BIJLAGE 2: INZAGEREACTIES

Een conceptversie van dit rapport is, conform artikel 56 van de Rijkswet Onderzoeksraad voor veiligheid, voorgelegd aan de betrokken partijen. Deze partijen is gevraagd het rapport te controleren op feitelijke onjuistheden en eventuele omissies.

De meeste partijen hebben gebruik gemaakt van de gelegenheid te reageren. Het commentaar heeft in veel gevallen wel, maar in sommige gevallen niet geleid tot aanpassing van het rapport. De reacties die niet hebben geleid tot aanpassing van het rapport zijn opgenomen in een tabel, waarbij tevens is opgenomen waarom de reactie niet is verwerkt.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
1	Fox-IT B.V.	4.1	"Ook slaagde hij erin gebruik te maken van de sleutels waarmee deze certificaten digitaal onder-tekend moeten worden als bewijs van hun echtheid".	Het gebruik maken van private sleutels vond plaats in het kader van het genereren van vervalste digitale certificaten. De term "ook" kan vervangen worden door "voor dit doel" of woorden van gelijke strekking.	Het inzagecommentaar legt een verband tussen twee gebeurtenissen dat de Onderzoeksraad niet heeft onderzocht.
2	voorm. compliance officer DigiNotar B.V.	4.1	Toevoegen na "… fouten"	, waren dubbel of bij het onderzoeken van de hack door DigiNotar zelf gegenereerd	Het materiaal waarover de Onderzoeksraad voor dit gedeelte van het onderzoek beschikte, wijst dit niet uit.
3	voorm. compliance officer DigiNotar B.V.	4.1	Toevoegen zin	Slechts een beperkt aantal certificaten zijn ook daadwerkelijk naar buiten gebracht door de hacker.	Uit het onderzoeksmateriaal leidt de Onderzoeksraad af dat slechts van een gering aantal certificaten vast staat dat zij in omloop zijn gebracht. Dat betekent niet dat er niet méér vervalste certificaten in omloop kunnen zijn gebracht. De tekst is op dit punt verduidelijkt.
4	Fox-IT B.V.	4.1	"Onduidelijk blijft of en van hoeveel van deze bruikbare certificaten ook daad-werkelijk misbruik is gemaakt […] Wel is aan-nemelijk dat dit intensief geprobeerd is […] Dit kan worden afgeleid uit het feit dat veel van de vervalste certificaten zijn getoetst aan de OCSP-whitelist. […] Of de pogingen succesvol waren […] behoorde niet tot de scope van het onderzoek".	De scope van het onderzoek, die in de laatste zin van deze alinea wordt beperkt, omvat expliciet niet de conclusie die in de eerste zin van dezelfde alinea wordt getrokken. De conclusie van onder andere Fox-IT is dat er wel degelijk misbruik is gemaakt van het *. google.com certificaat in een Man in the Middle (MITM) aanval die zich voornamelijk richtte op gebruikers in Iran.	De Onderzoeksraad kan op grond van de beschikbare informatie niet constateren dat de "man in the middle"-aanval succesvol is geweest. Op basis van het inzage-commentaar is nu een scherper onderscheid gemaakt tussen pogingen tot misbruik en succesvol misbruik.
5	VASCO Data Security International, Inc.	4.1.1	… Netwerk mogelijk al op 1 juni 2011 …	Graag bronvermelding toevoegen	Deze informatie ontleent de Onderzoeksraad aan vertrouwelijke informatie. De tekst is op dit punt verduidelijkt.
6	voorm. compliance officer DigiNotar B.V.	4.1.1	Detecteren	Voorkomen	Getuige de gebeurtenissen bij DigiNotar is het "intrusion prevention system" er niet in geslaagd de inbraak te voorkomen. Wel is de tekst naar aanleiding van het inzagecommentaar verduidelijkt.
7	voorm. compliance officer DigiNotar B.V.	4.1.1	Toevoegen	Onvolledig Er wordt niet ingegaan over de rol die de overheid (bijvoorbeeld AIVD, GOVERT en Logius) speelt bij een grootschalige aanval van een vreemde mogendheid. In het fysieke domein kan de burger of onderneming rekenen op bescherming van het leger. Bij het trekken van de parallel naar het Internet zou de overheid in deze situaties een actievere rol moeten spelen. In de DigiNotar casus heeft de overheid alleen geïnformeerd.	Het inzagecommentaar wijst niet op feitelijke onjuistheden
8	VASCO Data Security International, Inc.	4.1.1	… zwakheden benut in de webbrowser systemen, wat mogelijk was …	Zie Fox-IT rapport	Het inzagecommentaar doet geen voorstel tot aanpassing of correctie.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
9	voorm. compliance officer DigiNotar B.V.	4.1.1	.. relatief korte …	Het beleid van DigiNotar was gericht op het gebruiken van sterke wachtwoorden. Over de kwalificatie van dit specifieke wachtwoord kan het nodige over worden bediscussieerd en voorstel is om deze kwalificatie achterwege te laten. De indruk moet niet worden gewekt dat een paar karakters toevoegen aan het wachtwoord, de hack had kunnen voorkomen.	De Onderzoeksraad deelt de opvatting die in de laatste regel van dit inzagecommentaar tot uitdrukking komt, maar is niet van mening dat zijn rapport iets dergelijks impliceert.
10	voorm. compliance officer DigiNotar B.V.	4.1.1	Ten vijfde … ondertekenen	Onjuist en suggestief. In de eerste plaats wordt geen afzonderlijke geheime sleutel gebruik voor de zogenaamde intrekkingslijsten. Ten tweede is het beschikbaar zijn van de geheime mastersleutel om certificaten te ondertekenen als een “omstandigheid die er toe heeft bijgedragen” ook onjuist aangezien de mastersleutel actief moet zijn om de normale CA taken te kunnen uitvoeren. Om deze redenen waren vergaande maatregelen genomen om deze mastersleutel te beschermen. DigiNotar maakte gebruik van software en een zogenaamde HSM van de marktleiders op dit gebied wereldwijd. Deze software en HSM waren ook voorzien van alle mogelijk relevante product certificaties. Als onderdeel van de beveiliging van deze mastersleutel werd gebruik gemaakt van meerdere smartcards in combinatie met strikte functiescheiding. De hacker is blijkbaar in staat geweest om een zeer gerenommeerd systeem te hacken. Hiertoe is specifiek voor DigiNotar door de hacker een zogenaamde exploit gebouwd.	Dit inzagecommentaar maakt duidelijk dat de inbreker erin is geslaagd de master-sleutel die op het netwerk aanwezig was om intrekkingslijsten te ondertekenen, op de één of andere manier aan te wenden voor het ondertekenen van vervalste certificaten. Dit is in overeenstemming met de rapporttekst.
