Een Top Level Domein voor betrouwbare overheidscommunicatie

Een verkenning van de kansen en risico's

Colofon

DATUM	26-02-2013
VERSIE	1.0
PROJECTREFERENTIE	Top Level Domein als beveiligingsmaatregel
TOEGANGSRECHTEN	Projectteam en opdrachtgever
STATUS	Eindversie
EDITOR	Bob Hulsebosch
AUTEURS	Wolfgang Ebbers, Bob Hulsebosch & Martijn Oostdijk
OPDRACHTGEVER	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Synopsis

Dit rapport verkent wat de mogelijkheden van het inzetten een gTLD als beveiligingsmaatregel voor de Nederlandse overheid zijn. Het geeft inzicht in de kansen en risico's van een overheidseigen gTLD en de meerwaarde ervan ten opzichte van andere gerelateerde manieren om de overheidscommunicatie via het internet betrouwbaarder te maken.

Inhoudsopgave

Managementsamenvatting

Het Domain Name System (DNS) is het naamgevingssysteem op internet waarmee netwerken, computers, webservers, mailservers en andere toepassingen worden geïdentificeerd. Het DNS is opgebouwd als een hiërarchische en gedistribueerde database die een verscheidenheid aan data bijhoudt, waaronder domeinnamen en hun bijbehorende IP-adressen. De domeinnamen in een DNS database vormen een hiërarchische boomstructuur die de domain name space genoemd wordt. Bovenaan de boomstructuur bevinden zich de zogenaamde top level domeinen (TLDs), zoals .com en .nl. De lijst van TLDs wordt beheerd door ICANN. Onder de TLDs vallen de subdomeinen als *ebay*.com en *novay*.nl.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft bij ICANN een generiek top level domein (gTLD) aangevraagd: overheidnl. De belangrijkste potentiele toepassing van het .overheidnl gTLD is om hier een gesloten gTLD van te maken dat enkel registraties toelaat voor een door de overheid bepaalde doelgroep. Dit in tegenstelling tot een open gTLD dat in principe voor iedereen toegankelijk is. Met een gTLD is het mogelijk om eigen internetdomeinen op te zetten, zoals bijvoorbeeld www.paspoort.overheidnl. Daarnaast biedt een dergelijk gesloten en door de overheid gecontroleerd gTLD potentiele mogelijkheden om invloed uit te oefenen op de beveiliging en betrouwbaarheid van de online overheidscommunicatie en deze daarmee naar een hoger niveau te brengen.

Een belangrijke vraag is of de kansen en risico's die een eigen gTLD bieden om deze doelen te bereiken opwegen tegen die van situaties zonder eigen gTLD. Verschillende relevante situaties zonder eigen gTLD zijn denkbaar. Allereerst is er de huidige situatie waarin veel overheidsdomeinen onder .nl geregistreerd zijn en er in toenemende mate sprake is van een verbeterd beleid aangaande het registreren van domeinnamen en het effectueren ervan vanuit de overheid. De verbeteringen die plaats vinden omvatten consolidatie van overheidsdomeinen en richtlijnen voor de registratie ervan onder het .nl domein, en richten zich voornamelijk op de schaal van de Rijksoverheid en minder op de overheid in haar volle breedte. Daarnaast is er nog een situatie denkbaar waarin domeinen onder .overheid.nl geregistreerd worden i.p.v. onder een eigen gTLD als .overheidnl.

Dit rapport beschrijft en karakteriseert kort de drie verschillende situaties. Vervolgens verkent het de kansen en de risico's van een overheidseigen gTLD ten opzichte van de twee alternatieve situaties zonder eigen gTLD. Hierbij wordt onderscheid gemaakt in de kansen en risico's die kunnen ontstaan in termen van de beveiliging van de gTLD, de betrouwbaarheid van de communicatie ermee, de potentiele efficiëntie en kosten ervan, maatschappelijke acceptatie van gTLDs in het algemeen en overheids-gTLDs in het bijzonder, en bestuurlijke acceptatie van regievoering van de overheid op de eigen DNS namespace.

Voor elk van deze aspecten zijn, aan de hand van desk research, interviews met stakeholders en een expert sessie, de kansen en risico's in kaart gebracht, gewogen en afgezet tegen de andere situaties waardoor het toepassingspotentieel van een overheidseigen gTLD inzichtelijk is gemaakt. Interviews over het onderwerp zijn

gehouden met DNS(SEC) experts, beveiligingsexperts, communicatie-adviseurs en partijen die ook een gTLD hebben aangevraagd (politie, gemeente Amsterdam en de Vlaamse overheid). Nieuwe kansen en risico's die tijdens de interviews naar voren kwamen zijn weer meegenomen in latere interviews ter validatie. Alle verzamelde informatie diende als input voor een workshop waarbij experts binnen en buiten de overheid gevraagd werd om de kansen en risico's van een overheidseigen gTLD te wegen in termen van relevantie en de effort die nodig is om ze te verzilveren respectievelijk te mitigeren. Onderscheidt wordt daarbij gemaakt tussen de eindsituatie en de transitie-effort die nodig is om de eindsituatie te realiseren.

Deze verkenning is primair bedoeld voor beleidsmedewerkers van de Nederlandse overheid om inzage te krijgen in de kansen en risico's van een overheidseigen gTLD ten opzichte van de huidige en alternatieve situaties en hierop beleid te ontwikkelen. Ook voor andere partijen die overwegen een gTLD aan te vragen of dit al gedaan hebben kan het van meerwaarde zijn bij het ten uitvoer brengen ervan.

De uitkomst van deze verkenning is dat de absolute meerwaarde van de beveiligingsmogelijkheden die een gTLD biedt beperkt is ten opzichte van de andere situaties en te kenschetsen is als anders maar niet beter of slechter. Beschikbare beveiligingsmaatregelen om DNS veiliger te maken (DNSSEC) of om via DNS de communicatie te beveiligen (met bijvoorbeeld technologieën als DANE en DKIM) kunnen ook in de huidige situatie ingezet worden. Wel is er bij een gTLD meer controle over de beveiliging doordat er strengere eisen kunnen worden gesteld aan bijvoorbeeld de veiligheid van het registratieproces en is door het beperken van het aantal registranten beter te controleren. Het feit dat er door de greenfield situatie van een gTLD minder heterogeniteit is helpt hierbij om meer grip te krijgen op beveiliging van de domeinregistratie en het beheer ervan. In de huidige .nl situatie is deze controle beperkter, maar het is niet onmogelijk om deze ook hier te creëren door als overheid afspraken te maken met de .nl registry en registrars. Dit zou beschouwd kunnen worden als een verbeterde .nl situatie. In het geval van een .overheid.nl situatie, is de overheid volledig in control over wie daaronder domeinen registreert en hoe de beveiliging ervan ingericht is.

Vanuit communicatie-perspectief biedt een eigen gTLD beperkte meerwaarde betreffende de herkenbaarheid en de eenduidigheid van de overheidscommunicatie richting burgers of bedrijven. Hier hangt een prijskaartje aan dat mede bepaald wordt door te verwachten transitiekosten voor allerlei bestaande communicatieve uitingen. Deze zullen naar het zich laat aanzien significant zijn, ook voor dat deel van het bedrijfsleven dat naar overheidswebsites verwijst. Een .overheid.nl situatie biedt vanuit communicatieperspectief vergelijkbare meerwaarde tegen naar verwachting substantieel lagere kosten. Overheidswebsites worden t.o.v. de huidige .nl situatie herkenbaarder als ze vallen onder een gTLD of het .overheid.nl domein. Een zelfde effect wordt momenteel ook bereikt door te consolideren onder rijksoverheid.nl (b.v. www.rijksoverheid.nl/ministeries/bz en www.rijksoverheid.nl/ministeries/ez). Twee andere factoren spelen daarnaast mee die de herkenbaarheid van een domeinnaam (URL) minder relevant maken. Ten eerste navigeren veel gebruikers niet direct via het intoetsen van een domeinnaam (URL) in de browser maar doen dit voornamelijk via zoekmachines als Google. Ten tweede wordt met de komst van mobiele platformen en applicaties daarop de zichtbaarheid van een URL steeds minder voor de gebruiker.

De acceptatie en het draagvlak onder burgers en bedrijfsleven zijn lastig te bepalen maar lijken te worden ondermijnd door het ontbreken van duidelijke meerwaarde voor hen en de weinig intuïtieve naamgeving van de aangevraagde .overheidnl gTLD naam. Voor burgers ligt met de komst van de vele nieuwe gTLDs verwarring op de loer. Daarnaast vormen mogelijk significante transitiekosten een forse uitdaging voor het versnellen van de gebruikersacceptatie alsmede voor het versterken van het draagvlak in de samenleving forse uitdagingen. Het betreft hier dan voornamelijk technische transitiekosten als het opnieuw configureren van systemen en de aanschaf van nieuwe PKI certificaten. Bovendien is de impact niet beperkt tot de overheid zelf; secundaire kosten zijn bijvoorbeeld bedrijven die kosten moeten maken voor het wijzigen van bestaande verwijzingen naar overheidswebsites.

Met een overheidseigen gTLD vallen efficiency-slagen te behalen betreffende de vindbaarheid en authenticiteit van overheidscontent van de overheidswebsites. De grote mate van controle die een gTLD met zich meebrengt kan ten koste gaan van de flexibiliteit en vrijheid die overheidsorganisaties nu hebben om een domeinnaam aan te vragen. Er dient in geval van een overheidseigen gTLD rekening te worden gehouden met het feit dat het in sommige gevallen niet wenselijk is om een website onder overheidsvlag te voeren. Er zal dan beleid voor dergelijke vraagstukken moeten worden opgesteld.

Er zijn relatief veel risico's verbonden betreffende de uitvoerbaarheid van een eigen gTLD. Het mislukken ervan door de volledigheid van de uitrol verkeerd in te schatten kunnen desastreus zijn voor de acceptatie van een gTLD. Voordelen zijn te behalen met het inrichten van één centraal loket voor het aanvragen van domeinen. Dit vergroot de controle op registraties van domeinnamen en draagt bij tot een beter toezicht op het naleven van het gebruik van DNSSEC en de webrichtlijnen. Een dergelijk loket biedt dezelfde voordelen voor de huidige .nl en .overheid.nl situaties. Er dient gewaakt te worden dat het registratieproces niet (veel) omslachtiger wordt dan in de huidige situatie waarin organisaties relatief veel vrijheid genieten betreffende het aanvragen van domeinnamen. Er is kans op een bepaalde starheid die kan omslaan in de perceptie van een verlies van autonomie bij overheidsorganisaties waardoor ook het draagvlak voor een gTLD onder druk kan komen te staan. De breedte van de uitrol van een gTLD is bepalend voor het succes ervan en dient weloverwogen gemaakt te worden. Geldt het registreren van domeinnamen via het loket voor de gehele overheid inclusief decentrale overheden en organisaties met een publieke taak haalbaar of voor slechts een deel hiervan? Een gefaseerde aanpak van het uitrollen van een gTLD onder overheidsorganisaties behoort tot de mogelijkheden: begin overzichtelijk met bijvoorbeeld alleen de Rijksoverheid en verbreed na positieve ervaring eventueel naar mede-overheden. Een dergelijke aanpak is ook van toepassing bij een eventuele verbreding van de consolidatie activiteiten in de huidige .nl situatie en bij de .overheid.nl situatie.

De contractuele verplichtingen voor de gTLD eigenaar richting ICANN kunnen ook belemmerend werken. Bijvoorbeeld het aanvragen van de domeinnaam 'de.overheidnl' zal vanuit naamgevingsconventies niet worden toegestaan door ICANN. In een .overheid.nl zal dit geen probleem hoeven zijn. Daarnaast is de gTLD houder verplicht om alle transacties betreffende domeinregistraties en wijzigingen te publiceren op de publieke site van ICANN. Vanuit overheidsperspectief kan dit soms onwenselijk zijn (denk daarbij aan het voortijdig lekken van voorgenomen campagnes waarvoor een domeinnaam is aangevraagd).

De kosten van de aanschaf en het beheer van een gTLD zullen naar verwachting substantieel hoger zijn dan de huidige kosten of die voor de .overheid.nl situatie. Deze kosten komen dus bovenop de al eerder benoemde communicatieve en technische transitiekosten.

1 Inleiding

1.1 GENERIEKE TOP LEVEL DOMEINEN

Het Domain Name System (DNS) is het naamgevingssysteem op internet waarmee netwerken, computers, webservers, mailservers en andere toepassingen worden geïdentificeerd. Een domeinnaam is een naam in het DNS die verwijst naar een computeradres dat uit nummers bestaat, de zogenaamde IP-adressen. Het DNS functioneert als het telefoonboek van het computernetwerk. De vertaling van de naam naar het betreffende IP-adres geschiedt middels gedistribueerde DNS-servers.

Een domeinnaam kan in verschillende niveaus worden opgesplitst. Zo bestaat er een top level domein (TLD) met daaronder vaak second en third level subdomeinen. In het voorbeeld *www.novay.nl,* is *nl* het TLD, *novay* het second level domein en *www* het third level subdomein.

De lijst van TLDs wordt beheerd door ICANN[1], een internationale organisatie die verantwoordelijk is voor domeinnamen en adressering op internet. Deze lijst bestaat uit zogenaamde generieke TLDs (gTLDs zoals .com en .net) en landen TLDs (ccTLDs zoals .nl en .be). ICANN heeft enige tijd geleden besloten het aantal gTLDs uit te breiden. Onlangs sloot de eerste registratietermijn voor nieuwe gTLDs. Er zijn er maar liefst 1930 aangevraagd. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is een van de aanvragers en heeft een inschrijving gedaan voor het .overheidnl gTLD. De bedoeling van het .overheidnl gTLD is hier een gesloten gTLD van te maken dat enkel registraties toelaat voor een door de overheid bepaalde doelgroep. Dit in tegenstelling tot een open gTLD dat in principe voor iedereen toegankelijk is.

Er wordt vaak gepropageerd dat een gTLD nieuwe (business) mogelijkheden biedt en kansen creëert door de vrijwel ongelimiteerde combinaties van domeinnamen. Met een gTLD is het mogelijk om eigen internetdomeinen op te zetten, zoals bijvoorbeeld www.paspoort.overheidnl. Vooral op het gebied van marketing en branding bieden gTLDs uitdagende kansen. Daarnaast biedt een dergelijk gesloten en door de overheid gecontroleerd top level domein potentiele mogelijkheden om invloed uit te oefenen op de beveiliging en betrouwbaarheid van de online overheidscommunicatie en deze naar een hoger niveau te brengen.

1.2 ONDERZOEKSVRAAG

Het doel van dit onderzoek is te verkennen of dergelijke gepropageerde voordelen van een gTLD ook op de Nederlandse overheid en haar online communicatie van toepassing zijn. Mogelijk kleven er ook nadelen aan een eigen gTLD. De centrale onderzoeksvraag luidt dan ook als volgt: *welke kansen en risico's biedt een overheidseigen gTLD ten opzichte van situaties zonder eigen gTLD?*

De insteek daarbij is vooral te kijken naar de potentiele meerwaarde van een overheidseigen gTLD als beveiligingsmaatregel. Dit laatste dient opgevat te worden in brede zin, variërend van technische

[1] Internet Corporation for Assigned Names and Numbers.

beveiligingsmaatregelen (authenticatie, certificaten) tot betrouwbaarheid van de communicatie via het internet (beschikbaarheid, toezicht).

De centrale onderzoeksvraag valt uiteen in een aantal aandachtsgebieden met daarbinnen enkele specifieke onderzoeksvragen die de verkenning afbakenen in termen van kansen en risico's en eventuele impact van een gTLD. Hieronder formuleren we deze aandachtsgebieden en bijbehorende vragen.

