen worden voor Zoekdienst ingericht:

- De Ontwikkel-, Test- en Acceptatie-omgeving(en)
- De Productie-omgeving

6.13.2

Dienstverlening

Een Melding wordt door Opdrachtgever op de volgende manier aangemeld bij de servicedesk van Opdrachtnemer:

Service desk			
PI's	Normen		
Servicevenster	5x10 uur (8:00 uur - 18:00 uur)		
Service requests en incidentenstatusrapportage (Zie randvoorwaarde 7)		Prio 1 en 2	Overig
	De eerste 8 uur	Ieder uur één	Eén maal daags
	Na 8 uur	Eén maal daags	

In onderstaande tabel zijn de PI's voor de minimale Beschikbaarheid van de Technische Infrastructuur en de maximale oplostijden van incidenten in de productie-omgeving van Zoekdienst gedefinieerd.

Het prestatieniveau inzake de gebruikersondersteuning (Service requests) door Opdrachtnemer wordt gemeten door middel van de tijd waarin een vraag van een medewerker van Opdrachtgever en/of Dienstafnemer wordt beantwoord. Hiervoor gelden de volgende normen:

- Alle vragen worden direct in behandeling genomen;
- 80% van de vragen wordt binnen 15 minuten beantwoord;

- 90% van de vragen wordt binnen 2 uur beantwoord;
- 100% van de vragen wordt binnen 5 werkdagen beantwoord.

6.13.3

Prioriteiten & oplostijden

Voor Incidenten met betrekking tot de **Productieomgeving** is de volgende prioriteitenmatrix van toepassing, (indien een van de zaken onder een Prioriteit optreedt, zal het incident in overeenstemming met deze prioriteit worden geregistreerd en behandeld):

Prioriteiten Incidenten	
Prioriteit	Beschrijving prioriteit
Prio 1 - Hoog	<p>Zoekdienst/Informatiesysteem functioneert in het geheel niet. Uitval van een volledige website of webapplicatie.</p> <p>Een (ver)storing in Zoekdienst/Informatiesysteem die invloed heeft op de kwaliteit van Zoekdienst (juistheid, volledigheid, performance, veiligheid en degelijke) waardoor het Informatiesysteem onbruikbaar geworden is voor Opdrachtgever en/of een Dienstafnemer. Zoekdienst/Informatiesysteem genereert schadelijke gegevens voor Opdrachtgever, Dienstafnemer en/of gebruiker.</p> <p>Veiligheidsrisico's en beveiligingsincidenten ingediend door of in opdracht van Opdrachtgever, gedetecteerd door Opdrachtnemer en beveiligingsadviezen van GOVCERT.</p>
Prio 2 - Middel	<p>Zoekdienst/Informatiesysteem vertoont ernstig functionaliteitsverlies en/of (ver)storende tekortkomingen waardoor een (tijdkritisch) bedrijfsproces van Opdrachtgever en/of een Dienstafnemer ernstig wordt verstoord.</p> <p>Zoekdienst genereert ongewenste resultaten die niet schadelijk zijn voor Opdrachtgever, Dienstafnemer en/of gebruiker.</p>
Prio 3 - Laag	<p>Zoekdienst/Informatiesysteem vertoont (ver)storende tekortkomingen.</p> <p>Deze prioriteit kan alleen aan een Incident worden toegekend met goedkeuring van Opdrachtgever.</p>

Beschikbaarheid Front end Zoekdienst in productie-omgeving			
PI's		Normen	
Gegarandeerd beschikbaarheidsvenster		Front end (5x14)	
Beschikbaarheidsgarantie		99,0%	
Prioriteiten	Prio1	Prio2	Prio3
Maximale downtijd/TTR	3 uur	8 uur	40 uur
Detectietijd (90% garantie)	0,5 uur	0,5 uur	0,5 uur
Reactietijd (90% garantie)	1 uur	2 uur	8 uur
TBF 1.1	93 dagen		