11	voorm. compliance officer DigiNotar B.V.	4.1.1.	Gehele alinea	Onvolledig Er wordt geen melding gemaakt dat de waarschuwing tevens een geruststelling inhield namelijk dat de inschatting van Logius was dat deze aanvallen ‘niet op Nederland waren gericht’.	De bedoelde waarschuwing, in het bezit van de Onderzoeksraad, kan redelijkerwijs niet worden opgevat als een geruststelling.
12	Fox-IT B.V.	4.1.3	“Dit betreft overigens een ander bedrijf dan het bedrijf dat de inbraak heeft gereconstrueerd”.	De formuleringen in het rapport van verwijzingen naar derden die een rol hebben gehad in de beveiliging van DigiNotar kunnen momenteel voor verwarring zorgen. Het “gespecialiseerde bedrijf dat onder andere zogenaamde penetratietests uitvoerde” heeft zich in eerste instantie ook bezig gehouden met de reconstructie van de inbraak.	De Onderzoeksraad acht dit inzagecommentaar niet relevant voor zijn duiding van de feiten.
13	OPTA	4.1.4	Het…plaatsvinden.	Onvoldoende onderbouwing om tot deze conclusie te komen. Het Fox-it rapport laat een ander beeld zien.	DigiNotar B.V. deed, onder meer naar het oordeel van de auditerende instelling, wat nodig was om zijn certificaatdienstverlening zo veilig mogelijk te doen plaatsvinden. Ten aanzien van de beveiliging van het bedrijfsnetwerk constateert de Onderzoeksraad dat DigiNotar de voor het bedrijf geldende regels niet volledig heeft nageleefd.
14	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	4.1.4	Het bedrijf DigiNotar spande zich niet voldoende in ……	De nu opgenomen tekst is in tegenstelling met het op de vorige pagina gedane feitenrelaas. Hieruit blijkt dat DigiNotar aan zeer basale veiligheidseisen waaraan elke professioneel bedrijf zich, ongeacht welke dienstverlening zij uitvoert, te houden heeft, niet voldaan heeft.	Zie inzagereactie #13

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
15	voorm. compliance officer DigiNotar B.V.	4.1.4	Toch … certificaten.	Het is onduidelijk op welke wijze deze zin moet worden geduid. De uiteindelijke inbraak die gekwalificeerd kan worden als een 'advanced persistent threat' heeft kunnen plaats vinden door een complex aan factoren, veel kennis en deskundigheid en een ongelukkige samen-loop van omstandigheden zeker gezien de norm interpretatie van een jaar geleden.	De Onderzoeksraad is van oordeel van de bedoelde zin duidelijk is.
16	VASCO Data Security International, Inc.	4.1.4	… niet volledig heeft nageleefd en/of de richtlijnen voor de beveiliging van computer-systemen voor gekwalifi-ceerde certificatiedienst-verlening niet volledig zijn.	Tweede argumentatie wordt later in de conclusies bevestigd.	De Onderzoeksraad neemt deze reactie voor kennisgeving aan.
17	Logius	4.1.4	Het vergt….toe te passen.	Dit suggereert dat de CSP er alleen voor staat om te komen tot adequaat veiligheids-management. Echter de auditor moet zich een oordeel vormen of de beheersmaat-regelen (nadere invulling van de norm) die de CSP neemt wel tegemoet komen aan de controle doelstelling (ETSI norm). Pas als de auditor hier het oordeel over geeft dat alle beheersmaatregelen volledig en juist zijn leidt dit tot een goedkeurende verklaring. Vanzelfsprekend zijn er verschillende beheersmaatregelen mogelijk waarmee de norm volledig en juist kunnen worden geadresseerd.	De Onderzoeksraad deelt deze mening niet.
18	Logius	4.1.4	De Onderzoeksraad … gedaan	Op basis van (genoemde) feiten uit het FOX-IT rapport blijkt dat Diginotar aan zeer basale veiligheidseisen waaraan elke professioneel bedrijf zich, ongeacht welke dienstverlening zij uitvoert, te houden heeft, niet voldaan heeft .	Zie inzagereactie #13
19	voorm. compliance officer DigiNotar B.V.	4.1.4	Hierdoor – delen	Deels onterecht. De OPTA heeft wegens het ingevulde selfassessment in 2003 volledig inzicht gekregen in alle getroffen detailmaatregelen. Dit is echter niet meer geupdate nadien.	De rapporttekst heeft op dit punt betrekking op de auditverklaring, en niet op eventuele verantwoordingen door DigiNotar zelf.
20	Logius	4.1.5	De auditor….aan toetsen.	Gezien de conclusies is hoor-wederhoor met de Certificerende Instellingen (BSI Management en PwC) hier op zijn plaats. Bij de audit wordt er b.v. gebruik gemaakt van een Statement of Applicability en ISO/IEC 17021 heeft betrekking op de wijze waarop de auditor tot zijn oordeel komt.	PwC Certification B.V. is de gelegenheid geboden te reageren.
21	OPTA	4.2.1	De…worden	Waar baseert de onderzoeksraad deze vaststelling op? Meer voor de hand ligt om de uitgifte van certificaten te stoppen totdat het volledig duidelijk was hoe de aanmaak van valse certificaten is geschied en er daarna voor te zorgen dat deze mogelijk niet meer bestaat.	De visie van de Onderzoeksraad voor Veiligheid vergt dat risico's zoveel als redelijkerwijs mogelijk is worden beheerst. Het in deze passage beschreven handelen van DigiNotar komt de Onderzoeksraad, wanneer kennis van latere ontwikkelingen buiten beschouwing gelaten wordt, redelijk voor.