Beveiliging	• Welke eisen moeten gesteld worden om de overheidscommunicatie te beveiligen? • Hoe het toezicht te regelen over deze beveiligingseisen en de handhaving ervan? • Wat is de toegevoegde waarde van een gTLD voor de beveiliging van websites? • Wegen de kansen en risico's van het inzetten van een gTLD als beveiligings-maatregel op tegen die van de huidige beveiligingsmaatregelen in het .nl domein?
Communicatie	• Kan met behulp van een gTLD de echtheid van de overheidswebsites beter geborgd worden? • Kan er vanuit de overheid op een betrouwbare manier elektronisch met burger en bedrijfsleven gecommuniceerd worden via bijvoorbeeld portalen? • Hoe zit het met de schaarste aan domeinen? • Hoe de beveiliging te regelen van de communicatie met partijen buiten het veilige overheidsdomein? • Is verbreding van beveiligingsmaatregelen als DANE naar andere (g)TLDs gewenst om veilige communicatie van en naar de overheid te garanderen?
Efficiëntie en kosten	• Wordt het met een gTLD makkelijker om overheidsinformatie te vinden? • Wegen de baten van een gTLD op tegen de kosten (inclusief benodigde infrastructuur, beheer, toezicht en migratie)? Vooral als dit afgezet wordt tegen de huidige en andere mogelijke situaties waarbij het DNSSEC beveiligde .nl domein met technologieën als DANE en DKIM verder verbeterd wordt. • Hoe zit het met de kosten van het beheer van de gTLD, de eenmalige bijdrage aan ICANN ($185.000) en de jaarlijkse bijdrage aan ICANN ($25.000), en de kosten voor de migratie, communicatie en marketing? Welke factoren zijn er nog meer die de kosten van een gTLD bepalen en hoe hoog zijn deze kosten? Wegen deze op tegen de huidige kosten van de overheidsdomeinen?
Maatschappelijke acceptatie	• Wat vinden burgers en bedrijven van een gTLD in het algemeen? • Wat vinden burgers en bedrijven van een overheidseigen gTLD in het bijzonder? • Wat is de meerwaarde voor burgers en bedrijven? • Wat is nodig om vertrouwen te winnen? • Is een marketing/promotie campagne noodzakelijk? • Wat is de acceptatie van beveiligingsmaatregelen als DANE en DKIM in de internetgemeenschap, bijvoorbeeld onder browser vendors en makers van (mobiele) besturingssystemen? • Kunnen webbrowsers en mobiele besturingssystemen en apps overweg met beveiligingsmaatregelen als DANE en DKIM?
Bestuurlijke acceptatie	• Wat vinden de verschillende overheidsinstanties van een overheidseigen gTLD? • Hoe ziet de regievoering van een overheidseigen gTLD eruit en willen bestuurders zich hier aan conformeren? • Is het vanuit kansen- en risico-oogpunt wenselijk om de overheid regie te laten voeren op een overheidseigen gTLD DNS structuur met bijbehorende grip op beveiligingseisen en standaarden? • Biedt de greenfield situatie kansen? Zoja, welke? Wat zijn de risico's? • Hoe om te gaan met andere Nederlandse overheidspartijen die een gTLD hebben aangevraagd zoals de gemeente Amsterdam en de politie? • Scoping: Is het inzetten van een gTLD voor de gehele centrale overheid, decentrale overheden en organisaties met een publieke taak haalbaar of voor slechts een deel hiervan?
Uitvoerbaarheid	• Hoe ziet een mogelijke inrichting van de bij een gTLD behorende functies en registrar/registry rollen op hoofdlijnen eruit? • Hoe ziet de governance structuur eruit? • Wie zijn geautoriseerde registrars en hoe ziet het proces van domeinnaamregistratie er onder het overheidnl gTLD uit. Welke eisen moeten aan registrars gesteld worden? Wat zijn hierbij de overwegingen?

Uit deze lijst van relevante subvragen blijkt dat het probleemveld veelomvattend is. Een dergelijke greenfield situatie biedt op zichzelf weer kansen, maar ook risico's. Het betreft vraagstukken over maatschappelijk en bestuurlijk draagvlak, organisatorische processen, technologie, en standaarden. In de beantwoording van de vraagstelling zullen we dan ook, naast de letterlijke vragen, een systematiek toepassen die er voor zorg draagt dat de relevante aspecten de revue passeren.

1.3 ONDERZOEKSAANPAK

Het resultaat van de opdracht is een verkenning van de kansen en risico's die een overheidseigen gTLD biedt om de overheidscommunicatie op een hoger beveiligingsniveau te brengen en hoe dit te vertalen naar een bij een gTLD behorende beheerstructuur en bijbehorende functionaliteiten als registries en registrars.

Het startpunt van de verkenning is de huidige situatie waarbij de internet presence van de Nederlandse overheid onder het .nl domein vorm gegeven is (bijvoorbeeld rijksoverheid.nl, belastingdienst.nl, logius.nl, etc.). De kansen en risico's voor het inzetten van een overheidseigen gTLD zullen per aandachtgebied afgezet moeten worden tegen de huidige situatie. Daarnaast is er nog een andere situatie denkbaar waartegen een gTLD oplossing afgezet kan worden. Dit betreft een situatie waarin uitgegaan wordt van een zogenaamde second-level domeinen zoals gebruikelijk is in bijvoorbeeld Groot Brittannië met voorbeelden als .co.uk en .gov.uk. Een dergelijke situatie zou ook in Nederland toepasbaar zijn: .overheid.nl (of .gov.nl). Ook deze situatie zal vergeleken worden met een gTLD situatie.

De gekozen aanpak hiervoor bestond uit een aantal activiteiten:

1. Inventarisatie – Het in kaart brengen van de mogelijke kansen en risico's per deelaspect van een overheidseigen gTLD ten opzichte van de huidige en de hierboven geschetste alternatieve situaties door middel van desktop research.
2. Toetsen – Deze kansen en risico's toetsen in interviews met verschillende experts (beveiligingsexperts, DNS-experts, overheidsinstanties, uitvoeringsorganisaties). Nieuwe kansen en risico's die tijdens de interviews naar voren kwamen werden weer meegenomen in andere interviews ter validatie. De interviews vonden fysiek of telefonische plaats aan de hand van een vooropgestelde vragenlijst. Er zijn 11 interviews afgenomen.
3. Validatie en prioritering – De in de twee bovenstaande activiteiten verzamelde informatie diende als input voor een workshop waarbij experts binnen en buiten de overheid gevraagd werd om de kansen en risico's van een overheidseigen gTLD te wegen in termen van relevantie en de effort die nodig is om ze te verzilveren respectievelijk te mitigeren.
4. Analyse – Deze activiteit betrof het ordenen van alle bevindingen.

1.4 LEESWIJZER

Deze verkenning is primair bedoeld voor beleidsmedewerkers van de Nederlandse overheid om inzage te krijgen in de kansen en risico's van een overheidseigen gTLD ten opzichte van de huidige en alternatieve situaties en hiervoor

beleid te ontwikkelen. Ook voor andere partijen die overwegen een gTLD aan te vragen of dit al gedaan hebben kan het van meerwaarde zijn bij het ten uitvoer brengen.

De structuur van de verkenning is als volgt. De volgende sectie beschrijft het toepassingspotentieel van een overheidseigen gTLD als beveiligingsmaatregel. Het geeft een ordening van de kansen en risico's en zet deze af tegen de huidige en alternatieve situaties. Sectie 3 vat de bevindingen samen een geeft antwoord op de onderzoeksvragen.

2 Kansen en risico's

2.1 VERSCHILLENDE SITUATIES

De kansen en risico's van een overheidseigen gTLD zullen beschouwd worden ten opzichte van twee andere situaties:

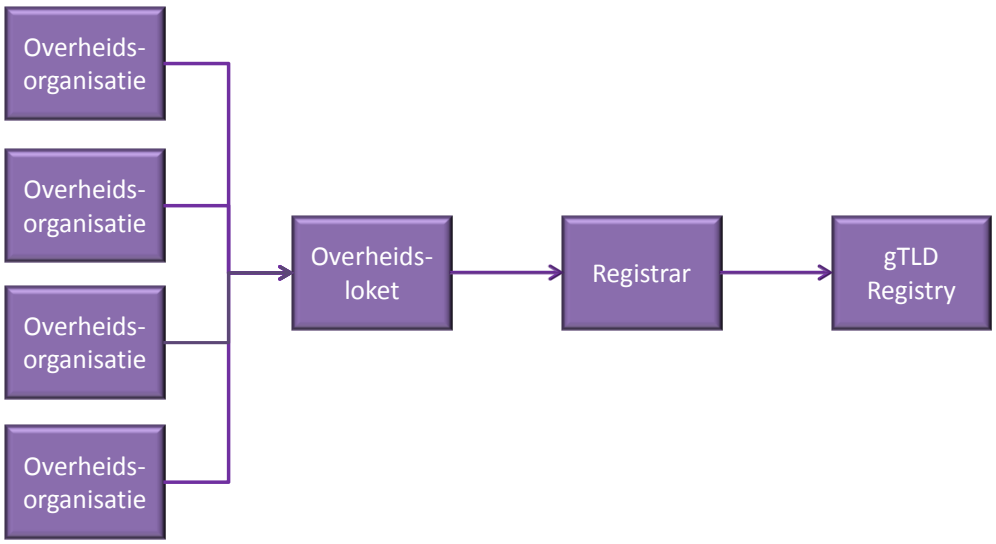
1. De huidige .nl situatie;
2. Een .overheid.nl second-level hiërarchie situatie.

Hierna volgt een korte beschrijving van de verschillende situaties, te beginnen met de gTLD situatie.

2.1.1 EEN OVERHEIDSEIGEN gTLD

Een overheidseigen gTLD geeft volledige controle over het inrichten en het beheer van het domein. Uit de aanvraag blijkt dat de overheid ervoor gekozen heeft om het .overheidnl gTLD toelaatbaar te maken voor alleen overheidsorganisaties (via bijvoorbeeld een centraal loket). Dit vergroot de controleerbaarheid ervan. Het ligt voor de hand om een enkele of een beperkt aantal registrars aan te wijzen voor het uitvoeren van de registraties. Dit neemt niet weg dat alle ICANN geaccrediteerde registrars gelijkelijk en zonder onderscheid toegang moeten krijgen als registrar voor ieder gTLD als ze dat aanvragen. Wel kan de gTLD eigenaar additionele eisen stellen aan bijvoorbeeld het registratieproces. Hierbij kan gedacht worden aan striktere beveiligingsmaatregelen aangaande de authenticatie van registrars. Daarnaast ligt het voor de hand dat SIDN de registry functie op zich neemt; het oprichten van een overheidseigen registry is niet realistisch (hoge kosten en vereist expertise). De nieuwe gTLDs zijn wel onderhavig aan ICANN toezicht en regelgeving. Zo is het o.a. verplicht om DNSSEC te gebruiken en mogen wijzigingen in de policy van het gTLD pas na toestemming van ICANN doorgevoerd worden.

De inrichting voor een gTLD situatie kan als volgt geschetst worden:



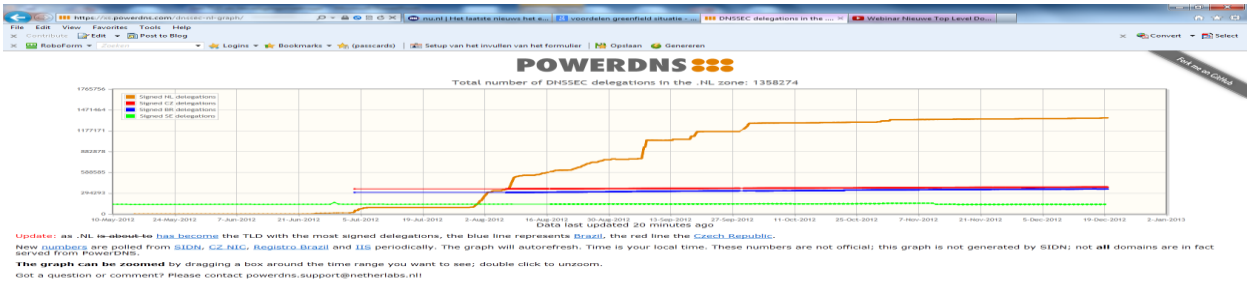
Figuur 1: Schematische weergave van een gTLD inrichting.

2.1.2 DE HUIDIGE .NL SITUATIE

Op dit moment zijn de meeste overheidsdomeinen geregistreerd onder het .nl domein dat door SIDN beheerd wordt. Er zijn momenteel ongeveer 3500 domeinnamen geregistreerd door de Rijksoverheid. Niet allemaal zijn ze in gebruik; de Rijksoverheid heeft ongeveer 700 websites. Een overzicht van deze websites is te vinden in het Websiteregister Rijksoverheid[2]. Hierin staat hoe ver de websites van de Rijksoverheid zijn met het invoeren van de webrichtlijnen en onder verantwoordelijkheid van welk departement een website behoort.

Het aantal domeinnamen dat door andere publieke en overheidsorganisaties (gemeenten, ZBO's) geregistreerd is zal vele malen groter zijn. De meeste domeinnamen zijn door een groot aantal verschillende commerciële registrars geregistreerd. Veel overheidsinstanties genieten de vrijheid om via elke willekeurige registrar een website te laten registreren (en hosten). Het Ministerie van Algemene Zaken is zelf ook registrar en registreert domeinnamen voor met name de Rijksoverheid. Niet alle overheidsdomeinen zijn onder .nl geregistreerd, er zijn er ook geregistreerd onder .eu, .org of .com.

Hoewel het .nl top-level domein DNSSEC beveiligd is en het aantal ondertekende .nl-domeinnamen explosief groeit (zie Figuur 2), zijn op dit moment nog niet alle daaronder hangende overheidswebsites DNSSEC beveiligd. Met de recente opname van de DNSSEC standaard in de zogenaamde 'pas toe of leg uit'-lijst zijn overheidsorganisaties verplicht deze veiligheidsstandaard te gebruiken. Alleen als zij goede redenen hebben om dat niet te doen, mogen zij daar van afwijken.



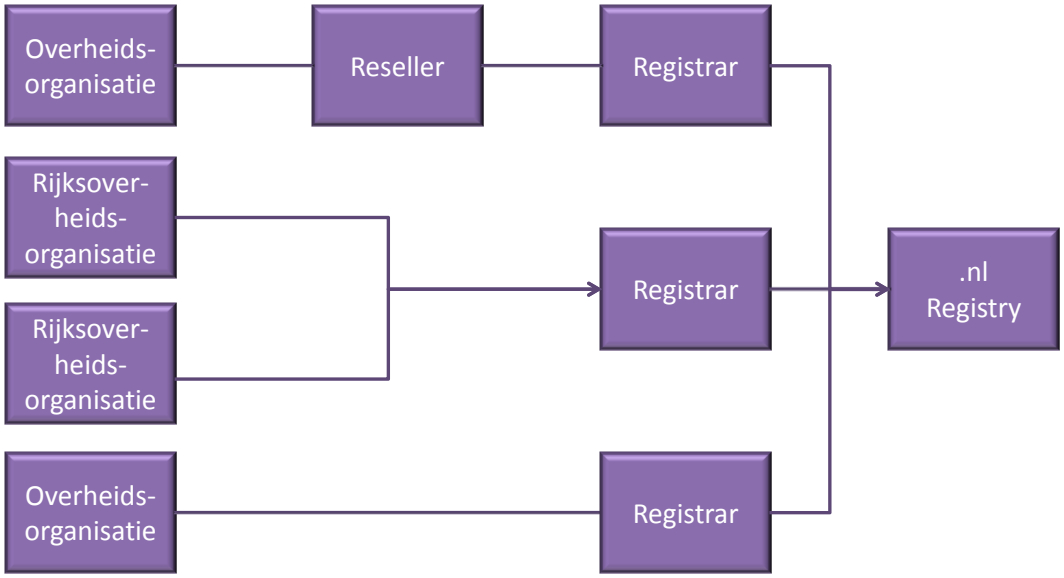
Figuur 2: .nl domein kent meest getekende delegaties (DNSSEC).