TBF 1.2	31 dagen
TBF 2.1	31 dagen
TBF 2.2	14 dagen

Beschikbaarheid Back end Zoekdienst in productie-omgeving			
PI's	Normen		
Gegarandeerd beschikbaarheidsvenster	Back end (5x10)		
Beschikbaarheidsgarantie	98,6%		
Prioriteiten	Prio1	Prio2	Prio3
Maximale downtijd/TTR	3 uur	8 uur	40 uur
Detectietijd (90% garantie)	0,5 uur	0,5 uur	0,5 uur
Reactietijd (90% garantie)	1 uur	2 uur	8 uur
TBF 1.1	93 dagen		
TBF 1.2	31 dagen		
TBF 2.1	31 dagen		
TBF 2.2	14 dagen		

In onderstaande tabel zijn de PI's voor de minimale Beschikbaarheid en de maximale oplostijden van incidenten in de acceptatie-omgeving van Zoekdienst gedefinieerd.

Beschikbaarheid Zoekdienst in acceptatie-omgeving			
PI's	Normen		
Beschikbaarheidsgarantie	In overleg		
Prioriteiten	Prio1	Prio2	Prio3
Maximale downtijd/TTR	3 uur	8 uur	40 uur
Detectietijd (90% garantie)	0,5 uur	0,5 uur	0,5 uur
Reactietijd (90% garantie)	1 uur	2 uur	8 uur
TBF 1.1	93 dagen		
TBF 1.2	31 dagen		

TBF 2.1	31 dagen
TBF 2.2	14 dagen

6.13.4

Leveranciers

De leveranciers die een rol spelen bij de Zoekdienst zijn:

leverancier	rol
Cappgemini	Applicatiebeheerder en technischbeheer

Zie paragraaf **8.3** voor de contactgegevens van de leveranciers.

7 Beheermiddelen

7.1 Mobiele telefoon

7.1.1 *Tactisch beheer*

Tactisch beheer beschikt over twee mobiele telefoons voor de standby dienst met hetzelfde nummer (duo-SIM).

Let op: op enig moment mag telkens maar één toestel aan staan.

Het mobiele nummer is:

[REDACTED]

N.B. Dit nummer mag niet aan klanten worden gecommuniceerd, aangezien dit nummer kan wijzigen. Ook wordt hiermee voorkomen dat dit nummer onterecht wordt gebeld. Het nummer mag wel worden verstrekt aan de Logius leveranciers (selecte groep).

Buiten kantooruren (werkdagen, 08:00 – 17:00 uur) worden oproepen naar het telefoonnummer van het Logius Servicecentrum (0900-5554555) na een boodschap en korte pauze doorgeschakeld naar het mobiele toestel.

De standby servicebeheerder neemt in de week dat hij/zij dienst heeft de eerste mobiele telefoon mee. De servicebeheerder die een week later standby dienst heeft neemt de tweede mobiele telefoon mee. Als de eerst aangewezen standby servicebeheerder tijdens de standby dienst niet meer in staat is om de standby dienst te draaien wordt deze overgenomen door de backup. Dit geldt alleen in uiterste noodzaak.

N.B. De backup standby servicebeheerder zet alleen op aangeven van de eerst aangewezen standby servicebeheerder de tweede mobiele telefoon aan.

De mobiele telefoon wordt tijdens kantooruren aangezet voor het ontvangen van Watchmouse berichten (zie paragraaf 7.4).

Tactisch beheer is verantwoordelijk voor het beheer van contactgegevens (namen, nummers) die in de mobiele telefoons zijn opgeslagen. Elke standby telefoon beschikt over dezelfde contactgegevens.

7.1.2 *Servicecentrum*

Het Servicecentrum beschikt over één mobiele telefoon voor de standby dienst. Het mobiele nummer is:

[REDACTED]

Dit nummer kan worden gebruikt op werkdagen van 08:00 – 22:00 uur.