22	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	4.2.2	Tekstvoorstel: "De onderzoeksraad kan niet meegaan in de gemaakte inschatting van Vasco en DigiNotar over het al dan niet melden van het incident bij opta en PA/ Logius. Daarbij merkt de onderzoeksraad verder het volgende op. Certificatie-dienstverlening…zijn meldplicht conform de strekking van de overeen-komst interpreteert en andere…op de hoogte stelt wanneer een melding van belang is voor de ontvanger…	In de voorgaande paragraaf wordt gesproken over de eigen afweging die DigiNotar gemaakt heeft om niet te melden. Uit het verloop van het incident, en andere onderzoeken zoals FOX-IT blijkt echter duidelijk dat het beheerssysteem van DigiNotar zodanig was ingericht dat toegang tot de andere omgevingen(zoals gekwalifi-ceerde en PKI overheidcertificaten) ook toen al niet uit te sluiten was. DigiNotar heeft echter besloten om niet te melden. Praktijk in de sector is dat incidenten publiekelijk worden gemeld en dat men afkoppelt van internet om te onderzoeken wat er aan de hand is. Daarbij wordt geen onderscheid gemaakt naar gekwalificeerde of ongekwalificeerde certificaten.	Voortschrijdend inzicht heeft de Onderzoeksraad ertoe gebracht in dezen geen standpunt in te nemen. De Onderzoeksraad treedt niet in de vraag of in de onderhavige situatie melden vanuit juridisch oogpunt verplicht was. Vanuit het grote belang van veilige certificaatdienst-verlening bezien, acht de Onderzoeksraad het echter noodzakelijk dat bedrijven in een dergelijke situatie incidenten aan relevante partijen melden. Dit geldt ook in de situatie dat het bedrijf in de veronderstelling vekeerde dat de problemen waren opgelost. Alleen als dergelijke incidenten gemeld worden, kan immers door de sector van incidenten geleerd worden.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
23	OPTA	4.2.2	De…heeft	DigiNotar heeft besloten het incident niet te melden. Uit de feiten, zoals onder meer vastgesteld door FOX-IT, blijkt echter dat het systeem van DigiNotar zodanig was ingericht dat niet kon worden uitgesloten dat onbevoegde derden zich ook toegang hebben verschaft tot segmenten die werden gebruikt voor de productie van gekwalificeerde en PKI overheidcertificaten. De vraag of DigiNotar zijn meldplicht heeft geschonden kan hier dan ook niet zo stellig ontkennend worden beantwoord.	Zie inzagereactie #22
24	Ministerie van Veiligheid en Justitie	4.2.2	Tekstvoorstel: dat DigiNotar in formele zin haar wettelijke meldplicht niet zonder meer geschonden lijkt te hebben.	de eerdere paragraaf geeft de raad ook al aan dat er tevens sprake is van een contractuele meldplicht aangaande relevante incidenten. DigiNotar heeft de afweging gemaakt om zowel niet te melden op grond van de meldplichten in formele alsmede in contractuele zin.	Zie inzagereactie #22
25	Logius	4.2.2	De Onderzoeksraad…. geschonden heeft.	DigiNotar heeft naar onze mening wel haar meldplicht in formele zin geschonden. De Raad refereert in deze aan art. 4 lid 3 van het contract tussen BZK en DigiNotar. Echter in hetzelfde contract (art. 4 lid 7) staat dat "DigiNotar verplicht is om op basis van kennis, die te zijner beschikking staat of zou moeten staan op grond van bij hem bekende feiten en omstandigheden, of kennis die op grond van zijn specifieke expertise bij hem aanwezig is of zou moeten zijn, actief BZK te informeren over de risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening van BZK kunnen bedreigen of beïnvloeden." Tevens staat er in het contract (art. 2 lid 2) dat DigiNotar gebonden is aan het Programma van Eisen van PKIoverheid. Zij dient zich te allen tijde te houden aan de in dit document beschreven eisen. PvE (onderdeel 3: Certificate Policy [..] eis 5.7.1-2 stelt: "De CSP informeert de PA actief over de risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden." Deze eisen zijn b.v. niet gerelateerd aan een eventuele compromittering van de DigiNotar PKIoverheid CA's en brengen met zich mee dat DigiNotar de Policy Authority (PA) PKIoverheid op basis van de in het PvE gestelde eis weldegelijk op de hoogte had moeten stellen nadat de inbraak was geconstateerd te weten op 19 juli 2011. Dat de inbraak bij DigiNotar een bedreiging was voor de betrouwbaarheid van de dienstverlening en ook het imago van de PKI voor de overheid is duidelijk gebleken. Logius heeft in samenwerking met GovCert en later het NCSC de nodige inspanningen moeten verrichten om de betrouwbaarheid in PKIoverheid richting met name de softwareleveranciers, overheidspartijen en burgers in stand te houden. Hierbij wil Logius ook nadrukkelijk wijzen naar de aandacht van de pers omtrent deze kwestie en de aard van de berichtgeving daaromtrent. Logius is van mening dat indien DigiNotar op 19 juli 2012 Logius direct had geïnformeerd, deze situatie anders was gelopen en in ieder geval veel meer ruimte was gebleven om te zorgen dat het vertrouwen van derden niet zou worden geschaad in het PKIoverheid stelsel.	Zie inzagereactie #22

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
26	voorm. compliance officer DigiNotar B.V.	4.3.1	Wat … op te zeggen.	Toevoegen. Blijkbaar was Logius niet in staat om de technologie leveranciers gerust te stellen over de andere deelnemers van het PKI Overheid stelsel. Opmerkingen ontbreken om de verschillende kwaliteit van de technologie leveranciers om certificaten fijnmazig te blokkeren. Sommige hadden hiertoe uitgebreide functionaliteit terwijl sommige hierop te kort kwamen en blijkbaar kozen voor politieke druk.	De Onderzoeksraad heeft niet onderzocht welke overwegingen de softwarefabrikanten hadden om hun vertrouwen in PKIoverheid te heroverwegen.
27	voorm. compliance officer DigiNotar B.V.	4.3.1	Een gevolg … te functioneren.	Veel te verstrekkend. Door het simpelweg vervangen van een certificaat zou het DigiD systeem weer functioneren. Wellicht door onvoldoende kennis een te verstrekkende opmerking.	De tekst verwoordt een inschatting van Logius. Of deze inschatting feitelijk juist was, doet voor het betoog niet ter zake.