Om een beter overzicht van alle Rijksoverheidswebsites te krijgen is het Ministerie van Algemene Zaken begonnen met een opschoningsactie. Veel in ongebruik geraakte websites worden weggehaald en er vindt een consolidatie plaats van Rijksoverheidswebsites onder rijksoverheid.nl. Tegelijkertijd streven het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met AZ ernaar dat websites voldoen aan de webrichtlijnen en DNSSEC beveiligd zijn. Ook het gebruik van de webhosting platformen wordt in toenemende mate gestandaardiseerd; een twintigtal grote platformen hosten meer dan 90% van de websites.

[2] Webisteregister Rijksoverheid, zie http://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/documenten-en-publicaties/rapporten/2013/01/10/websiteregister-rijksoverheid.html.

Waar nog verbetering in zou kunnen komen is het aantal registrars dat namens de overheid een domeinnaam mag registreren. Een toekomstige, verbeterde .nl situatie voor de Nederlandse overheid is denkbaar waarin een klein aantal 'preferred' registrars opereren die dit mogen doen. Deze registrars hebben hun eigen IT-beveiliging zodanig op orde dat deze voldoet aan de eisen van de overheid. Denk hierbij ook aan de beveiliging van de systemen voor het registreren van domeinnamen. Hierover zullen afspraken gemaakt moeten worden met SIDN als registry beheerder.

Schematisch ziet de inrichting voor registratie en beheer van de huidige .nl situatie voor de overheid (in brede zin) er als volgt uit:

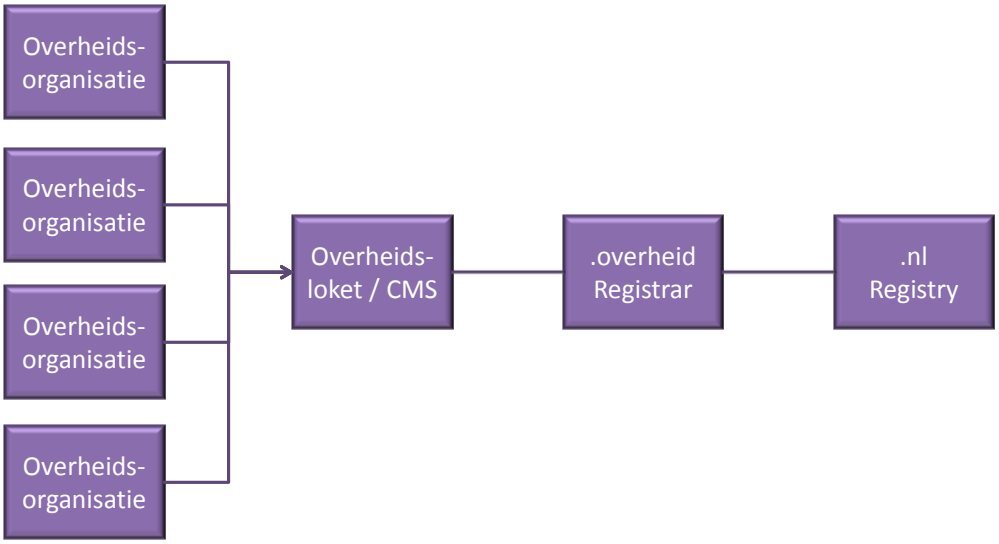


Figuur 3: Schematische inrichting van de .nl infrastructuur.

2.1.3 EEN .OVERHEID.NL SECOND-LEVEL HIERARCHIE SITUATIE

Analoog aan het Engelse model voor domeinnamen zou de Nederlandse overheid ook gebruik kunnen maken van een second-level hiërarchie. In dat geval vallen alle overheidswebsites onder .overheid.nl (of .gov.nl), zoals belastingdienst.overheid.nl en kadaster.overheid.nl. Het voordeel van deze constructie is dat het de Nederlandse overheid de volledige controle en vrijheid geeft over de inrichting van de DNS structuur onder het tweede niveau. Zij kan hiervoor bijvoorbeeld DNSSEC verplichten, kan toezien op de registraties en of deze voldoen aan naamgeving conventies en dergelijke.

De inrichting van een second-level hiërarchie situatie is geschetst in Figuur 4.



Figuur 4: Mogelijke inrichting van de .overheid.nl registratie en beheer infrastructuur.

Per deelaspect (beveiliging, communicatie, efficiëntie en kosten, maatschappelijke en bestuurlijke acceptatie, en uitvoerbaarheid) zullen nu de kansen en risico's worden geïnventariseerd van een gTLD t.o.v. de andere situaties.

2.2 BEVEILIGING

Soms komt de beveiliging onder druk te staan. Het recente DigiNotar incident, waarbij door valse certificaten de echtheid van websites ondermijnd werd, is hiervan een goed voorbeeld. Daarnaast blijft altijd de kans bestaan op website defacing[3], denial-of-service aanvallen[4], phishing mails[5], en domain squatting[6]. Kan een gTLD van meerwaarde zijn om de beveiliging van de overheidswebsites en email communicatie naar een hoger niveau te tillen?

Vanuit beveiligingsperspectief zijn de volgende kansen en risico's te identificeren.

2.2.1 KANSEN

2.2.1.1 WAARBORGEN VAN DE ECHTHEID VAN DE WEBSITES MET DNSSEC

Voor gebruikers is het belangrijk dat zij erop kunnen vertrouwen een bepaalde website daadwerkelijk van de overheid is en dat de data erop authentiek is. Ook voor open data is het wenselijk dat duidelijk is dat deze van de overheid komt.

Digitale certificaten worden gebruikt om de 'echtheid' van websites aan te tonen en om hiermee veilig te kunnen

[3] Zie bijvoorbeeld http://tweakers.net/nieuws/86893/anonymous-dreigt-overheidsgeheimen-openbaar-te-maken-na-defacen-ussc-punt-gov.html.
[4] Zie bijvoorbeeld http://www.tubantia.nl/algemeen/buitenland/hackers-leggen-zweedse-overheidssites-plat-1.2030660.
[5] Zie bijvoorbeeld http://www.rijksoverheid.nl/nieuws/2013/01/16/phishing-website-uit-de-lucht-gehaald-na-actie-belastingdienst.html.
[6] Domain- of cybersquatting is het registreren van een domeinnaam die identiek of gelijkaardig is aan een merk, handelsnaam, familienaam of elke andere benaming die iemand anders toebehoort, zonder zelf een legitiem recht of belang op deze benaming te hebben en met als doel schade toe te brengen aan een derde of er onrechtmatig voordeel uit te halen.

communiceren. Dergelijke certificaten worden uitgegeven door zogenaamde Certificate Authorities (CAs), die moeten fungeren als vertrouwde derde partijen. Het recente verleden heeft aangetoond dat de betrouwbaarheid van deze CAs, ondanks controle door auditors, in sommige gevallen te wensen overlaat[7]. De Diginotar hack leidde ertoe dat valse certificaten uitgegeven konden worden waardoor bezoekers van websites niet door hadden dat deze vals waren. Gegeven het feit dat in browsers momenteel certificaten opgeslagen worden van meer dan 150 CAs die voor willekeurige websites certificaten mogen ondertekenen is het bijna wachten op de volgende CA die gecompromitteerd raakt.

Alternatieve technieken zijn beschikbaar om de echtheid van websites op een meer gecontroleerde manier te vergroten zonder afhankelijk te zijn van alleen certificaten. Het inzetten van een gTLD is een oplossing die hiervoor nuttig kan zijn. Met een gTLD kan een eigen top level zone gecreëerd worden. Voor een gTLD wordt het gebruik van DNSSEC verplicht gesteld. DNSSEC is een uitbreiding op het DNS en verhelpt een aantal kwetsbaarheden in DNS waardoor de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. Dit doet DNSSEC door de DNS-informatie (de records) van een digitale handtekening te voorzien, zodat gecontroleerd kan worden of de inhoud authentiek is.

De authenticiteit van deze records kan gecontroleerd worden met behulp van de publieke sleutel voor dit domein. De hash ervan, het zogenaamde DS-record, wordt door de houder (via zijn registrar) één niveau hoger in de DNS-hiërarchie geplaatst (het zogenaamde trust anchor). Voor bijvoorbeeld rdw.overheidnl staat de hash van de publieke sleutel dus op de name-servers van de beheerder van het overheidnl gTLD. Daarmee kan geverifieerd worden dat de publieke sleutel die hij bij de adres-informatie van de name-server ontvangt inderdaad dezelfde is als die door de houder of beheerder van de domeinnaam bij het trust anchor is aangemeld. Zo wordt een 'keten van vertrouwen' (chain of trust) over de verschillende niveaus tot aan de root van de DNS-hiërarchie opgebouwd.

In vergelijking met de andere situaties valt deze gTLD kans als volgt te positioneren:

- Huidige .nl situatie: Bij een gTLD is de DNS keten voor de overheid in vergelijking met de huidige .nl structuur iets korter waardoor het resolven van domeinnamen marginaal sneller zal zijn en er voor een hacker één aanvalsvector minder is. Ondanks dat ook .nl DNSSEC beveiligd is, maken nog lang niet alle overheidswebsites hier gebruik van. De opname van DNSSEC op de lijst van standaarden voor de Nederlandse overheid verplicht partijen wel om hier gebruik van te maken wat de meerwaarde van een gTLD marginaal maakt.
- .overheid.nl situatie: Hier is sprake van een toename van de DNS keten waardoor de chain of trust langer is en het resolven van domeinnamen marginaal langzamer zal zijn. Daarnaast wordt er een extra aanvalsvector geïntroduceerd. Met het feit dat .nl DNSSEC heeft, valt met de uitrol van DNSSEC voor .overheid.nl nagenoeg precies hetzelfde te bereiken als met een eigen gTLD. Met het plaatsen van DNSSEC op de pas-toe-of-leg-uit lijst is het gebruik van DNSSEC onder .overheid.nl eenvoudig af te dwingen.

[7] Het eindrapport van Fox-IT over de DigiNotar hack, zie http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html.

2.2.1.2 TOEVOEGEN VAN ADDITIONELE BEVEILIGINGSMAATREGELEN

De beschikbaarheid van een DNSSEC-beveiligd gTLD biedt mogelijkheden voor het toevoegen van additionele maatregelen die de beveiliging verder vergroten. DANE, ofwel DNS-based Authentication of Named Entities, is een dergelijke maatregel. DANE bouwt verder op de cryptografisch beveiligde DNS-infrastructuur die met DNSSEC wordt aangelegd. DANE biedt een oplossing voor de meer dan 150 CAs waarop de browser moet vertrouwen voor het opzetten van een veilige verbinding (https) door informatie over certificaten in het DNS te plaatsen[8]. Bijvoorbeeld, informatie over het certificaat voor www.belastingdienst.overheidnl wordt opgenomen in de zone "belastingdienst.overheidnl". Met deze door DNSSEC beveiligde certificaatinformatie kan, nadat ze uit het DNS gehaald is, het certificaat dat gebruikt is voor een veilige en betrouwbare verbinding, gevalideerd worden. De hiervoor gebruikte certificaten en bijbehorende informatie hoeven niet noodzakelijkerwijs door de overheid (PKIoverheid certificaten) of door CAs uitgegeven te zijn, maar mogen ook door de organisatie achter de domeinnaam zelf gecreëerd worden. In dat geval is er sprake van een self-signed certificaat. Via DNSSEC wordt geborgd dat een self-signed certificaat daadwerkelijk bijeen domeinnaam/website hoort. Vanuit beveiligingsoogpunt is de meerwaarde van het gebruik van self-signed certificaten echter minimaal omdat DNSSEC net als de huidige CA infrastructuur ook een PKI is met zijn eigen kwetsbaarheden in het registrant-registrar-registry pad. Het geniet daarom de voorkeur om voor DANE CA-certificaten te gebruiken omdat het validatie van betrouwbaarheid via twee onafhankelijke paden mogelijk maakt.

De IETF DANE specificatie beschrijft o.a. de risico's van sleutelcompromittering en impact bij DANE en vergelijkt deze met het huidige publieke CA model[9]. Hierbij valt op dat DANE in combinatie met DNSSEC t.o.v. de CA aanpak meer flexibiliteit en fijnmazigheid biedt om e.e.a. te herstellen.

Een andere nuttige toepassing van DANE die bruikbaar is in een gTLD situatie is certificate pinning. Bij certificate pinning wordt aangegeven welke certificaat-autoriteiten certificaten voor een bepaald domein uitgeven. Dit was ook de manier waarop de DigiNotar-hack werd ontdekt: een Iraanse Gmail-gebruiker kreeg een waarschuwing van Chrome, omdat een website die zichzelf als Gmail presenteerde een DigiNotar-certificaat meestuurde om dat te 'bewijzen'. DigiNotar mocht van Chrome echter helemaal geen certificaten voor Gmail uitgeven. Op dit moment werkt certificate pinning enkel nog met Google-websites en alleen via Google Chrome. Of de functionaliteit kan uitgroeien tot een algemeen inzetbare veiligheidsmaatregel, is onzeker. Op dit moment zijn de certificate pins hardcoded, dus elke nieuwe 'pin' moet aan de broncode van Chrome worden toegevoegd. Dat is niet erg schaalbaar en maakt een overstap op een andere certificaat-autoriteit omslachtig. Met een technologie als DANE is dit proces te automatiseren. Het blijft wel een lapmiddel. Een efficiëntere techniek heet 'stapling' en maakt het mogelijk voor een browser om de echtheid van een certificaat tegen een DANE TLSA record in de zone te controleren. Daarmee verwijst het certificaat dus naar een domeinnaam en de domeinnaam naar het certificaat. Hieraan wordt momenteel gewerkt binnen de IETF[10].

[8] Met DANE had het DigiNotar debacle waarschijnlijk veel minder gevolgen gehad voor de overheidsdienstverlening.
[9] The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA specificatie, zie http://tools.ietf.org/html/draft-ietf-dane-protocol-23.
[10] Zie http://tools.ietf.org/html/draft-ietf-tls-multiple-cert-status-extension-03/

Een andere technologie die profiteert van een DNSSEC-beveiligd gTLD is betrouwbare e-mail uitwisseling via Domain Keys Identified Mail (DKIM). DKIM is onlangs door het Forum Standaardisatie op de pas-toe-of-leg-uit lijst gezet[11]. Ontvangende mailservers controleren de authenticiteit van een e-mail op basis van een DKIM handtekening die gezet is met een sleutel uit het DNS van de betreffende verzender. Door DKIM te gebruiken kan spam bestreden worden en weet de ontvanger altijd vanuit welk domein de mail verzonden is. Bedrijven en burgers kunnen zodoende veiliger met overheidsinstanties en ambtenaren communiceren.

Voor het gebruik van DANE dienen een aantal kanttekeningen gemaakt te worden: de technologie is nog volop in ontwikkeling en er is op dit moment nog geen browser die DANE ondersteund. Wel zijn er enkele plugins beschikbaar en zijn makers als Google en Mozilla bezig dit in te bouwen in hun browsers[12]. De verwachting is wel dat het nog wel enkele jaren zal duren voordat een technologie als DANE gemeengoed is. Voorwaarde daarbij is dat DNSSEC breed in gebruik is. DKIM daarentegen wordt al door verschillende grote mail-verzenders, commerciële dienstverleners en ISPs gebruikt[13].