N.B. Dit nummer mag niet aan klanten worden gecommuniceerd, aangezien dit nummer kan wijzigen. Ook wordt hiermee voorkomen dat dit nummer onterecht wordt gebeld.

De Helpdesk (Cendris) beschikt over dit nummer.

7.1.3

MT-leden

Het MT van Logius beschikt over een eigen mobiele telefoon die voor de standby dienst wordt gebruikt. Dit mobiele nummer is:



N.B. Dit nummer mag niet aan klanten worden gecommuniceerd, aangezien dit nummer kan wijzigen. Ook wordt hiermee voorkomen dat dit nummer onterecht wordt gebeld.

Het mobiele toestel wordt door de MT-leden tussen elkaar uitgewisseld op basis van het standby rooster. Elk MT-lid dat voor een bepaalde week als standby is aangewezen zorgt ervoor dat hij/zij in het bezit is van de standby mobiele telefoon.

Als het eerst aangewezen MT-lid niet in staat is om de standby dienst te draaien wordt deze overgenomen door een collega MT-lid.

7.2

Laptop

7.2.1

Inrichting laptop

Elke standby Servicebeheer medewerker beschikt over een laptop met docking station waarmee op kantoor en thuis toegang kan worden verkregen tot:

- Internet
- Logius/ICTU Intranet
- I:-schijf (Logius documenten)
- Logius Exchange (mail, agenda, taken, etc.)
- Clientele (service support systeem)
- DigiD beheeromgevingen
- CMS DigiD.nl (contentbeheer)
- CMS Logius.nl (contentbeheer)
- MailPlus (e-mail/sms-voorziening)

De laptops zijn voorzien van:

- Geactiveerd BIOS wachtwoord (t.b.v. toegangsbeveiliging)
- Ethernet aansluiting (voor vaste netwerkaansluiting)
- Wifi (voor draadloze netwerkaansluiting, zelf te configureren)
- Muis
- Windows XP + Internet Explorer (ICTU standaard)
- MS Office 2003 (ICTU standaard)
- OpenOffice (ICTU standaard)
- MS Outlook 2003 (ICTU standaard)
- Clientele client (test, acceptatie, productie)
- OpenVPN (ICTU standaard, voor beveiligde Internetverbinding)
- Virusscanner (ICTU standaard)
- VNC (voor het op afstand 'overnemen' van de laptop)

De map met gebruikersprofielen is versleuteld. Hiermee wordt voorkomen dat bij diefstal van de laptop de gebruikersdocumenten op de harde schijf kunnen worden uitgelezen.

Het gebruikersprofiel en de mailstore (mailbox) staan lokaal (op de laptop). De laptop gebruikers hebben geen adminrechten.

De laptops worden technisch beheerd door ICTU I&A. Bij vragen of verstoringen kan contact worden opgenomen met de ICTU Servicedesk. Deze is tijdens kantooruren (werkdagen, 08:30 – 17:00 uur) bereikbaar op:

070-8887744

Installatie van additionele software wordt op verzoek (na goedkeuring) door ICTU Servicedesk uitgevoerd door de laptop op afstand over te nemen (middels VNC).

7.2.2 *Gebruik laptop op kantoor*

De laptop kan op kantoor worden gebruikt, eventueel in combinatie met een docking station, om aan te loggen op het DH24-domein. Hiermee kunnen alle Logius voorzieningen worden benaderd.

7.2.3 *Gebruik laptop thuis*

Alle Logius voorzieningen (Intranet, I:-schijf, Exchange, Clientele, DigiD beheeromgevingen) dienen te worden benaderd door met de laptop een VPN verbinding op te zetten.

De vaste/draadloze verbinding naar Internet dient door de standby medewerkers zelf te worden geconfigureerd.