28	Belasting-dienst	4.3.1	Het woord aanvankelijk	Het gebruik van dit woord suggereert dat er nog iets na komt; dat vervolg wordt gemist	Paragraaf 4.3.3 behandelt het in het inzagecommentaar bedoelde ‘vervolg’: daar wordt geschetst hoe allengs bleek dat DigiNotar B.V. ook een cruciale partij voor de rijksoverheid was door hun betrokkenheid bij het leveren van BAPI-certificaten
29	VASCO Data Security International, Inc.	4.3.2	Het wees uit dat de inbreker diverse registra-ties in de logfiles van DigiNotar had gemanipu-leerd, waardoor de methode …	Zie Fox-IT rapport	Deze informatie ontleent de Onderzoeksraad aan vertrouwelijke geprekken. De tekst is op dit punt verduidelijkt.
30	Fox-IT B.V.	4.3.2	“maar aangezien […] niet door de inbraak getroffen was” “[…] zelfs al kon niet worden uitgesloten dat de server waarop de certificatiedienstverlening voor PKIoverheid plaats vond gecompromitteerd was, er was geen reëel risico dat frauduleuze PKIoverheid-certificaten in omloop waren”	Het staat vast dat de server waarop de certificatiedienstverlening voor PKIoverheid plaats vond gecompromitteerd was, in de zin dat de aanvaller zich de volledige toegang tot deze server had verschaft. De corresponderende private sleutel in de netHSM is in deze periode actief geweest blijkens de automatische generatie van een Certificate Revocation List (CRL). Gezien het feit dat de log-bestanden bovendien hun oorsprong vinden op de server die was gecompromitteerd, kan het niet worden uitgesloten dat de corresponderende private sleutel misbruikt had kunnen worden.	De Onderzoeksraad kan op grond van de beschikbare informatie niet constateren of de inbreker daadwerkelijk handelingen heeft uitgevoerd op de bedoelde server, maar kan evenmin uitsluiten dat dit het geval is geweest. De tekst is aangepast.
31	voorm. compliance officer DigiNotar B.V.	4.3.3		Toevoegen Door het handelen van de overheid en publicatie van een onjuist en onvolledig concept rapport heeft de OPTA vergaande maatregelen genomen. Hierdoor zijn een aantal partijen onevenredig zwaar getroffen. De OPTA heeft geforceerd certificaten laten intrekken terwijl op een juiste risico analyse de certificaten voor een bepaalde periode toch gebruik hadden kunnen worden en een veel geleidelijke migratie mogelijk was geweest.	Het inzagecommentaar reikt geen feiten aan die deze zienswijze ondersteunen. Los daarvan onthoudt de Onderzoeksraad zich van oordelen zoals het gevraagde, zolang deze geen inzicht bieden in de wijze waarop het onderzochte voorval zich ontwikkeld heeft.
32	voorm. compliance officer DigiNotar B.V.	4.3.3		Toevoegen De overheid heeft in de casus van DigiNotar vele conflicterende rollen vervuld. De overheid in zijn rol AIVD, nationale veiligheid, inkoper, gebruiker, toezichthouder en eigenaar van PKI Overheid leiden tot een complexe situatie.	Voor het inzicht in de gebeurtenissen, zoals door de Raad onderzocht, doet deze opmerking niet ter zake. Het maakt geen deel uit van het onderzoek door de Onderzoeksraad.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
33	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	4.4	Van het later ontstane gebrek hieraan is niet met zekerheid te zeggen of dat gerechtvaardigd was. Feit was wel dat de maat-schappelijke en overheids-dienstverlening op basis van de gebeurtenissen bij DigiNotar grote kans liep om ontwricht te worden.	De relatie tussen beide conclusies in deze opeenvolgende zinnen is onduidelijk: als het gebrek aan vertrouwen niet gerechtvaardigd zou zijn, dan was er ook geen kans op grote ontwrichtingen.	Het verloop van de gebeurtenissen rond DigiNotar B.V. laat een plotselinge vertrouwensomslag zien. Het vertrouwen dat partijen als Logius en OPTA in DigiNotar B.V. stelden voor het incident was onvoldoende geborgd door feitelijke toetsing. De Onderzoeksraad is van oordeel dat Logius en OPTA zich voorafgaand aan het incident meer betrokken hadden moeten tonen bij het bedrijf, en zich werkelijk hadden moeten overtuigen van de betrouwbaarheid van diens dienstverlening en de risico's die er waren. Als zij zelf goed zicht hadden gehad op de feitelijke situatie bij DigiNotar B.V. hadden zij de gebeurtenissen beter kunnen beoordelen en zouden ze minder overvallen zijn geweest.
34	OPTA	4.4	Voorafgaand…OPTA.	Van blind vertrouwen in Diginotar is geen sprake. OPTA baseerde zich op het onderzoek van de auditor, die Diginotar minimaal jaarlijks doorlichtte. Indien over door de auditor geconstateerde afwijkingen, of de wijze waarop deze zijn opgelost, twijfels bestonden, stelde OPTA daarover vragen bij de certificatiedienstverlener. Zo nodig werd ook aangekondigd dat de registratie zou worden beëindigd als bepaalde non-conformiteiten niet binnen een bepaalde termijn zouden worden opgelost.	De formulering is aangepast. De Onderzoeksraad blijft van mening dat OPTA en Logius, zich tezeer lieten leiden door het onderzoek van de auditerende instelling, en zelf te weinig activiteiten ontplooiden om te beoordelen of de kwaliteit van de certificatiedienstverlening door DigiNotar B.V. naar hun maatstaven toereikend was.
35	Logius	4.4	Als de..worden.	DigiNotar heeft naar onze mening wel haar meldplicht in formele zin geschonden. Zie argumentatie bij 4.2.2 bladzijde 42, regel 1 t/m 2 m.b.t. "De Onderzoeksraad … geschonden heeft".	Zie inzagereactie #22
36	Ministerie van Binnenlandse Zaken en Koninkrijksr-elaties	4.4	Als…mag worden. De inbraak op zich ..door het bedrijf. Wel wreekt zich in het vervolg de keuze die DigiNotar gemaakt heeft om OPTA en met name PA Logius niet op de hoogte te stellen. Wanneer immers op 29 augustus 2011 aan het licht komt dat…..	Het is gebruikelijk dat dit soort incidenten altijd gemeld wordt aan de toezichthouders, juist om het bestaande vertrouwen te bevestigen. Daarbij is het ook mores in deze sector dat incidenten publiekelijk worden gemeld (zie ook hierboven).	De Onderzoeksraad deelt de mening dat het melden van incidenten wenselijk is, zoals ook in het rapport tot uitdrukking wordt gebracht. Het inzagecommentaar reikt geen nadere feiten aan die de bewering onderbouwen dat het publiekelijk melden van incidenten in deze sector gebruikelijk is.