In vergelijking met de andere situaties valt deze gTLD kans als volgt te positioneren:

- Huidige .nl situatie: Aanvullende beveiligingstechnologieën als DANE en DKIM kunnen even goed in een gTLD als in de huidige .nl situatie gebruikt worden mits DNSSEC aanwezig is. Dit laatste is nog niet het geval voor alle overheidswebsites. Een aandachtspunt is dat het met DNSSEC en DANE eenvoudig een beveiligde webserver op te zetten is voor valse domeinen. Gecombineerd met typosquatting kan dit erg misleidend zijn voor de gebruiker. Bijvoorbeeld, de houder van de valse overheidssite overhijd.nl kan eenvoudig zijn eigen DANE certificaat op zijn eigen name-server valideren en daarmee richting de gebruiker aantonen dat het veilig is. Met een gTLD zal dat minder eenvoudig te realiseren zijn omdat niet iedereen zomaar een subdomein onder .overheidnl kan aanvragen (zie verder sectie 2.2.1.5 over typosquatting). De meerwaarde van een gTLD bij DKIM is dat sleutel op het hoogste niveau geplaatst kan worden en alle onderliggende domeinen hiervan kunnen profiteren. Voor de .nl situatie is dat anders omdat in dat geval elke overheidsorganisatie zijn eigen DKIM beheer zal moeten uitvoeren wat minder efficiënt is.
- .overheid.nl situatie: Ook hier geldt dat er geen meerwaarde is voor DANE t.o.v. de gTLD situatie. DKIM sleutelbeheer kan vanuit het overheidsniveau in DNS centraal gecoördineerd worden waarmee het efficiënter kan werken dan in de andere situaties.

2.2.1.3 CONTROLE OVER REGISTRANTS, REGISTRARS EN REGISTRY

Een gTLD biedt aan de houder meer controle over de registratie van domeinen door registrars. Het registreren van domeinen onder .nl kan bij meer dan 1500 registrars die bij SIDN zijn aangesloten[14]. Dergelijke registrars zijn meestal commerciële organisaties die naast het registreren van domeinnamen ook andere diensten als website design en hosting verlenen. Met name lagere overheden (gemeenten) maken gebruik van en zijn dus afhankelijk van

[11] Zie http://www.forumstandaardisatie.nl/actueel/item/titel/dnssec-dkim-sikb-en-visi-op-pas-toe-of-leg-uit-lijst/.
[12] Zie bijvoorbeeld http://www.imperialviolet.org/2011/06/16/dnssecchrome.html.
[13] Zie http://www.dkim.nl/nl/gebruik.
[14] Zie https://www.sidn.nl/nc/over-nl/registrar-zoeken/registrars-alfabetisch.

zulke commerciële registrars. Er zijn ook overheidsdiensten onder bijvoorbeeld .org, .net, .info, .nu, .cz en .es waarmee het om nog veel meer registrars gaat met een bijbehorende veel grotere variëteit aan beleid (ook internationaal). Sommige overheidsorganisaties zijn daarentegen zelf registrar zoals de Belastingdienst/Centrum voor Infrastructuur en Exploitatie en het Ministerie van Algemene Zaken (Dienst Publieke Communicatie).

Voor een gesloten gTLD als .overheidnl mag slechts de overheid als houder nieuwe domeinen aanvragen, en deze kan ervoor kiezen om dit bij een beperkt aantal registrars te doen die het vertrouwen van de overheid genieten. Deze publieke of commerciële registrars dienen geaccrediteerd te zijn door ICANN[15] en kunnen onder een stringenter (dan SIDN nu voor .nl doet) beleid nieuwe domeinnamen aanvragen onder .overheidnl voor overheidsinstanties (de zogenaamde registrants). De gTLD houder staat het vrij om additionele eisen stellen aan de registrar betreffende bijvoorbeeld de operationele beveiliging van het registratieproces. Dergelijke eisen worden vastgelegd in de registry-registrar overeenkomst. Er dus meer controle over het aantal registrars en de aansturing ervan (zie verder sectie 2.6.1.2). Vanuit continuïteitsoverwegingen is het niet verstandig om te opteren voor één registrar. Hiermee wordt een single-point-of-failure geïntroduceerd.

Wel bestaat de kans dat, indien er geopteerd wordt voor een beperkt aantal geselecteerde commerciële registrars, het marktverstorend kan werken. Dergelijke registrars zullen door andere registrants als betrouwbaarder ervaren worden en de voorkeur genieten ten opzichte van partijen die niet namens de overheid mogen registreren. Gezien het grote aantal domeinnamen dat de overheid afneemt, zal het selectieproces waarschijnlijk aanbesteed moeten worden. Met de keuze voor publieke, overheidseigen registrars vallen een marktverstoring en aanbesteding te voorkomen.

Daarnaast is de overheid als houder van een gTLD vrij een van de (beste) bestaande registries te kiezen of zelf een eigen registry te beginnen (mits deze ICANN geaccrediteerd is). Dat laatste is vanuit het oogpunt van kosten en benodigde expertise een weinig realistisch scenario. ICANN kan wel de contractuele registry ‘laten’ vervangen. De vervangende registry mag ook niet zonder meer zelf gekozen worden, maar moet worden goedgekeurd door ICANN (zie verder ook sectie 2.6.2.3).

Ten opzichte van de andere situaties vallen de volgende zaken op:

- Huidige .nl situatie: In de huidige situatie heeft de overheid via veel verschillende registrars domeinen aangevraagd[16]. Ondanks het feit dat het Ministerie van Algemene Zaken zelf een registrar is, maken relatief veel overheidspartijen en publieke organisaties gebruik van een commerciële registrar (voor lagere overheden is dit vaak de hosting provider)[17]. Onduidelijk is hoe deze laatste registrars de beveiliging hebben ingericht. Kijkende naar het relatief grote aantal registrars, is de kans relatief groot dat er bij een van hen iets fout kan gaan wat schadelijk kan zijn voor de overheid. Daar komt bij dat met het verplaatsen van

[15] Pagina 24 van het ICANN Applicant Guidebook, zie http://newgtlds.icann.org/en/applicants/agb.
[16] Zie http://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/documenten-en-publicaties/rapporten/2012/07/12/websiteregister-rijksoverheid.html.
[17] Een inventarisatie, via de SIDN Whois dienst, van de registrars van domeinnamen behorende bij de Rijksoverheid of lagere overheden wijst uit dat de laatstgenoemden voornamelijk gebruik maken van commerciële registrars.

beveiligingsfunctionaliteit naar DNS (met DNSSEC en DANE) dergelijke partijen een kritiekere rol gaan innemen en het is nog maar de vraag of ze dat kunnen. Immers, DNSSEC sleutel- en DANE certificaatmanagement zijn over het algemeen geen kernspecialisaties van registrars. Met een gTLD is het aantal registrars eenvoudiger te beperken tot bij voorkeur kleine set van gespecialiseerde partijen. Met een goede beveiliging van deze registrar zijn de risico's op een incident kleiner dan in de huidige situatie.
Deze situatie zou verbeterd kunnen worden door het aantal registrars dat voor de overheid een domein kan aanvragen te beperken. Hierover zullen afspraken met de registry gemaakt moeten worden. De registry voor .nl kan bijvoorbeeld de registrar van het Ministerie van Algemene Zaken en overige registrars een bijzondere status geven en een aangescherpt toelatingsbeleid faciliteren. Dit laatste bestaat bijvoorbeeld uit het eisen van sterke authenticatie voor het registreren van domeinen of het uitvoeren van een DNSSEC key roll-over (zie verder hieronder). De meerwaarde van een gTLD voor deze kans en ten opzichte van deze verbeterde situatie is dus minimaal.

- .overheid.nl situatie: Ook hiervoor geldt dat de overheid zelf kan bepalen wie onder het second-level domein namen kan/mag registreren. Er hoeven geen afspraken met SIDN gemaakt te worden. Ook hier is de meerwaarde van een gTLD dus marginaal.

2.2.1.4 VEILIGERE REGISTRATIE EN BEHEER

Bij gebruik van DNSSEC ontvangt de web browser via het DNS adres-informatie waarvan de digitale handtekening is gevalideerd[18]. De authenticiteit van deze informatie kan gecontroleerd worden met behulp van de publieke sleutel voor dit domein. Deze wordt door de houder (via zijn registrar) één niveau hoger in de DNS-hiërarchie geplaatst (het zogenaamde trust anchor). Voor een .nl-domeinnaam staat de publieke sleutel in het registratiesysteem van SIDN en wordt er een verwijzing naar de sleutel gepubliceerd in de .nl zone.

Het trust anchor is cruciaal voor de betrouwbaarheid van het bijbehorende domein. Het is daarom van groot belang dat niet geautoriseerde derden (bv. aanvallers) in staat zijn om het trust anchor te vervangen of een ander trust anchor toe te voegen. Om dit te kunnen waarborgen dient het kanaal voor het wijzigen van het trust anchor goed beveiligd te worden. Dit kanaal loopt van registrant via de registrar naar de registry. Bij alle betrokken partijen moeten maatregelen getroffen worden om de veiligheid te garanderen. Het verdient aanbeveling om bij het inrichten van de beveiliging van dit kanaal gebruik te maken van internationale standaarden op het gebied van informatiebeveiliging (denk aan FIPS 140, diverse NIST standaarden en ISO 27001), en bovendien regelmatig de implementatie en handhaving van het beveiligingsbeleid door een externe partij (auditor) te laten toetsen.

In een gTLD situatie kan de eigenaar specifieke eisen stellen aan de registrars betreffende de beveiliging van de registratie van domeinen. Hierbij dient specifiek gedacht te worden aan strengere beveiligingsmaatregelen voor het verkrijgen van toegang tot registratiesystemen bij de registry door de registrars zoals sterke (twee-factor) authenticatie. Vooral wanneer de beveiliging zich steeds meer verplaatst naar het DNS (met DNSSEC sleutels en DANE certificaten) is het van belang dat de toegang tot de registratiesystemen en de omgevingen voor DNSSEC

[18] Het komt zelden voor dat de digitale handtekening door de browser (eindclient) gevalideerd wordt. Meestal vindt validatie plaats op de recursive caching name server waar de browser (eindclient) gebruik van maakt.

sleutelmanagement en DANE certificaatmanagement goed beveiligd zijn. Voorwaarde is wel dat de registry de registrars als zijnde van de overheid of namens de overheid opererend kan authenticeren. Een goed ingericht proces voor identificatie en registratie van gebruikers is hiervoor noodzakelijk.

In vergelijking met de andere situaties valt deze gTLD kans als volgt te positioneren:

- Huidige .nl situatie: SIDN is als registry voor .nl een betrouwbaar trust anchor voor DNSSEC. Bij .nl kunnen meer dan 1500 registrars domeinen aanmaken via specifieke registratie-omgevingen. In tegenstelling tot de gTLD situatie zijn in deze situatie de processen om dit op een veilige manier te doen veel minder goed controleerbaar. De huidige beveiliging van de registratie is gebaseerd op een 'full-blown' implementatie die bij wereldwijd gebruik door alle registrars stand houdt en door ICANN zo is opgezet en wordt geregisseerd. Echter, met de toevoeging van additionele beveiligingsmaatregelen als DNSSEC en mogelijk DANE certificaten is het wenselijk dat ook beveiliging van de registratie navenant is. Hiervoor schiet bijvoorbeeld de huidige op gebruikersnaam en wachtwoord en IP-whitelisting gebaseerde toegang tot registraties-omgevingen tekort. Sterkere oplossingen als twee-factor authenticatie genieten dan de voorkeur. Bij een gesloten gTLD is dit relatief eenvoudig af te dwingen en in te richten. Met andere woorden, DNSSEC en DANE zijn controleerbaarder te beveiligen met een gTLD dan in de huidige situatie. Verschillende registries (Nominet, SIDN[19]) maken gebruik van een zogenaamde 'registrar lock' om meer controle te krijgen over het registratieproces. Dat betekent dat veranderingen pas doorgevoerd worden nadat is nagebeld met de betreffende eigenaar. Bijvoorbeeld als er wat veranderd wordt in www.google.co.uk dan wordt er eerst met Google gebeld of dat wel in orde is. Een dergelijke lock is verplicht voor alle gTLDs. SIDN denkt ook na over een verbeterde versie van hun oplossing om ook domain-hijacking te kunnen belemmeren. Het beveiligen van de registratie en het beheer is in deze situatie iets lastiger te regelen maar niet onoverkomelijk. Met SIDN zou afgesproken kunnen worden dat registrars die namens de overheid domeinen mogen aanvragen zich met sterke authenticatie oplossingen moeten authenticeren. Ook hier dient SIDN te controleren dat de registrar namens de overheid mag handelen.
- .overheid.nl situatie: Ook in deze situatie is de overheid in control wie mag registreren en kan daarbij ook eisen stellen aan de beveiliging van de registratie. Het zelfde geldt voor de beveiliging van de toegang tot de DNSSEC en DANE beheersystemen. Wel dienen processen als 'registrar lock' zelf geïmplementeerd en uitgevoerd te worden door de overheid.

2.2.1.5 MINDER LAST VAN TYPOSQUATTING

Typosquatting is een vorm van misbruik van het internet gebaseerd op het feit dat mensen zich wel eens vergissen bij het intypen van een websiteadres. De typosquatter zet een website op, waarvan het adres (domeinnaam) slechts heel weinig verschilt van het adres van een populaire website. Alle internetgebruikers die dezelfde tikfout of vergissing maken, komen terecht op de website van de typosquatter. Typosquatting wordt gebruikt om bezoekers te trekken naar een malafide site om daar geld mee te verdienen, om bezoekers van een concurrent te lokken, bijvoorbeeld naar een zoekmachine, veilingsite of een webwinkel, om mensen toegangscodes of creditcard-

[19] De dienstverlening van SIDN hieromtrent heet ".nl Control". Meer informatie is terug te vinden op de afgeschermde registrar omgeving (https://www.sidn.nl/registrars/nl-registratie/nl-control/).

gegevens te ontfutselen door de website van een populaire website van een bank of internetwinkel na te bootsen, voor het verspreiden van computervirussen, adware, spyware en dergelijke, of om de originele website of een persoon te bespotten.

Ook het kapen van een domeinnaam is mogelijk. In 2000 bijvoorbeeld moest het bedrijf De Digitale Advocaat de domeinen ‘regering.nl’, ‘miljoenennota.nl’, ‘troonrede.nl’ en ‘prinsjesdag.nl’ afstaan aan de Staat. De rechter oordeelde hiertoe omdat:

- het gebruik van deze domeinnamen door een particulier verwarring schept, omdat bezoekers van de site verwachten informatie van de regering aan te treffen;
- de overheid wordt belemmerd om via internet de burgers te informeren;
- met de toewijzing door de SIDN rechtmatig gebruik nog niet vaststaat en hieraan geen rechten ontleend kunnen worden.

Domeinnamen die evident bij de overheid behoren, zijn via de rechter dus terug te krijgen. Daarnaast blijft er altijd een grijs gebied in de huidige situatie (denk daarbij aan domeinnamen als www.kadasterdata.nl) waarbij het niet duidelijk is of het een overheid of private website betreft. Een overheidseigen gTLD biedt hier uitsluitsel. De burger kan in de gTLD redelijk snel herkennen dat hij te maken heeft met een overheidswebsite.