7.3 **Beheeromgevingen**

7.3.1 *DigiD voor burger*

De applicatie DigiD Machtigen beschikt over aparte beheeromgevingen. Deze zijn toegankelijk middels de URLs:

Omgeving	URL
Beheer (productie)	
Munin (productie)	
Beheer (pre-productie 1)	
Beheer (pre-productie 2)	
Beheer (acceptatie 1)	
Beheer (acceptatie 2)	
Beheer (acceptatie 3)	
Munin (acceptatie)	

In de kantooromgeving (Apeldoorn, Den Haag) moet hiervoor de proxy (in de browser configuratie) worden uitgeschakeld.

In verband met een IP-restrictie zijn deze omgevingen uitsluitend te benaderen vanuit kantoor (Den Haag, Apeldoorn) of via de VPN-verbinding (met de laptop).

7.3.2 *DigiD voor bedrijven* <volgt>

7.4 Watchmouse

7.4.1 *Achtergrond*

Watchmouse (www.watchmouse.com) is een tool waarmee een bewaking wordt gedaan op de werking van DigiD en Digipoort (SOAP). De wijze van melding gebeurt middels één of meerdere van hierna beschreven sms-berichten op het stand-by toestel.

In de meeste gevallen zullen meerdere berichten worden verstuurd, dus van alle onderdelen één. Want vaak zal het zo zijn dat als de één het niet doet, de ander het ook niet doet. Maar het kan zijn dat er maar één bericht wordt verstuurd. Dan heeft alleen dat onderdeel een probleem. Zodra je een bericht ontvangt moet er contact opgenomen worden met de helpdesk van Atos.

N.B.1 In principe is Atos verantwoordelijk voor deze controle en wordt Tactisch beheer bij problemen gebeld door Atos. Het kan echter zijn dat Watchmouse problemen eerder constateert dan Atos.

N.B.2 Meldingen worden niet per sms gegeven op elke zondag vanaf 23:55 tot maandagochtend 06:05. Dit heeft te maken met het onderhoudswindow van DigiD. Door de inrichting van Watchmouse is gekozen om dit iedere week in te stellen ondanks dat het een maandelijks actie betreft.

7.4.2 *Website DigiD*

Indien er problemen zijn met de website van DigiD kan de volgende melding verstuurd worden:

```
ALERT! www.digid.nl: Not matched. De http-service op  
'www.digid.nl' werkt niet naar behoren sinds jjjj-mm-dd  
hh:mm:ss.
```

Indien het probleem weer is hersteld, wordt je daarover ook weer op de hoogte gebracht middels het volgende sms-bericht:

```
OKAY www.digid.nl. De http-service op 'www.digid.nl'  
werkt weer naar behoren.
```

7.4.3 *Authenticatieserver voor burgers*

Indien de authenticatieserver voor burgers niet bereikbaar is, wordt onderstaande melding verstuurd.

```
ALERT! as.digid.nl: Not matched. De https-service op  
'as.digid.nl' werkt niet naar behoren sinds jjjj-mm-dd  
hh:mm:ss.
```

Hierdoor zijn burgers niet in staat om via een afnemer een product middels DigiD te gebruiken.

Als de service weer is hersteld wordt je hierover bericht middels sms met de volgende tekst:

```
OKAY as.digid.nl. De https-service op 'as.digid.nl'  
werkt weer naar behoren.
```

7.4.4 *Authenticatieserver voor klanten*

Indien de authenticatieserver voor burgers niet bereikbaar is, wordt onderstaande melding verstuurd.

```
ALERT! was.digid.nl: Not matched. De https-service op  
'was.digid.nl' werkt niet naar behoren sinds jjjj-mm-dd  
hh:mm:ss.
```

Als deze melding wordt gegeven, kunnen afnemers zich niet melden bij DigiD en daardoor kunnen Burgers geen producten afnemen middels DigiD.