37	Logius	4.4	Het niet…meer baten.	Hier wordt niet belicht dat DigiNotar door haar eigen handelen zijnde het niet op 19 juli aan diverse stakeholders (overheid, softwareleveranciers) melden van de inbraak het onheil over haar zelf heeft afgeroepen. Dit geldt zeker internationaal waar de softwareleveranciers vrijwel per direct de commerciële tak van DigiNotar uit de browser hebben verwijderd omdat zij ook pas op 29-8-2012 door DigiNotar op de hoogte zijn gesteld. De communis opinio binnen de internet community is dat dit DigiNotar de das om heeft gedaan. I.t.t. het bedrijf Comodo dat b.v. wel tijdig een hack heeft gemeld. Zij worden nog steeds vertrouwd door de browserpartijen. Tevens heeft DigiNotar in de eerste week (29-8 t/m 2-9) van de crisis door het probleem met de registratie van de computersysteem-gebeurtenissen (zie blz. 45 regel 7 t/m 9 van het voorliggende rapport), onvoldoende of geen duidelijkheid kunnen geven over de volledige omvang van de hack. Het ontbreken van deze audit trail, met als gevolg te late, onjuiste en onvolledige communicatie, was mede fnuikend voor het vertrouwen in DigiNotar.	Dit inzagecommentaar verhoudt zich naar het oordeel van de Onderzoeksraad slecht tot de door Logius gevolgde handelwijze in de dagen tussen 29 augustus en 2 september. Als de vertrouwensbreuk met DigiNotar B.V. primair veroorzaakt zou zijn door het niet-melden van het bedrijf op 19 juli, dan had het in de rede gelegen dat Logius meteen op 29 augustus tot afsluiting was overgegaan, in plaats van het bedrijf in die week gelegenheid te bieden zich te revancheren.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
38	voorm. compliance officer DigiNotar B.V.	4.4	Zij – DigiNotar	Ongenuanceerd. Op operationeel niveau bestond bij Logius wel degelijk een indruk van de kennis en kunde van DigiNotar. Periodiek werd deelgenomen aan het overleg met PKI Overheid gecertificeerde CA's. In dit overleg werd specifiek gesproken over de situatie bij DigiNotar bijvoorbeeld het wel/niet gevoelig zijn voor SSL attacks (door batch gewijze verwerking en toevoeging van gegevens zouden eerder voorgevallen SSL attacks bij DigiNotar niet kunnen plaatsvinden). Ook als onderdeel van de aanbestedingsprocedures werd door DigiNotar veel detail gegevens verstrekt over de implementatie van maatregelen en het kwaliteitssysteem. Ook werden daarover detail vragen gesteld door de aanbestedende partij. Onder meer zijn recente aanbestedingen gedaan voor: • Tennet certficaten • Diverse ministeries en Gemeenten • Logius en ICTU SSL certificaten • TAXI project	Hiermee wordt bedoeld dat Logius als toezichthouder te veel afging op het oordeel van de auditor. De auditrapportages die Logius bij de certificaatdienstverlener kon inzien, maakten niet duidelijk op welke overwegingen het oordeel van de auditor is gebaseerd omdat het auditrapport alleen afwijkingen van de norm vermeldt. Hierdoor is het voor Logius eigenlijk onmogelijk op basis van dit rapport eigenstandig te besluiten of zij vinden dat vertrouwen in deze certificaatdienstverlener gerechtvaardigd is.
39	OPTA	5.3.1		Conformiteitsverklaring TTP.NL moet zijn conformiteitsverklaring ETSI 101 456. De minister van EL&I wijst de auditors aan > artikel 18.16 Tw	Het TTP.NL-certificaat stelt dat de auditerende instelling bevestigt dat, gebaseerd op de certificerings audit volgens het TTP.NL schema voor management systeem certificering, het management systeem van de certificatie-dienstverlener voldoet aan de vereisten in ETSI TS 101 456 en ETSI 102 042. Om verwarring te voorkomen spreekt de Onderzoeksraad nu in het rapport over TTP.NL-verklaring in plaats van over TTP.NL-conformiteitsverklaring.
40	voorm. compliance officer DigiNotar B.V.	5.3.1	De certificatiedienst-verlener – incidenten	Onvolledig De term compromitering van de van zijn private sleutel, is niet sluitend omschreven.	Het is niet duidelijk wat hier bedoeld wordt. De Onderzoeksraad heeft aangesloten bij de letterlijke tekst uit het contract
41	Logius	5.4.1	Logius…PKIoverheid-certificaten.	Logius is derdelijnstoezichthouder als het gaat om gekwalificeerde elektronische handtekeningen certificaten want daar is de auditor de eerstelijnstoezichthouder en OPTA tweedelijnstoezichthouder. Logius is tweedelijnstoezichthouder bij systeemcertificaten waarbij de auditor de eerstelijnstoezichthouder is.	De Onderzoekraad is van oordeel dat de toezichthoudende rol van Logius niet tweede of derdelijns is. Logius' rol als toezichthouder kent geen wettelijke basis. Zijn rol als toezichthouder vloeit voort uit de privaat-rechtelijke overeenkomst tussen Logius en de marktpartijen die hij toestaat PKIoverheid certificaten te leveren mits zij zich aan de regels zoals vastgelegd in de overeenkomst houden. Deze positie geeft Logius, naar het oordeel van de Onderzoeksraad, de verant-woordelijkheid er voor te zorgen dat partijen de regels kennen en er actief op toe te zien dat partijen de regels naleven. Dit eerste doet zij door middel van het actief uitdragen van het programma van eisen. Het tweede doet zij slechts indirect, gebaseerd op auditverklaringen en signalen van anderen. De Onderzoeksraad is van oordeel dat, blijkens de wijze waarop het toezicht door Logius is ingericht en de eigen kwalificatie van derdelijnstoezichthouder, Logius zich onvoldoende bewust is geweest van de verantwoordelijkheden die uit haar rol als contractpartij voortvloeien.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
42	Logius	5.4.1	Deze…instaat.	Logius is niet de opdrachtgever van de CSP's in de zin van opdrachtgever-leverancier verhouding waarbij een opdrachtgever de leverancier betaalt voor zijn diensten. Logius beheert het PvE schema, de Minister staat borg voor het schema. Daarnaast houdt Logius toezicht op de CSP's.	Logius sluit een overeenkomst af met de partijen die PKIoverheid-certificaten willen leveren. Deze overeenkomst verbindt partijen er toe te voldoen aan de eisen die Logius stelt. Het betreft eisen vastgelegd in de overeenkomst en eisen vastgelegd in het door de minister ven Binnenlandse Zaken en Koninkrijksrelaties vastgestelde Programma van Eisen PKIoverheid. De certificaten worden uitgegeven in naam van de Staat der Nederlanden. Logius geeft aan dat deze certificaten een hoge mate van veiligheid kennen. Gezien deze context acht de Onderzoekraad het enerzijds de verant-woordelijkheid van Logius de regels actief uit te dragen, en anderzijds daadwerkelijk te verifieren of partijen zich aan de overeengekomen afspraken houden. Dat Logius niet voor de diensten betaalt doet hier niet aan af.