Typosquatting en domeinkaping zijn goede redenen om een eigen gTLD te voeren. Het wordt veel duurder en omslachtiger om bijvoorbeeld de gTLD overheitnl aan te vragen voor typosquatting doeleinden. ICANN zal hier waarschijnlijk op basis van het gelijkheidscriterium ook geen toestemming voor geven. Wel blijft de mogelijkheid bestaan om bijvoorbeeld onder andere (g)TLDs een domein te claimen dat lijkt op een Nederlandse overheidsorganisatie. Denk hierbij aan svb.bank (zie verder ook sectie 2.3 over communicatie).

Waar ook rekening mee gehouden dient te worden is het risico op typosquatting via subdomeinen onder verschillende TLDs. Voor ieder subdomein onder .overheidnl is het wenselijk om ook het bijbehorende subdomein onder .nl en overheid.nl aan te vragen om typosquatting risico’s af te vangen. Dus naast belasting.overheidnl zullen ook belasting.overheid.nl (die via overheid.nl al is afgeschermd) en belasting.nl moeten worden aangevraagd. Deze zullen geregistreerd moeten blijven door de overheid anders zullen ze door anderen geregistreerd worden en vormen ze zelf een bron voor typosquatting. Hiermee wordt het huidige typosquatting probleem niet opgelost.

Een interessant aspect is de automatische aanvul functionaliteit van sommige browsers. Bijvoorbeeld Chrome vult automatisch een URL aan met .com waardoor .overheidnl al snel verwordt tot overheidnl.com. In deze context is het in ieder geval verstandig om overheidnl.nl en overheidnl.com te vergaren.

Kijkende naar de andere situaties biedt deze kans in meer of mindere mate een meerwaarde:

- Huidige .nl situatie: Hier zal typosquatting onverminderd doorgaan. Het is voor een burger minder eenvoudig om het herkennen dat het een website van een overheidsorganisatie betreft. Wetgeving geeft voldoende mogelijkheden om hier via juridische wegen paal en perk aan te stellen.
- .overheid.nl situatie: In deze situatie worden de mogelijkheden voor typosquatting beperkt door de specifieke hiërarchie. Alleen varianten op ‘overheid’ zijn mogelijk voor squatters (overhijd, overheit,

overhijd). Deze beperkte set van typosquatting varianten dient geregistreerd te worden of hier dient goed op worden toegezien, zodat eventuele squatters snel tot de orde geroepen kunnen worden. De herkenbaarheid is er voor de burger ook voor deze situatie door een volledige migratie van de huidige domeinnamen naar domeinen onder overheid.nl door te voeren.

2.2.2 RISICO'S

2.2.2.1 TOENEMENDE COMPLEXITEIT EN EXPERTISE

DNSSEC is verplicht bij een gTLD. Met het gebruik van DNSSEC neemt ook de complexiteit van het beheer van domeinen toe. De praktijk wijst uit dat DNSSEC erg foutgevoelig is en dat wanneer er iets fout gaat, dit minder snel te repareren is. Websites zijn daardoor relatief lang offline. De mogelijke introductie van DANE maakt dit nog urgenter omdat fouten in de configuratie (bijvoorbeeld door certificaten waarvan de geldigheid verlopen is) tot niet-bereikbaarheid kunnen leiden. De toenemende complexiteit en de grotere verantwoordelijkheid van het beheren van DNSSEC keys op TLD niveau (denk aan zaken als key storage, roulatie, key ceremonies, publicatie van de policy en procedures) vereist expertise. Experts op het gebied van DNSSEC beveiliging zijn nodig. Het is de vraag of de benodigde expertise overheidsbreed aanwezig is.

Ten opzichte van de andere situaties is dit risico in meer of mindere mate aanwezig:

- Huidige .nl situatie: Op dit moment is slechts een deel van de overheidsdomeinen DNSSEC beveiligd. Veel domeinen zijn recentelijk overgegaan en het gebruik van DNSSEC is dus nog relatief nieuw. Er zijn gevallen bekend waarbij een overheidswebsite offline is geweest door problemen met DNSSEC.
- .overheid.nl situatie: Ook hier geldt dat er door een gebrek aan DNSSEC expertise risico's kunnen ontstaan voor de beschikbaarheid van overheidswebsites. Daar komt bij dat door de langere trust chain er een grotere kans op fouten is.

2.2.2.2 BROWSER BLIJFT DE ZWAKSTE SCHAKEL

Het hele systeem is zo veilig als de zwakste schakel. Op dit moment is de browser nog steeds het meest kwetsbare onderdeel en dat lossen ook DNSSEC of een gTLD niet op. Is een PC bijvoorbeeld besmet met malware, dan zijn meestal ook de resolver (het onderdeel van het besturingssysteem op de PC dat verantwoordelijk is voor de vertaling van domeinnamen naar IP-adressen) en de lokale cache te manipuleren waardoor de gebruiker nog steeds te misleiden is. Voor alle situaties is dit een risico. Het is echter geen argument om niet andere zwakke schakels aan te pakken. Belangrijk is dat er geen "false sense of security" ontstaat met een gTLD (inclusief DNSSEC en DANE).

Het recente verleden heeft laten zien dat populaire browsers niet altijd even goed omgaan met nieuwe TLDs; het duurde verschillende maanden voordat de browsers nieuwe TLD als .cz en .post herkenden[20]. Hier dient rekening mee gehouden te worden bij het in gebruik nemen van een gTLD.

2.2.2.3 CONTRACTUELE VERPLICHTINGEN / BEPERKINGEN

Het contract tussen een domeinhouder en .nl is anders dan het contract tussen een gTLD domeinhouder en ICANN.

[20] Zie http://domainincite.com/11673-apple-google-and-microsoft-still-dont-understand-new-tlds.

Dit laatste contract wordt gekenmerkt door zijn dikte. Onderdeel van dat contract is dat een gTLD eigenaar alle data onderbrengt bij een derde partij om ervoor te zorgen dat als de domeineigenaar failliet gaat, de domeinen eronder hierdoor niet getroffen worden, er is dan een backup (data escrow). De vraag is of het wenselijk is dat alle overheidsdata bij een derde partij ligt.

Conform de contractuele afspraken zullen bepaalde procedures gevolgd dienen te worden. Dit kan resulteren in een bepaalde starheid van het gTLD. Als bijvoorbeeld bij overheid.nl iets veranderd moet worden, dan kan SIDN dat direct doorvoeren in het registratiesysteem[21]. Voor wijzigingen in een gTLD is dit minder triviaal: verschillende partijen zullen ernaar moeten kijken (IANA, NTIA, Verisign, ICANN) voordat veranderingen doorgevoerd kunnen worden. Dat kost minimaal 4 à 5 dagen, en dat is, als de gTLD DNS-servers onder een (denial of service) aanval liggen en er extra servers bijgeschakeld moeten worden, lang. Hier geldt dat voorkomen beter is dan genezen en er van tevoren goed gekeken moet worden welke server capaciteit nodig is om dergelijke aanvallen aan te kunnen.

In deze context geldt het volgende voor de andere situaties:

- Huidige .nl situatie: Hier zijn veel minder contractuele verplichtingen en is er meer flexibiliteit. Wel is er een afhankelijkheid van de robuustheid van .nl maar deze is zeer goed gebleken de afgelopen jaren.
- .overheid.nl situatie: Een manier om meer flexibiliteit te creëren is door een tweede niveau te introduceren onder het .nl ccTLD voor landcodes. Een dergelijk secondlevel domein is te zien in Groot Brittannië waarbij academische instituten geregistreerd worden als .ac.uk, bedrijven onder .co.uk en non-gouvernementele organisaties onder .org.uk. Het voordeel hiervan is dat veranderingen onder .uk relatief snel doorgevoerd kunnen worden (zonder toestemming aan ICANN te vragen). Dit model heeft ook nadelen: het resulteert in langere namen, het introduceert meer typefouten (ongeveer 7% van de bezoekers vergeet bijvoorbeeld om .co of .gov ertussen te zetten en gaan direct naar .uk[22]), partijen moeten soms namen dubbel registreren en het brengt extra kosten met zich mee. Nominet, de registry voor .uk in Engeland, onderzoekt momenteel of het huidige model wel het beste is. Overigens is .gov.nl volgens de Whois service van SIDN al voor de overheid gereserveerd door het Ministerie van Algemene Zaken[23].

2.3 COMMUNICATIE

Een gTLD brengt voor gebruikers mogelijk meer helderheid in de online aanwezigheid van de Nederlandse overheid inclusief decentrale overheden en andere organisaties met een publieke taak. Het is in de huidige situatie voor de burger of een bedrijf niet altijd duidelijk of ze te maken heeft met een overheidsorganisatie. Met een overheids-gTLD kan een burger bijvoorbeeld in een oogopslag zien dat www.kadaster.overheidNL (is nu www.kadaster.nl) een overheidswebsite is en het commerciële www.kadasterdata.nl niet. Iets dat bijvoorbeeld met de komst van steeds meer op open data gebaseerde diensten een sterk toenemende behoefte kan worden. Het zelfde geldt in potentie voor portalen voor dienstverlening richting de burger en/of bedrijfsleven. Dit neemt niet weg dat het ook voor kadaster.overheid.nl of overheid.nl/kadaster herkenbaar voor de burger kunnen zijn als overheidsdomeinen.

[21] Eventuele DNS wijzigingen worden maximaal binnen 2 uur in de zonefile verwerkt.
[22] Uit het interviewgesprek met Nominet.
[23] Zie de online Whois service van SIDN: https://www.sidn.nl/nc/over-nl/whois/.

Er is enige gelijkenis met de introductie van de eigen huisstijl van de Rijksoverheid, welke naast een verbeterde herkenbaarheid ook van meerwaarde is om misleiding en misbruik (beeldrecht) te voorkomen.

De volgende communicatieve kansen en risico's zijn geïdentificeerd.

2.3.1 KANSEN

Voor het bedrijfsleven worden de nodige communicatieve kansen van een eigen gTLD gepropageerd. Typische voorbeelden zijn:

- Merkuitbreiding: door domeinnamen op het tweede niveau aan gewaardeerde partners en wederverkopers te verstrekken, kunnen bedrijven het aanzien en vertrouwen van hun merken uitbreiden. Hiermee worden zakenrelaties versterkt, waardoor nieuwe joint-marketingmogelijkheden worden gecreëerd en nieuwe doelgroepen worden bereikt.
- Klanten- en merkbinding: Bedrijven kunnen eigen e-mailadressen aanbieden, waarmee consumenten zich op een totaal nieuwe manier aan hun favoriete merk kunnen associëren. Hiermee worden marketingmogelijkheden uitgebreid en nieuwe inkomstenstromen gecreëerd.

Hoewel deze kansen niet direct van toepassing zijn voor de overheid, biedt een gTLD op communicatief gebied zeker kansen.

2.3.1.1 VERSTERKING OVERHEIDSIMAGO

Een gTLD kan, net als de eigen huisstijl van de Rijksoverheid, als imago-versterkend keurmerk worden gepositioneerd waar dan allerlei veiligheidsstatements vanuit kunnen stralen, mits goed en realistisch ingevoerd. Gewaakt dient wel te worden niet te ver door te slaan en – zoals al eerder aangegeven – geen 'false sense of security' te creëren.

Over de andere situaties kan het volgende gezegd worden:

- Huidige .nl situatie: Ondanks het feit dat .nl een goede reputatie geniet onder burgers, is de overheidsreputatie daar minder zichtbaar. Wel zijn er sterke merknamen als belastingdienst.nl waarmee geconcurreerd zal moeten worden bij de introductie van een overheids-gTLD.
- .overheid.nl situatie: Deze situatie leent zich er ook voor om het overheidsimago te versterken.

2.3.1.2 AANDACHTTREKKENDE GEBEURTENIS

De invoering van een gTLD is een aandachtrekkende gebeurtenis op zich. In het specifieke geval van .overheidnl leent de situatie zich uitstekend voor een veiligheidscampagne. De 'brand-name' van het gTLD kan daarmee gevestigd worden.

Het voeren van een campagne voor de huidige .nl situatie heeft weinig zin omdat er weinig zichtbaars verandert voor de burger en het bedrijfsleven. In de .overheid.nl situatie kan een campagne wel meerwaarde hebben. De burger kan dan gewezen worden op het feit dat alle overheidsorganisaties onder .overheid.nl hangen zodat deze zeker weet dat het een overheidsorganisatie betreft.

2.3.1.3 EENDUIDIGHEID EN KWALITEITSVERBETERING

Het invoeren van een gTLD biedt, bij een verplichtend karakter, als voordeel voor de centrale overheid dat er een eenduidigheidslag of kwaliteitsslag gemaakt kan worden: “u mag alleen onder .overheidnl opereren, als u voldoet aan de webrichtlijnen”. Ook in de naamgeving kan e.e.a. afgedwongen worden om te voorkomen dat onwenselijke URLs ontstaan.

Ten opzichte van de huidige oplossing is dit een grote meerwaarde. In het geval van consolidatie van overheidsorganisaties onder .overheid.nl kan een zelfde effect bereikt worden.

2.3.1.4 VERBETERDE VINDBAARHEID

Een gTLD is tegelijk een manier om de vindbaarheid van websites te vergroten, bijvoorbeeld via zogenaamde directie navigatie. Het invoeren van een webadres in de navigatiebalk rotterdam.overheidnl betekent voor de gebruiker zekerheid en snelheid om op de gemeentepagina van Rotterdam uit te komen. Een dergelijke verbeterde vindbaarheid is echter ook te bereiken met de consolidatie van overheidswebsites onder .overheid.nl (b.v. rotterdam.overheid.nl) of via rijksoverheid.nl/ministeries/.

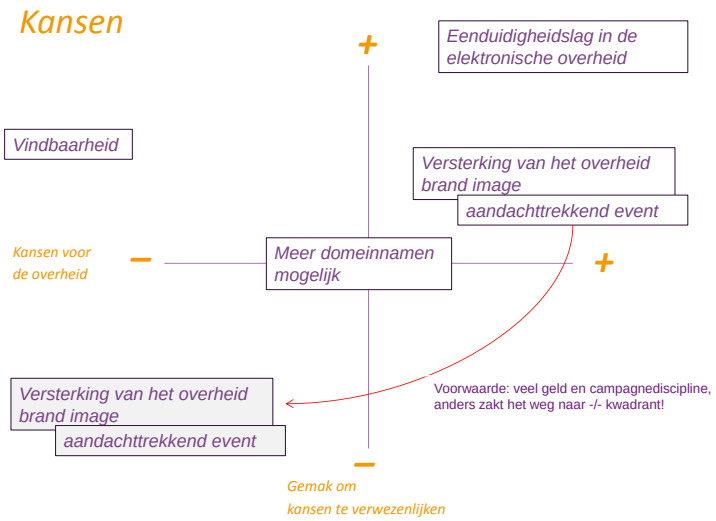
2.3.1.5 MEER KEUZEVRIJHEID IN DE DOMEINNAAM

Het aantal mogelijke domeinnamen is groter dan in de huidige .nl situatie. Er is alleen concurrentie binnen het overheidsdomein. De overheid hoeft onder dit domein niet te concurreren bij met de private sector als het gaat om domeinnamen. Het zelfde geldt hierbij voor de .overheid.nl situatie. Wel dient in ogenschouw genomen te worden dat het in sommige gevallen wenselijk is om ook de naam onder .nl (of andere TLDs) te laten registreren. In dat geval is er geen meerwaarde.

De twee cruciale vragen bij hierboven beschreven kansen zijn natuurlijk:

- hoe waardevol is die kans eigenlijk;
- hoeveel moeite is er voor nodig om die kans te verwezenlijken?

De antwoorden op deze twee vragen hangen wat .overheidnl betreft sterk af van de positie die men inneemt: die van de eigen organisatie of de centrale overheid. In enkele interviews en een werksessie met 5 communicatiespecialisten van verschillende overheidsorganisaties zijn de kansen voor de centrale overheid als volgt gepercipieerd:



Figuur 5: Communicatieve kansen.