Als de service weer is hersteld wordt je hierover bericht middels sms met de volgende tekst:

```
OKAY was.digid.nl. De https-service op 'was.digid.nl'  
werkt weer naar behoren.
```

7.4.5 *Applicatieserver voor DigiD*

Indien de applicatieserver niet beschikbaar is, kunnen Burgers geen aanvragen, activeringen doen en ook 'mijn gegevens' is dan niet mogelijk. De volgende melding wordt via sms verstuurd.

```
ALERT! applicaties.digid.nl: Not matched. De https-  
service op 'applicaties.digid.nl' werkt niet naar  
behoren sinds jjjj-mm-dd hh:mm:ss.
```

Als de applicatieserver weer beschikbaar is wordt de volgende melding teruggekoppeld.

```
OKAY applicaties.digid.nl. De https-service op  
'applicaties.digid.nl' werkt weer naar behoren.
```

7.4.6 *DigiD voor bedrijven*

Indien deze server niet bereikbaar is, kunnen bedrijven niet authenticeren. De volgende melding wordt via sms verstuurd.

```
ALERT! bedrijven.digid.nl: Not matched. De https-service  
op 'bedrijven.digid.nl' werkt niet naar behoren sinds  
jjjj-mm-dd hh:mm:ss.
```

Als de server weer beschikbaar is wordt de volgende melding teruggekoppeld.

```
OKAY bedrijven.digid.nl. De https-service op  
'bedrijven.digid.nl' werkt weer naar behoren.
```

7.4.7 *Digipoort (SOAP)*

Indien Digipoort (SOAP) niet beschikbaar is wordt de volgende melding via sms verstuurd.

```
ALERT! PI protal productie: Timeout of monitor sequence:  
de script service op 'www.procesinfrastructuur' werkt  
niet naar behoren sinds jjjj-mm-dd hh:mm:ss.
```

Als Digipoort (SOAP) weer beschikbaar is wordt de volgende melding teruggekoppeld.

```
OKAY! PI protal productie: Timeout of monitor sequence:  
de script service op 'www.procesinfrastructuur' werkt  
weer sinds jjjj-mm-dd hh:mm:ss.
```

7.5

MailPlus

Met behulp van MailPlus (een product van Blinker, zie www.blinker.nl) kunnen grootschalig e-mail en/of sms-berichten worden verstuurd naar Logius medewerkers en externe contactpersonen. Het is een externe voorziening, zodat er geen afhankelijkheid bestaat van de Logius infrastructuur (mocht deze niet beschikbaar zijn). Toegang tot deze voorziening wordt verkregen via Internet. Wanneer er een mailing vanuit Mailplus is verstuurd wordt er ook een e-mail gestuurd naar servicecentrum.intern@Logius.nl met daarin de verstuurde e-mail en de betreffende doelgroep.

Raadpleeg bijlage A voor het gebruik van MailPlus.

In MailPlus worden op basis van klantgegevens in Clientele communicatiedoelgroepen aangemaakt. Deze groepen worden samengesteld op basis van de positie van de contactpersoon (Logius of extern), product waarover de contactpersoon geïnformeerd wenst te worden en de wijze (e-mail en/of sms) waarop deze geïnformeerd wenst te worden.

De doelgroepen worden op regelmatige basis ververst door een nieuwe import van klantcontacten.

MailPlus wordt beheerd door een functioneel beheerder van Tactisch beheer. Back-up is de adviseur binnendienst van Dienstverlening.

N.B.1 Deze voorziening is toegankelijk voor aangewezen servicebeheerders en senior medewerkers van het Servicecentrum.

7.5.1

Communicatie

Enkele tips over de communicatie via Mailplus:

1. datum en tijd staan al in de mail zelf, anders in tekst verwerken:
"Vanaf 11.33 vanochtend..."
2. telefoonnummer met spatie en kostenvermelding: 0900 5554 555 /
(10 ct p/m)
3. Geachte heer/mevrouw, (schuine streep)
4. lettergrootte 10pt
5. ~~opt-out-informatie toevoegen: Als u deze mail niet meer wilt~~
~~ontvangen, mail dan naar servicecentrum@logius.nl~~

Door de opzet van MailPlus zijn de communicatie per sms en communicatie per e-mail twee verschillende handelingen.