43	OPTA	5.4.2	Zij…zelf.	Onjuist. "Actief toezicht" is, in tegenstelling tot re-actief toezicht, toezicht dat op eigen initiatief van de toezichthouder wordt uitgevoerd. OPTA hield op eigen initiatief toezicht. Indien twijfels bestonden ten aanzien van door de auditor geconstateerde afwijkingen of de wijze waarop deze zijn opgelost stelde OPTA daarover vragen bij de certificatiedienstverlener. Zo nodig werd ook aangekondigd dat de registratie zou worden beëindigd als bepaalde non-conformiteiten niet binnen een bepaalde termijn zouden worden opgelost.	OPTA baseert zijn toezichtactiviteiten primair op de auditrapportages. Dit beoordeelt de Onderzoekraad als reactief toezicht. De term is veranderd in indirect toezicht.
44	voorm. compliance officer DigiNotar B.V.	5.4.3	Dit laatste – gecontroleerd	Op zijn minst ten dele onjuist Een verklaring kan immers ook niet gegeven worden zonder dat er daadwerkelijk certificaten in productie zijn aangemaakt en ook zijn ingetrokken. Alle productionele processen en procedures werden tijdens een audit gecontroleerd in de praktijk. Er moesten bijvoorbeeld "echte" taxi gekwalificeerde certificaten worden uitgegeven en gebruikt, alvorens de audit kon worden afgerond en het certificaat verstrekt.	In de tekst is nu tot uitdrukking gebracht dat de auditor - zij het beperkt - de feitelijke werkwijze van de certificaatdienstverlener controleerde.
45	OPTA	5.4.3	Logica…is.	Onjuist. In ieder geval staat in elke conformiteitsverklaring dat de conformiteit met ETSI 101 456 is getoetst, waardoor de waarde van een dergelijke verklaring voor OPTA duidelijk is.	De Onderzoeksraad bedoelt hier de certificering conform TTP.NL-schema. Omdat hij begrijpt dat TTP.NL-conformiteitsverklaring voor onduidelijkheid zorgt is gekozen voor de term TTP.NL-verklaring. Zie voor toelichting begrippenlijst.
46	OPTA	5.5.1	De…bedreigen.	Voor gekwalificeerde certificaten geldt dat het zicht op deze risico's nu zeer zeker wel bestaat.	Het rapport beschrijft de situatie ten tijden van het DigiNotarincident. Zicht op risico's betekent naar het oordeel van de Onderzoeksraad dat systematisch is gekeken wat de risico's zijn en hoe hier mee omgegaan dient te worden.
47	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	5.5.1	Tekstvoorstel: "De Raad concludeert dat onvol-doende zicht bestaat op de risico's die de veiligheid van digitale certificaten bedreigen die niet onder-worpen zijn aan het regime van oftewel OPTA oftewel PA overheid?"	Onduidelijk is hier welke certificaten de Raad bedoelt. Voor de risico's binnen de beide stelsels die door de Raad beschreven zijn, namelijk het PKI overheidstelsel en de gekwalificeerde elektronische handtekening heeft het DigiNotar incident er in ieder geval feitelijk toe geleid dat dit zicht nu zeker wel bestaat. Voor het niet gereguleerde stelsel zijn slechts de regels van de zogenaamde Web browser fabrikanten relevant: voldoen daaraan stelt certificaatverkopers in staat om bijvoorbeeld SSL-certificaten te doen accepteren als vertrouwd. Overigens heeft zowel het DigiNotar als het Comodo incident ervoor gezorgd dat de web browser fabrikanten, verenigd in het CAB-forum, bezig zijn met aanscherpen van hun eisen.	De Onderzoeksraad duidt hier op het risico-bewustzijn betreffende alle certificaten. Ook de PKIoverheid-certificaten en de gekwalificeerde certificaten.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
48	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	5.5.1	Tekstvoorstel: De Onderzoeksraad is van mening dat de Minister van Binnenlandse Zaken vanuit zijn coördinerende verant-woordelijkheid voor ICT binnen de rijksoverheid de voorwaarden dient te scheppen en bewaken waaronder afzonderlijke rijksoverheids organisaties in staat zijn om optimale invullen te geven aan hun eigen verantwoordelijkheid voor digitale veiligheid. Daar waar de minister geen bevoegdheden heeft, zoals naar de mede-overheden, wordt de minister sterk aangeraden om deze voorwaarden te delen met deze organisaties, zodat zij vanuit hun eigen verant-woordelijkheid invulling kunnen geven aan de digitale veiligheid van hun organisaties. Binnen dit …….	De Minister heeft feitelijk slechts bevoegdheden voor de rijksoverheid op het gebied van coördinatie. Die stelselverant-woordelijkheid kan en zal de minister nemen, zoals reeds blijkt uit de aan de TK gemelde nadere maatregelen ten aanzien van het PKI overheidstelsel.	De Onderzoeksraad is van oordeel dat de rijksoverheid een stelselverantwoordelijkheid heeft voor digitale veiligheid bij overheids-organisaties. Deze verantwoordelijkheid houdt in dat zij de randvoorwaarden moet scheppen die het individuele overheids-organisaties mogelijk maken hun verant-woordelijkheid te nemen voor digitale veiligheid. Deze stelselverantwoordelijkheid geldt naar de mening van de Onderzoeksraad voor de gehele publieke sector.
49	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	5.5.1	“heeft” veranderen in “had”	Zie hierboven; het DigiNotar incident heeft feitelijk reeds tot nieuwe maatregelen geleid	Logius blijft zichzelf - ook in de reactie op het conceptrapport - omschrijven als derdelijns-toezichthouder. Dit past naar het oordeel van de Onderzoeksraad, niet bij de verant-woordelijke positie die Logius heeft.