Toelichting vanuit de expertgroep en interviews:

- Imago moet bij een gTLD in een aandachttrekkend event rond veiligheid gecombineerd worden: dan moet er wel een heel gedisciplineerde exercitie plaatsvinden, met veel middelen. Er hoeft maar iets mis te gaan (een van de vele overheden doet iets verkeerd) het imago komt fors onder druk te staan. En dan is de daadwerkelijke technische migratie nog niet eens in de beschouwing meegenomen. Het wordt een communicatieve operatie te vergelijken met de invoering van de Euro of een campagne rond de millennium bug (met bijbehorend budget). De aandacht kan ook een risico met zich meebrengen. Er zullen vragen komen of de kosten die een dergelijke operatie met zich meebrengen te rechtvaardigen zijn in tijden van bezuiniging terwijl het zeer de vraag is of de kosten opwegen tegen de baten. De mogelijkheden om vanuit andere TLDs te communiceren worden beperkter en het is de vraag of dit wenselijk is (zie ook het punt hieronder).
- Imago in combinatie met de eenduidigheidsslag is zeker een kans voor de centrale overheid, maar het levert vanuit het perspectief van de individuele overheden geen voordeel op. Sterker nog, het maakt het voor een aantal overheden die in hun campagnes samenwerken met de semi-publieke en private sector alleen maar lastiger. Die partners willen geen sterke associatie met de overheid, bijvoorbeeld omdat dat bij bepaalde doelgroepen alleen maar weerstand oproept. Denk aan inentingscampagnes of campagnes gericht op drop-out jongeren. Heel veel organisaties zijn niet van de overheid alleen, vaak spelen er publieke en private belangen waardoor het lastig zal zijn te kiezen voor een bepaalde domeinnaam (.overheidnl of .nl of .overheid.nl?). Dit kan verwarrend werken richting de burger en/of bedrijven. Het verplichtende karakter kan ertoe leiden dat partijen tegen gaan werken of mogelijkheden gaan zoeken om er onderuit te komen.
- Als het gaat om het vinden van overheidsinformatie (denk hierbij naast de gebruikelijke informatie ook aan open data) is de meerwaarde van een gTLD marginaal. Verschillende geïnterviewden en sessiedeelnemers gaven aan dat uit de webstatistieken van verschillende overheden toenemend blijkt dat veel gebruikers binnen komen via zoekmachines als Google en niet direct via het intoetsen van een URL. Een bevinding die gestaafd wordt door onderzoeker van Deursen (2010) die aangeeft dat basale operationele vaardigheden

als het invoeren van adressen in de adresbalk geen vanzelfsprekende vaardigheden zijn.[24] Het is daarnaast nog maar de vraag of de relatieve vindbaarheid zal toenemen. De overheid is immers een dusdanig grote partij dat ze toch wel vindbaar is op het Internet. Sturen op directe navigatie kan zelfs nadelig zijn: gebruikers komen dan, ten opzichte van zoekmachines, veel minder snel bij de webcontent waar ze naar op zoek zijn en mogelijk afhaken[25].

- Het voordeel van meer keuzevrijheid in domeinnamen wordt gezien, maar laat zich relativeren bedenkende dat het ook kan als een subdomein van .overheid.nl. Dus bijvoorbeeld kadaster.overheid.nl.

2.3.2 RISICO'S

Een gTLD genereert naast communicatieve voordelen ook enkele risico's.

2.3.2.1 VERWARRING

Er is een reële kans op verwarring bij de gebruiker tijdens de adoptieperiode. De huidige gTLD inrichting kent 21 categorieën (.com, .eu, .net, .org, etc.) en met de komst van de vele honderden nieuwe gTLDs zal het voor de internetgebruiker (burger) lastiger worden om de weg op het internet te vinden. Men zal eraan moeten wennen en de kans is groot dat er verwarring ontstaat: "welke is het?" of "Wat is het verschil tussen belastingdienst.nl en belastingdienst.overheidnl?" Het zal in deze verwarrende situatie en naast alle andere nieuwe gTLDs moeilijker worden om een reputatie op te bouwen als betrouwbaar en veilig domein.

Een dergelijke verwarring speelt niet in de huidige .nl situatie. Hooguit is daar verwarring over of het wel een overheidswebsite betreft of niet. In de .overheid.nl situatie zal de burger moeten wennen aan de nieuwe constructie van de domeinnamen van overheidswebsites. Ook hier geldt dat er verwarring kan ontstaan over welke URL de juiste is: rdw.nl of rdw.overheid.nl? De ervaring van het Britse Nominet is dat veel burgers het second-level domeinnaam vergeten in te typen. Bij .overheid.nl kan dat dus ook gebeuren.

2.3.2.2 LENGTE DOMEINNAAM

Korte domeinnamen genieten over het algemeen de voorkeur, er hoeven dan minder karakters ingetoetst te worden. De lengte van het aangevraagde overheidnl is 8 tekens langer dan .nl. Dat betekent dat er meer kans op typefouten is. Ten opzichte van .overheid.nl is de type-lengte bijna even lang (op de punt na).

Ook relatief lang zijn de aangevraagde .amsterdam en .vlaanderen gTLDs. Echter, relatief veel Amsterdamse en Vlaamse domeinhouders hebben deze naam al in hun huidige domeinnaam onder .nl staan (bijvoorbeeld www.mediacafe-amsterdam.nl). Dat zorgt ervoor dat er bij een gelijknamige gTLD geen extra karakters ingetoetst hoeven worden.

---

[24] Internet skills, vital assets in an information society, Van Deursen, 2010, pag 146.

[25] De basisrelevantie van de overheidswebsites staat garant voor zeer goede organische vindbaarheid. Bij een generalistische- en naamsbekende website als Rijksoverheid.nl bestaat het directe verkeer (waarbij een domeinnaam getypt is) minder dan 15%. Websites spannen zich in om het verkeer op de homepage te minimaliseren en bezoekers meteen op de juiste pagina te ontvangen.

2.3.2.3 MERKMISBRUIK

Merkmisbruik is ondanks dat dit met een gesloten gTLD minder zou moeten worden nog steeds aan de orde. Er zijn meer dan 1000 gTLDs aangevraagd, die bijvoorbeeld de volgende, met .overheidnl concurrerende, combinaties mogelijk maken: ind.cafe , svb.bank of duo.sex.

Daarnaast is het wenselijk om voor nieuwe domeinnamen onder het overheids-gTLD ook de .nl variant (tijdelijk) te hebben om misbruik te voorkomen. Afgezien van de vraag of dit haalbaar is, zal dit ook de huidige naamgevingsconventies beïnvloeden.

2.3.2.4 LEGACY

Er is sprake van legacy: de oude domeinnamen onder .nl zullen in beheer moeten blijven. Het vrij laten vallen van uwv.nl, rdw.nl of belastingdienst.nl is vragen om ongelukken. Dergelijke legacy domeinen zullen op een betrouwbare manier beveiligd moeten worden en/of verwijzen naar de nieuwe domeinen onder .overheidnl. Het aanhouden van veel van de bestaande domeinnamen brengt ook kosten met zich mee. De kosten die nu gemaakt worden voor het hebben van deze domeinnamen zal tot in lengte van dagen blijven terugkeren, ook al worden de domeinnamen niet meer gebruikt.

In de huidige .nl situatie is geen sprake van legacy omdat wordt doorgegaan met de huidige domeinnamen. De .overheid.nl situatie kent een gelijke legacy problematiek als bij de gTLD situatie. Ook hier zullen de oude domeinnamen in beheer moeten blijven om misbruik te voorkomen. Echter, wanneer er gedurende een langere gewenningsperiode simultaan gebruik van de gTLD en de oude conventies gemaakt zal worden, dan is dat een risico m.b.t. de implementatie van gTLD conventies.

2.3.2.5 COMMUNICATIEVE TRANSITIEKOSTEN

Er zullen transitiekosten voor allerlei bestaande communicatieve uitingen moeten worden gemaakt. Zo zullen vele huisstijl en multi-channel uitingen moeten worden aangepast: briefpapier, folders, advertenties, visitekaartjes, interactive voice response systemen, autobestikkering, gevelversiering van gebouwen, etc. Overal wordt wel een .nl domein genoemd. Vanuit dat oogpunt is er enige gelijkenis met de overgang naar één Rijkshuisstijl. Voor de invoering hiervan bedroegen de kosten zo'n 20 miljoen Euro[26]. Deze kosten zijn indicatief en zullen waarschijnlijk lager liggen bij een gTLD[27]. Tegenover de eenmalige investering voor de Rijkshuisstijl staat een structurele besparing van vijf miljoen euro per jaar[28]. Het is nog maar de vraag of de transitiekosten van de invoering van een gTLD ook terugverdiend zullen worden gezien de relatief lage kosten van de huidige situatie. Hooguit valt te besparen op een efficiëntere inrichting van het beheer door consolidatie van subdomeinen en standaardisatie van beheeromgevingen (zie verder ook sectie 2.5 over kosten). Interviewkandidaten geven aan dat de communicatieve kosten redelijk gedrukt kunnen worden door eerst het oude communicatiemateriaal op te maken. De transitieperiode die in ieder geval nodig is, biedt hiervoor voldoende mogelijkheden.

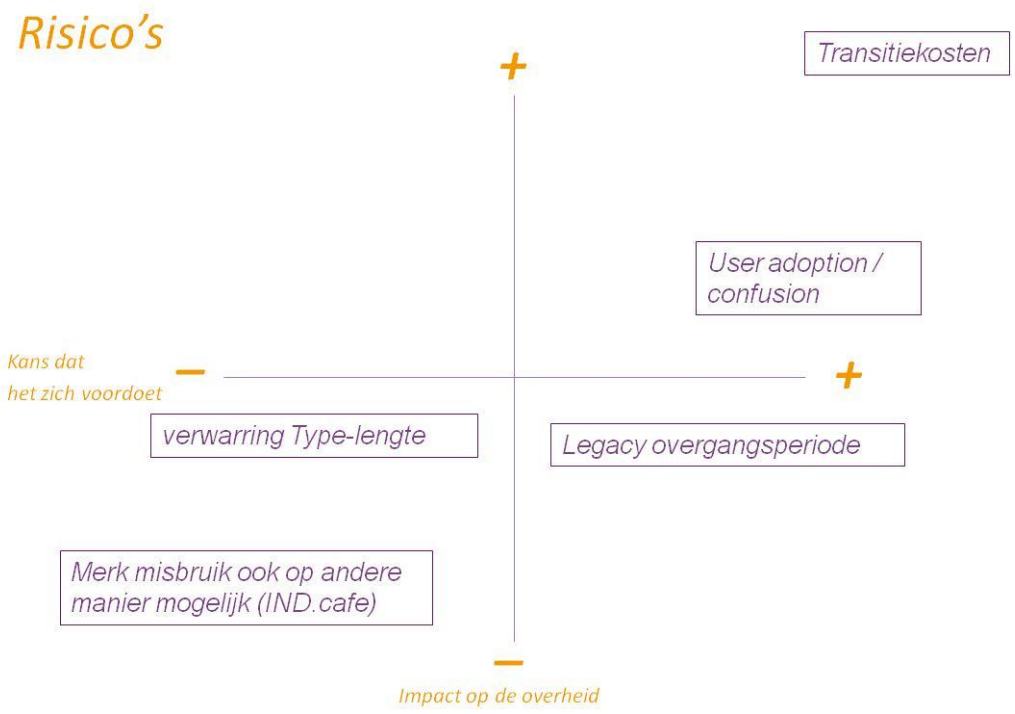
[26] Voor de invoering van de Rijksstijl was een bedrag van €18.525.000 over de periode 2008-2010 beschikbaar.
[27] Bij de invoering van de Rijkshuisstijl kwam veel meer kijken zoals bijvoorbeeld het specificeren van het gewenste papier zodat dit bij verschillende leveranciers besteld kon worden.
[28] Bron: http://www.rijkshuisstijl.nl/index.cfm/i-base-1rijkslogo/project/vraag-en-antwoord/.

Niet uitgesloten is dat rekening gehouden moet worden met draagvlak vergrotende veranderstrategieën en overheidsinterne en externe communicatiecampagnes. De kosten van een dergelijk verandertraject en bijbehorende campagnes dienen in ogenschouw genomen te worden bij de afweging om een gTLD te gaan gebruiken.

Ook voor deze communicatieve risico's gelden twee vragen:

- hoe groot is de kans dat het risico zich voordoet;
- wat zijn de gevolgen van het nadeel?

In enkele interviews en een werksessie met 5 communicatiespecialisten van verschillende overheidsorganisaties zijn de risico's als volgt gepercipieerd (noot: bij de risico's was er weinig tot geen verschil in het standpunt dat de specialisten innamen: vanuit de centrale overheid of de eigen organisatie).



Figuur 6: Communicatieve risico's.

Toelichting vanuit de expertgroep en interviews:

- Verwarring bij de gebruiker tijdens de zogenaamde adoptieperiode. De kans hierop is groot, ook met inachtneming van andere brands die fors in de markt zijn gezet. Denk aan rijksoverheid.nl, belastingdienst.nl en overheid.nl.
- De lengte van het nieuwe gTLD ten opzichte van .nl vormt een risico, maar net als met de verbeterde vindbaarheid als kans geldt bij dit risico hier dat het er op lijkt dat er steeds minder direct genavigeerd wordt.
- Merkmisbruik wordt als risico erkend, maar is er in principe nu ook al. Het beeld bestaat dat veel gebruikers nauwelijks letten op de navigatiebalk, veel meer afgaan op en zich laten misleiden door de look & feel van

een webpagina. Een logo van bijvoorbeeld de Rijksoverheid is hiervoor een duidelijker middel. Omdat burgers erop moeten kunnen vertrouwen dat dit logo alleen door de Rijksoverheid wordt gebruikt is er een auteursrechtelijk voorbehoud op het logo gemaakt. Tevens heeft zij het beeldmerk als hoogheidsteken gedeponeerd[29]. Door deze handelingen is het voor de Rijksoverheid mogelijk om bij misbruik van het logo op te treden. Hierdoor zal misbruik van het logo niet snel plaatsvinden, ondanks dat het betrekkelijk eenvoudig is het logo te hergebruiken op een malafide website.

- Legacy/overgangsperiode: het is evident dat overheid de .nl domeinnamen moeten blijven vasthouden. De kosten hiervan zijn minimaal en te overzien[30].
- Er zullen zeker enorme transitiekosten voor allerlei bestaande communicatieve uitingen moeten worden gemaakt. Het gaat namelijk niet alleen om visitekaartjes of briefpapier maar ook om fleetmarking (auto's met URLs er op gestickerd) en gevels. Dat brengt wederom weer een imagorisico met zich mee dat zich in deze tijd van economische recessie moeilijk uit te leggen is als de voordelen in termen van veiligheid en betrouwbaarheid niet evident zijn.

2.4 ACCEPTATIE EN DRAAGVLAK

De verdere ontwikkeling en acceptatie van het gTLD is in grote mate afhankelijk van het vertrouwen van de gebruikers (burgers en bedrijven) in de veiligheid en betrouwbaarheid van de online overheidscommunicatie. Waar zitten de kansen en risico's om dit vertrouwen te winnen?

2.4.1 KANSEN

2.4.1.1 GREENFIELD SITUATIE

Een nieuw gTLD creëert een greenfield situatie. Dat wil zeggen dat er een min of meer gestandaardiseerde omgeving is voor overheidspartijen waarbinnen ze op een gecontroleerde manier domeinnamen kunnen aanvragen, beheren en beveiligen. Dit voordeel is in de praktijk slechts gedeeltelijk haalbaar omdat de huidige situatie nog steeds in stand en veilig gehouden moet worden. Van een betrekkelijke greenfield situatie is ook sprake bij de .overheid.nl situatie. Maar ook hier geldt dat het in stand houden van legacy situaties het greenfield enigszins vervuild.