7.6

Handboek incident- en calamiteitenbeheer

Dit document dient als naslagwerk voor zowel incidentmanagement als calamiteitenbeheer.

7.7

Quick Reference kaart

Voor zowel incidentmanagement als calamiteitenbeheer is een Quick Reference kaart beschikbaar. Hierop staan de belangrijkste zaken (waaronder de relevante contactgegevens) voor de incidentmanagers, standby managers en Logius woordvoerder.

Elke standby medewerker dient een Quick Reference kaart bij zich te hebben als hij/zij standby dienst heeft.

Deze documenten worden beheerd door Tactisch beheer.

8 Contactgegevens

8.1 Logius

De contactgegevens van de relevante Logius medewerkers staan in de Quick Reference kaart voor Incidentbeheer en die voor calamiteitenbeheer.

Daarnaast zijn deze contactgegevens ook geregistreerd in Clientele en MailPlus.

8.2 Klanten

8.2.1 Belastingdienst

Tijdens een Digistorm periode wordt bij een incident met prio 2 of hoger van DigiD voor burgers de Belastingdienst worden ingelicht. In MailPlus zijn contactgegevens (mobiele nummers en e-mailadressen) ingevoerd, waarmee berichten kunnen worden verstuurd. Hieronder de overige contactgegevens.

contactpunt	telefoon	bijzonderheden
Servicedesk		Kantooruren
Berichtenverkeer		
Calamiteit:		
1. [REDACTED]	[REDACTED]	07.30 - 20.30 (ma - vr) 09.00 - 17.00 (zaterdag)
2. [REDACTED]	[REDACTED]	7 x 24 uur via MailPlus
Escalatie: Ketenmanager [REDACTED]	[REDACTED]	7 x 24 uur via MailPlus
Algemene Onderwerpen [REDACTED]	[REDACTED]	08:00 - 17:00 via MailPlus

8.2.2 Digipoort klanten

Hieronder de belangrijkste Digipoort klanten (overheidsdeelnemers) en bedrijfsdeelnemers. Contactgegevens van klanten bevinden zich ook in MailPlus.

Organisatie	Telefoon	Mobiel	rol
Belastingdienst - berichtendienst		[REDACTED]	Klant
Nationale Helpdesk		[REDACTED]	Klant
Douane - Standby 1			
Nationale Helpdesk Douane - Standby 2		[REDACTED]	Klant
Nationale Helpdesk Douane	[REDACTED]		Klant
LNV Helpdesk		[REDACTED]	Klant
CBS		[REDACTED]	Klant
UWV		[REDACTED]	Klant
KVK	[REDACTED]		Klant

Cargonaut			Hub
Dexx BVBA			Hub
Port Infolink			Hub

8.3

Leveranciers

De contactgegevens van leveranciers op operationeel niveau (voor Incidentmanagers) staan in de Quick Reference kaart voor incidentbeheer.

De contactgegevens van leveranciers op managementniveau (voor standby managers) staan in de Quick Reference kaart voor calamiteitenbeheer.

BIJLAGE A: Bekende fouten

DigiD voor burgers:

<i>Symptoom</i>	<i>Mogelijke oorza(a)k(en)</i>	<i>Actie</i>
verzenden van de sms-transactiecode lijkt niet te werken	Er is een probleem bij één specifieke provider	Verder is er een site van GoldenBytes waarop eventueel bekende verstoringen op vermeld staan. De site is: http://noc.alldata.nl/ .
	De koppeling tussen DigiD en GoldenBytes werkt niet	Atos kan vaststellen of de koppeling met GoldenBytes up-and-running is
	Er zijn problemen met de verzendfaciliteit	