50	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	5.5.1	Alinea laten vervallen	De Onderzoeksraad geeft zelf aan dat zij dit niet uitputtend heeft onderzocht, en de latere beschouwing van digitale veiligheid bij een aantal organisaties onderbouwt dit beeld slechts minimaal. De tekst zoals voorgesteld bij 62/51-56 biedt de mogelijkheid om met dit veronderstelde gebrek aan inzicht pro-actief aan de slag te gaan.	Het is voor organisaties niet goed mogelijk zelf de betrouwbaarheid van certificaten vast te stellen. Daarom is het van belang de betrouwbaarheid middels PKIoverheid, wet-geving of zelfregulering wordt gegarandeerd.
51	Logius	5.5.1	De passieve…. opdrachtgever heeft.	De conclusie over de rolopvatting is onjuist. Zie bovenstaande opmerking bij argumentatie bij 4.1.3, bladzijde 37, regel 19 t/m 21 inzake de zinsnede “Het Ministerie… TTP.NL-conformiteitsverklaring.” En Zie bovenstaande opmerking bij argumentatie 5.4.1, bladzijde 59, regel 6/m 15 inzake de zinsnede “Logius…overleggen.” En Zie bovenstaande opmerking bij argumentatie 5.4.1, bladzijde 59, regel 17 inzake de zinsnede “Logius…PKIoverheid certificaten.” En Zie bovenstaande opmerking bij argumentatie 5.5.1, bladzijde 63, regel 9 t/m 17 inzake zinsnede “Wat betreft….beperkt”.	Logius sluit een overeenkomst af met de partijen die PKIoverheid-certificaten willen leveren. Deze overeenkomst verbindt partijen er toe te voldoen aan de eisen die Logius stelt. Het betreft eisen vastgelegd in de overeenkomst en eisen vastgelegd in het door de minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde Programma van Eisen PKIoverheid. Logius geeft aan dat deze certificaten een hoge mate van veilig-heid kennen. Gezien deze context moet van Logius worden verwacht dat het enerzijds de regels actief uitdraagt en anderzijds daad-werkelijk verifieert of partijen zich aan de overeengekomen afspraken houden. Dat Logius niet voor de diensten betaalt doet hier niet aan af.
52	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	6.3.2	De Onderzoeksraad constateert dat de strategie van multikanaal-benadering….vertrouwen van de Klant”.	De onderzoeksraad doet echter geen uitspraak over de veiligheid van deze multikanaalbenadering, alleen over de continuïteit van de dienstverlening.	De Onderzoeksraad onderschrijft dit commentaar, maar dat heeft niet geleid tot wijziging van de rapporttekst. De constatering van de Onderzoeksraad is relevant voor de latere constateringen over multikanaalbenadering als beheersmaatregel.
53	Een in de verkenning betrokken bancaire instelling	6.3.2	“niemand had rekening gehouden met dit scenario” vervangen door “dit scenario werd als zeer onwaarschijnlijk beschouwd”		De Onderzoeksraad heeft geen signalen gehad dat dit scenario eerder was voorzien.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
54	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	6.3.3		Deze conclusie ondergraaft de conclusie dat de ingerichte stelsels geen meerwaarde hebben, immers juist door de stelsels konden partijen elkaar snel vinden	De conclusie gaat niet over de ingerichte stelsels, maar plaatst vraagtekens bij het vermogen van de overheid om een volgende digitale crisis aan te kunnen pakken zonder gerichte draaiboeken.
55	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Algemeen	Alvorens inhoudelijk op uw rapport in te gaan wijs ik u erop dat de normen voor ICT certificaten inter-nationaal bepaald zijn. Gegeven het internationale karakter van internet hebben nationale wet- en regelgeving slechts beperkte impact op het stelsel van certificaten als zodanig. Daarbij speelt dat naast regelgeving van internationale instanties (zowel bovennationaal als internationaal erkende expertise centra) de normen voor een belangrijk deel in de praktijk vorm krijgen en door de internationale ICT gemeen-schap als gangbare mores worden gehanteerd. Bij het beoordelen van concrete situaties dient dit gehele stelsel in ogenschouw genomen te worden.		De Onderzoekraad onderkent de internationale dimensie van certificaatdienst-verlening. Voor wat betreft PKIoverheid ligt de regie echter in handen van de minister van Binnenlandse Zaken en Koninkrijks-relaties.
56	OPTA	Algemeen	Samenhang toegezegde veranderingen Door onderzoeksbureau Logica en door de Rijks Audit Dienst zijn eerder onderzoeken uitgevoerd naar het incident bij DigiNotar. In grote lijnen komen de bevindingen van de Onderzoeksraad voor Veiligheid overeen met deze twee eerdere onder-zoeken. Mede naar aan-leiding van deze twee onderzoeken heeft de minister van Binnenlandse Zaken en Koninkrijks-relaties en de minister Economische Zaken, Landbouw en Innovatie reeds een aantal maat-regelen toegezegd die het toezicht op certificatie-diensten moeten verbeteren. Het college zou graag willen weten of de Onderzoeksraad voor Veiligheid deze maat-regelen adequaat acht.		De Onderzoeksraad is van mening dat de betrokken partijen - de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Economische Zaken, Landbouw en Innovatie, OPTA, Logius, certificaatdienstverleners - zelf moeten bepalen welke mate van digitale veiligheid gewenst is, en dan maatregelen moeten treffen die passend zijn om dit niveau te bereiken. De getroffen maatregelen zijn naar de mening van de Onderzoeksraad zinvol. De Onderzoeksraad is evenwel van oordeel dat van een structureel veiliger digitale overheid pas sprake kan zijn als ook de oorzaken van het ontstaan van problemen worden weggenomen.