2.4.1.2 BETERE BESCHERMING EIGEN MERK

Iedereen is vrij een .nl domein aan te vragen. Deze worden uitgedeeld volgens het principe van 'first come, first served'. Zo kunnen domeinnamen die van interesse zijn voor de Nederlandse overheid door anderen 'ingepikt' worden. Uit onderzoek onder bedrijven blijkt wel dat een eigen gTLD mogelijkheden biedt om de eigen merknaam beter te beschermen, vooral als men erin slaagt om het gTLD bekend/populair te maken[31].

Veel domeinnamen zijn al vergeven onder .nl, .eu en/of .com waardoor het voor nieuwe bedrijven en ook

[29] Zie http://www.rijkshuisstijl.nl/index.cfm/i-base-1rijkslogo/basiselementen/rechten/.

[30] De kosten voor een .nl-domein variëren, maar de gemiddelde prijs ligt tussen de 4 en 15 euro. Hierin zijn niet de kosten van het beheer van de infrastructuur, personeel voor systeembeheer, datacenterkosten, website ontwikkeling, website beheer, etc. meegenomen.

[31] Gepresenteerd op 8 december 2011 tijdens het SIDN webinar over "Nieuwe Top Level Domeinen 2012: unieke kans of bedreiging?" Zie https://www.sidn.nl/nieuws/nieuwsbericht/article/nieuwe-top-level-domeinen-2012-unieke-kans-of-bedreiging/.

overheidsorganisaties moeilijk is om een domeinnaam met de eigen naam te registreren. Zo heeft de voetbalclub Ajax niet ajax.com (en .eu) in gebruik; Ajax heeft straks wel het eerste recht op ajax.amsterdam. De discussie over een beter gecontroleerde uitgifte van domeinnamen onder .nl speelt al enige tijd[32]; en hier wordt actie op genomen vanuit de Rijksoverheid.

Kijkende naar de andere situaties, dan valt het volgende op:

- Hudige .nl situatie: De Nederlandse overheid claimt via de rechter regelmatig met succes bepaalde domeinnamen die aan de staat toebehoren terug. Voorbeelden hiervan zijn regering.nl, miljoenennota.nl, prinsjesdag.nl, troonrede.nl[33] en ministerpresidentrutte.nl[34]. Op deze manier heeft de overheid een middel om de eigen 'merken' te beschermen. De meerwaarde van een gTLD is dus beperkt.
- .overheid.nl situatie: Ook hier geldt, net als bij een gTLD, dat de overheid volledig in control is over de subdomeinen eronder. Deze kunnen niet ingepikt worden door anderen. Rechtszaken worden hierdoor voorkomen.

2.4.2 RISICO'S

2.4.2.1 WEINIG INTUÏTIEVE NAAM

Intuïtief zal de burger een punt tussen overheid en nl zetten. Dit is de gebruikelijke naamgevingsconventie op het Internet en dat is de burger eenmaal zo gewend. Ook in reclamespotjes wordt "punt-nl" vaak gebruikt als marker om de online presence kracht te geven.

Het is mogelijk en te overwegen om een wijzigingsproces van de gTLD naam op te starten bij ICANN. De vraag is echter wat een herkenbare en acceptabele naam is. Kijkende naar de criteria van ICANN hieromtrent lijkt .overheid te generiek en zal op grond daarvan waarschijnlijk afgewezen worden. In de in november 2012 gepubliceerde 'early warning' lijst van ICANN staan geen bezwaren tegen .overheidnl[35].

Uiteraard speelt de vraag of de burger met de komst van de vele nieuwe gTLDs (er zijn er 1930 aangevraagd) door de bomen het bos nog wel ziet en er gebruik van zal gaan maken. Een uitgekiende communicatiecampagne over het hoe en waarom van een overheids-gTLD zal zeker nodig zijn om gebruikers op het goede spoor te zetten. Want er kleven ook gebruikersnadelen aan dit gTLD. Zo zullen gebruikers die niet met bookmarks werken in sommige gevallen een langere URL gaan intoetsen. Een URL die ze bovendien niet meteen gewend zijn [.overheidnl] in plaats van [.nl]. Los van alle typefoutrisico's en malafide partijen die daar wellicht op willen inspelen; waarom zou de gebruiker dat moeten willen? Wat is de meerwaarde? In een eventuele campagnevoorbereiding moet daar goed over worden nagedacht. Waarover ook in een eventuele campagnevoorbereiding moet worden nagedacht, is hoe de overgangsfase vorm te geven. Daarmee bedoelen we een overgangsfase waarin om zowel informatietechnische als marketing/communicatietechnische (noem het nog even aanhouden van het oude postadres) redenen sprake is van twee extensies voor dezelfde website gedurende een nader te bepalen periode.

---

[32] Zie http://tweakers.net/nieuws/32013/overheid-wil-meer-controle-houden-over-domeinnamen.html en http://tweakers.net/nieuws/52258/sp-uitgifte-domeinnamen-moet-overheidstaak-worden.html.
[33] Zie http://retro.nrc.nl/W2/Nieuws/2000/10/03/Med/01.html.
[34] Zie http://www.techzine.nl/nieuws/27038/overheid-naar-rechter-om-domeinnaam-te-claimen.html.
[35] Bron: https://gacweb.icann.org/display/gacweb/GAC+Early+Warnings.

Ten opzichte van de andere situaties verhoud dit risico zich als volgt:

- Huidige .nl situatie: Dit is voor veel gebruikers de vertrouwde structuur voor domeinnamen. Hier zijn ze mee opgevoed.
- .overheid.nl situatie: Deze naamgeving is intuïtiever dan .overheidnl en daardoor gebruikersvriendelijker.

2.4.2.2 VERTROUWEN IN DE NAAM

In de website statistieken is duidelijk te zien dat burgers meer vertrouwen hebben in .nl dan in een niet-.nl domein (bv .eu of .com). In de loop der jaren heeft .nl onder burgers een bepaalde reputatie opgebouwd waar ze aan hechten. Bovendien leren gebruikers dat Nederlandstalige sites met een ander TLD verdacht zijn (denk hierbij aan o.a. de discussie rondom www.telefoongids.com die gepeperde facturen aan naïeve MKB-ers stuurt). Het is de vraag of en op welke termijn een nieuw gTLD een zelfde betrouwbare reputatie zal opbouwen. Het branden van .overheidnl zal daarnaast gaan indruisen tegen de bestaande branding van rijksoverheid.nl (waar de afgelopen tijd sterk op is ingezet).

Voor bedrijven en overheidsorganisaties geldt dit net zo. Ze hebben vaak veel effort (tijd en geld) gestoken in het vestigen van een brand-name op het Internet. Zo hecht de Belastingdienst veel waarde aan de in de loop der jaren sterk gevestigde belastingdienst.nl-naam en veel gemeentes aan [gemeentenaam].nl. Voor veel burgers zijn ze onder deze naam te vinden op het Internet. Overstappen naar een nieuwe naam zal enige overredingskracht vereisen.

Daarnaast heeft Amsterdam ook zelf een gTLD aangevraagd. Het is niet ondenkbaar dat de gemeente Amsterdam hier ook gebruik van zal maken. Hier kunnen mogelijk conflicten ontstaan die het draagvlak ondermijnen.

Voor de andere situaties geldt het volgende:

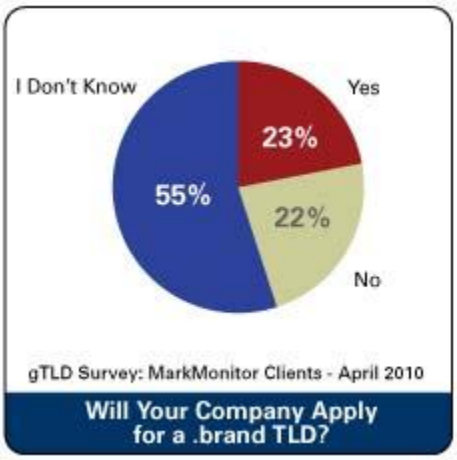
- Huidige .nl situatie: .nl geniet een bepaalde reputatie dat .overheidnl niet meteen zal hebben. Verschillende overheidsorganisaties hebben onder dit TLD een vertrouwde naam opgebouwd. Onder .overheidnl zal dit vertrouwen opnieuw moeten worden opgebouwd.
- .overheid.nl situatie: In dit geval profiteert een organisatie zowel van de goede .nl reputatie als van de overheidsnaam. Re-branding van merknamen als belastingdienst.nl zal nodig zijn.

2.4.2.3 ONDUIDELIJKE MEERWAARDE

Voor veel geïnterviewde partijen is de meerwaarde van .overheidnl niet duidelijk. De verwachting is dat het ook voor veel bestuurders van overheidsorganisaties onduidelijk zal zijn wat de voordelen zijn die een gTLD biedt in termen van beveiliging (korte chain of trust, controle over onderliggende zones en hun beveiliging, etc.) en de greenfield situatie die ontstaat, om een overstap te rechtvaardigen.

Uit recent onderzoek naar de perceptie van het bedrijfsleven over de nieuwe gTLDs blijkt enige terughoudendheid:

het wordt teveel als push ervaren en de voordelen zijn beperkt[36]. Een in 2010 uitgevoerd marktonderzoek door MarkMonitor is indicatief voor de terughoudendheid van bedrijven tegenover een gTLD. 23% van de bedrijven heeft interesse, 22% van de bedrijven heeft geen interesse, en 55% van de bedrijven weet het nog niet (zie Figuur 7). Van alle bedrijven die een gTLD overwegen toe te passen, zei 70% dat dit vooral een defensieve zet zal zijn[37]. 95 bedrijven werkten mee aan het onderzoek.



Figuur 7: Bedrijven terughoudend over aanschaf gTLD.

Een ander onderzoek van de Vlaamse overheid om het draagvlak te toetsen voor een gTLD voor Vlaanderen onder meer dan 450 stakeholders faalde jammerlijk. Ondanks herhaalde pogingen om de enquête onder de aandacht van de stakeholders – waaronder ISPs, overheden en vertegenwoordigers uit het bedrijfsleven – te brengen bleef de response steken op 2 volledig ingevulde formulieren[38]. Er werd voorzichtig geconcludeerd dat het onderwerp weinig of niet leeft in de samenleving. Hiermee dient rekening gehouden te worden bij de uitrol van een gTLD.

De onduidelijke meerwaarde van een gTLD en het ogenschijnlijk gebrek aan interesse hiervoor binnen de samenleving bieden kansen voor de huidige .nl situatie en eventuele verbetering daarin betreffende het toezicht en de beveiliging van de registratie. Voor deze situatie zijn er geen grote kosten en effort gemoeid om te migreren en hoeven er geen zorgen gemaakt te worden over maatschappelijk draagvlak. Dit maakt de noodzaak van een concrete meerwaarde minder relevant. In iets mindere mate geldt dit ook voor de .overheid.nl situatie.

2.5 EFFICIËNTIE EN KOSTEN

Biedt een gTLD efficiency-winst ten opzicht van een .nl aanpak? Zijn er hierdoor kosten te besparen?

[36] Gepresenteerd op 8 december 2011 tijdens het SIDN webinar over “Nieuwe Top Level Domeinen 2012: unieke kans of bedreiging?” Zie https://www.sidn.nl/nieuws/nieuwsbericht/article/nieuwe-top-level-domeinen-2012-unieke-kans-of-bedreiging/.
[37] Bron: https://www.markmonitor.com/mmblog/new-gtld-survey-shows-that-many-intend-to-apply-but-that-the-majority-are-undecided/.
[38] Bron: http://docs.vlaamsparlement.be/website/htm-vrg/600372.html.

2.5.1 KANSEN

2.5.1.1 PROCESMATIGE UNIFORMITEIT EN EFFICIËNTIE

Het inzetten van een gesloten gTLD biedt kansen voor het creëren van meer procesmatige uniformiteit voor het aanvragen, inrichten en beheren van overheidsdomeinen. De huidige situatie kenmerkt zich door domeinen die door tal van verschillende registrars en registrants zijn aangevraagd en onder verschillende top level domeinen hangen. De overheid heeft slecht zicht op welke domeinnamen zij geregistreerd heeft. Daarnaast worden soms vreemde domeinen door de overheid geregistreerd[39]. Een gTLD kan hier een consoliderend effect op hebben.

Voor de andere situaties is deze kans als volgt te karakteriseren:

- Huidige .nl situatie: Deze situatie werd tot voor kort gekenmerkt door een gebrek aan overzicht en uniformiteit in de registratie van domeinnamen door overheidsorganisaties. Hierdoor bleek het lastig te controleren of websites aan de webrichtlijnen voldeden en of de domeinen gebruik maakten van DNSSEC. Het implementeren van dergelijke verbeteringen is door de veelheid aan verschillende beheersystemen weinig efficiënt. Op dit moment wordt er gewerkt aan verbetering op deze vlakken. De ministeries van BZK en AZ zijn samen een rijksbrede opschoonactie gestart om ervoor te zorgen dat de websites die de rijksoverheid beheert ook echt zullen voldoen aan de webrichtlijnen. Een onderdeel daarvan is het consolideren van de vele websites onder rijksoverheid.nl. Hier is beleid voor gedefinieerd dat moet zorgen voor meer stroomlijning in het registratieproces en het beheer van de domeinnamen. Ook worden veel websites geschrapt. Voor deze websites zou het niet efficiënt zijn om te investeren in het voldoen aan de webrichtlijnen en om de bijbehorende domeinen te beveiligen met DNSSEC. Richting de burger en het bedrijfsleven wordt met radiospotjes getracht de naamsbekendheid van het domein te vergroten. Met een gTLD worden deze activiteiten ondermijnd alsmede de kosten die hiervoor gemaakt zijn. In deze situatie is ook sprake van een beperkt aantal registrars waardoor de controle over de registratie van domeinnamen efficiënter uit voeren is. Ook is sprake van een meer gestandaardiseerde aanpak voor de inrichting van domeinen binnen de overheid. Deze verbeterde .nl situatie voorziet dus ook in procesmatige uniformiteit. Dit betreft voornamelijk de Rijksoverheid, bij de lagere overheden is men nog niet zo ver.
- .overheid.nl situatie: Ook hiervoor geldt dat de overheid volledige controle heeft over wie domeinnamen aanvraagt en hoe deze ingericht worden. De meerwaarde van een eigen gTLD is vanuit het perspectief van procesmatige uniformiteit dus minimaal.

2.5.2 RISICO'S

2.5.2.1 HOGE AANSCHAF EN BEHEERKOSTEN

De kosten voor het hebben van een gTLD bestaan uit de aanvraag ($185.000) en de jaarlijkse bijdrage aan ICANN ($25.000). Naast de kosten voor het beheer van de registry backend komen vaak nog andere kosten voor eventuele juridische procedures, marketing activiteiten, inwinnen van advies, administratieve handelingen, personeelskosten en technische zaken. Eventuele registrar-kosten kunnen hier nog bijkomen voor het laten registreren van domeinen. Het business plan voor de verwerving en exploitatie van het Friese .frl top level domein geeft een totale kosteninschatting

[39] Zie http://www.hpdetijd.nl/2010-01-14/de-kwestie-godverdommenl/.

van 2.8 miljoen Euro over een periode van 5 jaar[40]. Ten opzichte van de huidige situatie is dit een stuk duurder. De kosten voor enkele duizenden geregistreerde domeinen zijn marginaal (~50.000 Euro). De domeinen onder het gTLD kunnen gratis verstrekt worden.