57	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Algemeen	In de eerste plaats gaat het daarbij over uw conclusie over stelsel-verantwoordelijkheid. Daarbij dient opgemerkt te worden dat de stelsel-verantwoordelijkheid voor alle verschijningen van PKI binnen Nederland niet door de minister van Binnenlandse Zaken en Koninkrijksrelaties genomen kan worden. Ik heb daarvoor niet het mandaat noch de wettelijke titel. Daar waar het gaat om de stelsel-verantwoordelijkheid voor het PKI-overheidstelsel heb ik die onverkort wel.		De Onderzoeksraad merkt op dat de rijks-overheid in dezen een tweeledige verant-woordelijkheid heeft. Zij is verantwoordelijk voor de kwaliteit van de voorzieningen die zij zelf ter beschikking stelt aan overheids-organisaties, om de digitale veiligheid te waarborgen. Ook heeft zij, naar het oordeel van de Onderzoeksraad, een verant-woordelijkheid om zodanige omstandigheden te scheppen dat afzonderlijke (overheids) organisaties optimaal invulling geven aan hun eigen verantwoordelijkheid voor het waar-borgen van digitale veiligheid. Deze laatste verantwoordelijkheid wordt aangeduid als de stelselverantwoordelijkheid van de rijksover-heid voor digitale veiligheid. De onder-zoeksraad onderschrijft uw mening dat u geen stelselverantwoordelijkheid heeft voor alle verschijningen van PKI in Nederland.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
			Ik heb daarop gehandeld na de Diginotar casus, zoals ik heb toegelicht aan de Tweede Kamer in mijn brief van 16 maart 2012. De vervolgacties die uit de diverse onderzoeken naar voren komen, en die naar mijn overtuiging invulling geven aan uw opmerkingen ter versterking van het PKI overheidstelsel, zijn ondertussen ook reeds in gang gezet. Ik zal daarop hier dan ook niet verder ingaan. Maar nogmaals, een volledige stelsel-verantwoordelijkheid heb ik niet en ik verzoek u dan ook dit conform mijn bevoegdheden te beschrijven. (Kamerstukken II, 2011–2012, 26 643, nr. 230)		
58	Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Algemeen	In de derde plaats wijst u op de snelle omslag in vertrouwen, en vraagt u zich af of dit terecht is. U wijst er ook op dat er verbeteringen in het toezicht stelsel mogelijk zijn. De verbeteringen in het toezichtstelsel zijn onderkend en ik heb reeds een eerste aanzet gegeven om het certificatenstelsel robuuster en betrouw-baarder te maken, zoals ook gemeld in mijn bovengenoemde brief aan de Tweede Kamer naar aanleiding van de onder-zoeken van Logica en de Rijks accountantsdienst. Maar zelfs deze verbete-ringen laten onverlet dat een partij die zich niet aan de mores houdt die gebruikelijk is voor certifi-catiedienstverlening, en eveneens niet overgaat tot het snel melden van een incident, zich opnieuw in een vergelijkbare situatie kan bevinden. Juist daarom is het goed dat in de DigiNotar casus de overheid het vertrouwen snel heeft opgezegd. Daarmee is tevens aan andere leveranciers getoond dat het schenden van vertrouwen consequenties heeft en ook in de toekomst zal hebben.		Deze passage is aangepast: De Onderzoeksraad is van oordeel dat Logius en OPTA zich voorafgaand aan het incident meer betrokken hadden moeten tonen bij het bedrijf, en zich werkelijk hadden moeten overtuigen van de betrouwbaarheid van diens dienstverlening en de risico's die er waren. Als zij zelf goed zicht hadden gehad op de feitelijke situatie bij DigiNotar B.V. hadden zij de gebeurtenissen beter kunnen beoordelen en zouden ze minder overvallen zijn geweest.

Nr	Partij	Para-graaf	Reactie	Argumentatie	Reactie Onderzoeksraad
59	OPTA	Algemeen	Ten slotte: de Onderzoeksraad voor Veiligheid lijkt te suggereren dat een oplossing voor de door de Onderzoeksraad gesignaleerde problemen gevonden zou kunnen worden in de wijze waarop het college toezicht houdt. Indien de Onderzoeksraad voor Veiligheid die mening is toegedaan, wil het college u in concluderende zin er op wijzen dat de wijze van toezicht houden dus geen vrije keuze van het college is, maar door de wet- en regelgeving is vastgelegd en begrensd.		De wetgever heeft de rol van OPTA in het toezicht op certificaatdienstverleners beperkt. Niettemin is de Onderzoeksraad van mening dat OPTA zich te gemakkelijk in een marginale rol schikt. De Onderzoeksraad verwacht van een publieke toezichthouder dat deze van zich laat horen wanneer de wet- en regelgeving een effectieve taakuitoefening onmogelijk maakt, en ook dat deze de grenzen van zijn bevoegdheden opzoekt als hij dat nodig acht voor een goed functioneren van de sector waarin hij opereert.
60	Een in de verkenning betrokken Nederlandse gemeente	Algemeen	Eén portal i.pl.v. 400+ gemeentesites (aanbeveling)	Is een gewenste utopie, maar kan alleen gerealiseerd worden door een strakke regie(besluitvorming) vanuit de landelijke overheid.	Het rapport behandelt de stelsel-verantwoordelijkheid voor digitale veiligeheid van de rijksoverheid.
61	Belasting-dienst	Algemeen	In het rapport zou hier en daar kunnen worden gelezen dat de Raad vindt dat iedere overheids-organisatie de digitale beveiliging van de hele keten moet borgen, zodat de digitale gegevens die bij deze organisatie in handen zijn, geborgd zijn.	Dit is een miskenning van ketens en de afhankelijkheden hierin. Kennelijk worstelt de Raad daar ook mee, want hij noemt ook hier en daar dat Logius en de minister van BZK op bestuurlijk niveau systeemverantwoordelijk zijn. Analogie met de oude wereld kan hier helpen. Wij innen en betalen euro's maar niemand houdt de BD toch verantwoordelijk voor de waardevastheid van de euro? Wij sturen dingen met de post. Als er massaal post geopend wordt bij Post.NL houdt toch niemand de BD verantwoordelijk voor deze gegevensverliezen? Er was bij Diginotar vooral een dreiging van beschadiging van identiteiten en secundair gegevensverlies. En daar kan niet iedere organisatie verantwoordelijk voor zijn.	De Onderzoeksraad merkt op dat de rijksoverheid ten aanzien van digitale veiligheid een tweeledige verantwoordelijkheid heeft. Zij is verantwoordelijk voor de kwaliteit van de voorzieningen die zij zelf ter beschikking stelt aan overheidsorganisaties, om de digitale veiligheid te waarborgen. Daarnaast heeft zij, naar het oordeel van de Onderzoeksraad, een verantwoordelijkheid om zodanige omstandigheden te scheppen dat afzonderlijke (overheids)organisaties optimaal invulling geven aan hun eigen verantwoordelijkheid voor het waarborgen van digitale veiligheid.