In vergelijking met de andere situaties komen de kosten van een gTLD naar verwachting hoger uit:

- Huidige .nl situatie: De aanschafkosten van domeinnamen onder .nl zijn relatief laag. De hosting en beheerkosten zullen door de relatief grote wildgroei aan overheidswebsites en door het gedistribueerde karakter ervan wel relatief hoog liggen, maar nog steeds veel lager t.o.v. het beheer van een gTLD. Gemiddeld liggen de kosten van domeinregistratie en hosting van een website ergens tussen de €50 en €350 per jaar. Omdat nu gebruik gemaakt wordt van relatief veel verschillende webhostingplatformen, zal het beheer van de websites erop minder efficiënt zijn dan in een meer gestandaardiseerde omgeving. Door toenemende consolidatie van registrars en webhostingplatformen vallen er efficiëntieslagen te behalen door bijvoorbeeld slim hergebruik van kennis en technologieën (zoals pop-ups voor cookies of hoe om te gaan met bepaalde webrichtlijnen). Dat een dergelijke consolidatie qua kosten zijn vruchten afwerpt is al goed waar te nemen bij de Rijksoverheid; de Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken geeft aan dat de 3500 geregistreerde domeinnamen de Rijksoverheid jaarlijks ongeveer €5.000 kosten.
- .overheid.nl situatie: Ook hier zijn efficiëntievoordelen te behalen door consolidatie onder dit domein. Bovendien vervallen de aanschafkosten voor veel (nieuwe) domeinnamen. Er dient wel rekening gehouden te worden met het feit dat sommige onder .nl geregistreerde domeinen behouden moeten blijven.

2.5.2.2 TECHNISCHE TRANSITIEKOSTEN

Naast de communicatieve kosten (zie sectie 2.3.2.5) zitten er ook technische kosten aan een transitie van .nl naar .overheidnl:

- Het aanhouden en beheren van de oude overheidsdomeinen en ervoor zorgen dat bezoekers op de bijbehorende websites doorgestuurd worden naar de websites onder .overheid.nl. De kosten voor het aanhouden van de oude domeinen zijn nihil, het beheer ervan zal beperkte kosten met zich meebrengen.
- De technische transitie kan in theorie met een vertaaltabel relatief simpel verlopen. De aanname is dat alle partijen de domeinen conform de daarvoor geldende technische specificaties hebben ingericht. Indien dat niet het geval is, kunnen de transitiekosten snel oplopen. Bijkomende factor is dat het gebruik van DNSSEC vanwege de extra complexiteit tot hogere kosten leidt. Dat is op zichzelf niet gerelateerd aan het al-dan-niet hebben van een eigen gTLD; DNSSEC staat op de pas-toe-of-leg-uit lijst en moet dus in ieder geval worden uitgerold, dus die kosten worden hoe dan ook gemaakt.
- Er zijn sites die gebruik maken van SSL/TLS certificaten om een veilige verbinding op te zetten. Deze certificaten hebben een domeinnaam in zich. Een eventuele migratie naar een gTLD betekent ook dat nieuwe SSL/TLS certificaten voor het gTLD aangeschaft zullen moeten worden. Dergelijke certificaten zijn op dit moment niet zomaar bij de gebruikelijke certificatenleveranciers te halen. Hier zullen afspraken over gemaakt moeten worden.

[40] Bron: Verwerving en exploitatie .frl Top Level Domein – businessplan, 19 december 2011, versie 1.01.

- Systemen die gebruik maken van domeinnamen (registratieformulieren, inlogschermen, betaalsystemen, mobiele applicaties, inkoopsystemen, etc.) en deze valideren zullen getest moeten worden of ze in staat zijn om te gaan met een nieuw gTLD. Naast de kosten die dit testen met zich meebrengen, komen ook eventuele additionele kosten voor het aanpassen van de systemen indien de test faalt.

Ook het bedrijfsleven zal te maken krijgen met additionele kosten bij de introductie van een gTLD. Veel websites verwijzen bijvoorbeeld naar overheidsinstanties als de Belastingdienst of RIVM. Dergelijke links zullen aangepast moeten worden. De vraag is of dat zal gebeuren; vooral passieve content zal niet zo snel meer veranderen naar .overheidnl. Ook in de machine-to-machine of server-to-server communicatie vanuit het bedrijfsleven met de overheid zullen of configuratieniveau instellingen en certificaten aangepast moeten worden.

In tegenstelling tot de open gTLDs zoals .amsterdam en .vlaanderen valt er voor de overheid niet zomaar commercieel of anderszins te verdienen aan de verkoop van domeinnamen onder .overheidnl aan niet-overheidspartijen. Hierdoor ontbreekt er een bron van inkomsten om de kosten van de gTLD te dekken.

Door het ingezette verbeterproces van de huidige zullen voornamelijk kosten bespaard worden. De transitie zelf brengt weinig technische kosten met zich mee. Additionele kosten liggen vooral in het organisatorische domein zoals de inspanning die nodig is voor de consolidatie en het houden van toezicht. Let wel, dit betreft voornamelijk de Rijksoverheid. Er hoeven geen nieuwe certificaten aangeschaft te worden en bedrijven zullen geen extra kosten hoeven maken.

Bij een transitie naar een .overheid.nl situatie zal er iets meer technische effort nodig zijn om alle websites onder dit domein te plaatsen. Certificaten zullen vernieuwd moeten worden (hoewel dit in een DANE situatie geen kosten met zich hoeft mee te brengen) en bedrijven zullen kosten moeten maken omdat de overheidsdomeinnamen structureel veranderen. Dergelijke transitiekosten zullen overeen komen met de kosten die gemaakt zullen worden in een gTLD situatie.

2.6 UITVOERBAARHEID – BEHEER EN INRICHTING

2.6.1 KANSEN

2.6.1.1 BETROUWBARE REGISTRY

De veiligheid van het gTLD staat of valt met een goede beheersorganisatie. Uit de aanvraag van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties blijkt dat deze rol toebedeeld is aan SIDN, een professionele organisatie die hiervoor alle vereiste kennis en middelen bezit. Het beheer van het .nl domein wordt immers al door SIDN gedaan. Het selecteren van een betrouwbare en onafhankelijke registry beheerder kan een positieve uitstraling hebben op de betrouwbaarheid van de gTLD. Het zelfde geldt voor de .nl en .overheid.nl situaties die nu profiteren van de SIDN als betrouwbare beheerder van .nl. Het gevolg is dat de veiligheid van ‘www.overheidnl.’ vergelijkbaar zal zijn met die van ‘www.overheid.nl’ met dien verstande dat SIDN de veiligheid van resp ‘.nl’ en ‘.overheidnl’ in gelijke mate zal garanderen en dat de overheid de veiligheid van resp. ‘www.overheid’ en ‘www’ in gelijke mate zal doen.

Hoewel het vanuit controleperspectief misschien wenselijk zou zijn om zelf de registry in te richten wordt dit door alle geïnterviewde partijen afgeraden. De kosten hiervoor zijn hoog en de vereiste expertise hiervoor is niet aanwezig binnen de overheid.

2.6.1.2 ÉÉN CENTRAAL LOKET VOOR GECONTROLEERDE REGISTRATIE

De partijen die domeinnamen namens registrants, of houders, registreren, worden aangeduid als registrars. Voor het .nl domein zijn meer dan 1500 registrars actief. Deze bedrijven registeren de domeinnamen namens aanvragers. SIDN heeft voor het registreren van domeinnamen al een in de praktijk bewezen proces ingericht. Zoals in de aanvraag van het gTLD blijkt is dit voor .overheidnl een gesloten systeem waar alleen overheidsorganisaties domeinen onder mogen registreren (één registrant). Uit de interviews blijkt ook dat er een voorkeur is om het aanvragen van domeinnamen via een centraal 'loket' te laten verlopen. Die aanvragen gelden voor alle bestuurslagen, op dit moment is er echter geen beheerorganisatie die alle bestuurslagen bedient. Maar het is maar de vraag of er van meet af aan een nieuwe organisatie moet komen. Het kan wellicht ook (eerst) bij een bestaande organisatie worden ondergebracht, waarbij voor deze functie het taakveld van die organisatie wordt uitgebreid naar alle bestuurslagen. Mogelijke organisaties voor een centraal loket zouden het Ministerie van Algemene Zaken, KING of Logius kunnen zijn. Laatstgenoemde bedient overigens al meerdere bestuurslagen.

Het centrale loket communiceert dan weer met een registrar die de daadwerkelijke domeinregistratie doet. Het Ministerie van Algemene Zaken, dat nu ook al een registrar is en verantwoordelijk is voor rijksoverheid.nl zou hiervoor een geschikte partij kunnen zijn ware het niet dat zij nog geen ICANN accreditatie heeft. Dit laatste is een vereiste voor gTLD registrars.

Het voordeel van een centraal loket is dat er meer controle gevoerd kan worden over het registratieproces en ook de beveiliging ervan beter gegarandeerd kan worden. Bovendien worden afhankelijkheden van tussenpartijen weggenomen.

Met betrekking tot de andere situaties vallen de volgende zaken op:

- Huidige .nl situatie: Hier is nog steeds sprake van een groot aantal loketten voor registratie van domeinnamen. Er is nauwelijks controle over te voeren. Door de consolidatieslag bij de Rijksoverheid is hier een duidelijk loket gekomen voor registratie van domeinnamen. Het Ministerie van Algemene Zaken treedt in deze situatie op als een loket voor het consolideren van domeinnamen en websites voor de Rijksoverheid. Voor een bredere overheidscontext, zou er nagedacht kunnen worden over het beperken van het aantal registrars tot een selecte groep die onder een bepaalde mate van toezicht staat van de overheid en waarmee in samenspraak met de registry afspraken zijn gemaakt over de veiligheid van het registratieproces.
- .overheid.nl situatie: Hier is sprake van een centrale beheerder die toeziet op registraties onder dit second-level domein. Toegang tot registratiesystemen wordt gecontroleerd door de eigenaar van dit domein. Met andere woorden, een centraal loket voor registratie van domeinnamen is prima in te richten zonder een eigen gTLD te hebben.

2.6.2 RISICO'S

2.6.2.1 ONTBREKEN GOVERNANCE

Het inrichten van een centraal loket vereist het inrichten van processen en procedures voor het registeren van domeinen onder .overheidnl. Dergelijke maatregelen ontbreken momenteel alsmede een goed ingerichte governance-structuur waarin alle belanghebbenden betrokken zijn. Het centrale loket krijgt, afhankelijk van de breedte waarin de gTLD voor de overheid zal ingezet worden, van doen met potentieel 1600 overheidsorganisaties. Allemaal met hun eigen belangen, eisen en wensen. Om nog maar te zwijgen over hun denkbeelden over bekostiging en afdracht.

Het is daarom niet voor niets dat een dergelijk brede vorm van governance ontbreekt in de huidige situatie. Het feit dat het lastig is om in deze situatie beleid te maken voor het inrichten en beheren van domeinen om dit beleid te effecturen mag echter niet als motivatie voor de overgang naar een gTLD mag niet gebruikt worden . Anders zal dat in de nieuwe situatie niet anders zijn.

Scoping van de reikwijdte van het gTLD is belangrijk om de governance ervan goed vorm te geven. Hiervoor kan geput worden uit de resultaten die op de schaal van de Rijksoverheid behaald zijn op dit gebied. Vanuit de Rijksoverheid wordt er door de ministeries van BZK en AZ gewerkt aan meer governance in de huidige situatie. Er is sprake van beleid om de onoverzichtelijkheid en vrijblijvendheid te beperken via het opschonen van domeinen, consolidatie en beter toezicht.

Voor .overheid.nl zal, net als bij een gTLD, een bepaalde governance structuur nodig zijn.

2.6.2.2 STARHEID – VERLIES VAN AUTONOMIE

De huidige situatie maakt het voor veel overheidspartijen mogelijk om snel en flexibel een nieuw domein te registreren via een willekeurige registrar. Deze vrijheid komt mogelijk onder druk te staan met de inrichting van een centraal loket voor registratie onder een gTLD als bijvoorbeeld .overheidnl. Er dient gewaakt te worden dat het registratieproces niet (veel) omslachtiger wordt dan in de huidige situatie. Deze starheid kan omslaan in de perceptie van een verlies van autonomie bij overheidsorganisaties waardoor ook het draagvlak voor een gTLD onder druk kan komen te staan. In een .overheid.nl situatie is sprake van een zelfde mate van starheid; voor de huidige .nl situatie blijft een bepaalde mate van vrijheid bestaan voor overheidsorganisaties om bijvoorbeeld hun eigen registrar te kiezen. Dit geldt vooral voor lagere en decentrale overheden als gemeenten en uitvoeringsorganisaties.

2.6.2.3 VERKEERDE UITVOERING

Er bestaat een kans dat de uitvoering van een gTLD verkeerd gaat. Het risico zit daarbij voornamelijk in de volledigheid waarmee van de overgang naar het nieuwe gTLD. Een halfwassen implementatie is te beschouwen als mislukt en komt neer op de facto de huidige situatie maar dan duur gekopieerd en is dus een risico. Veel kansen om het opnieuw te doen zullen er niet komen.

Belangrijk is de reikwijdte van het gTLD te bepalen: alleen rijksoverheid of inclusief alle andere overheidsinstanties als uitvoeringsorganisaties en gemeenten? De reikwijdte bepaald de complexiteit van de overgang en de kans op succes. Een mogelijk succesvol transitieproces zou kunnen zijn om te beginnen met de rijksoverheid en, nadat aangetoond is dat dit haalbaar en meerwaarde biedt, verder te verbreden naar andere (semi-)overheidsinstanties. Wellicht valt een dergelijke gefaseerde uitvoering in te passen in het huidige verbeter- en consolidatieproces dat gaan is onder rijksoverheid.nl.

Met betrekking tot de .overheid.nl situatie geldt ook een dergelijk risico, zij het dat de kosten en effort die hiermee gemoeid gaan veel male lager zullen zijn dan in een gTLD situatie. In de huidige situatie is dit risico er niet. Hier zou men zich kunnen afvragen wat er fout gegaan aangaande het aanvragen en beheren van domeinen om zodoende een beter toekomstig beleid hieromtrent uit te kunnen voeren.

2.6.2.4 VERPLICHTINGEN RICHTING ICANN

Aan het beheren van een gTLD zitten naast de controle over de uit te delen zones ook verplichtingen. Ze dwingen de beheerder bijvoorbeeld om de volledige zonefile te publiceren, om een publieke, niet afgeschermde WHOIS te draaien, en om alle transacties qua domeinregistraties en wijzigingen te publiceren op de publieke site van ICANN. Dit laatste kan vanuit overheidsperspectief soms onwenselijk zijn.

Wanneer een domeinnaam aangevraagd wordt, wordt eerst gekeken of de voorgestelde naam nog beschikbaar is. In een openbare WHOIS kan iedereen zien wie de juridische houder is van een domein. Afhankelijk van de mate van openbaarheid kan dit de privacy van de houder schenden of de mogelijkheid bieden voor derden om bijvoorbeeld e-mail adressen te gaan verzamelen met alle nadelige gevolgen van dien (spam). Afhankelijk van de afspraken die met ICANN gemaakt zijn en die contractueel zijn vastgelegd, heeft de gTLD exploitant verder minder eigen macht om diensten aan te passen of toe te voegen als het systeem eenmaal draait, waardoor ingrijpen lastig kan zijn.

Een andere verplichting is het vinden van een onafhankelijke derde partij voor data escrow. In het geval dat de houder van .overheidnl niet meer aan zijn verplichtingen kan voldoen, kan ICANN hiermee een derde partij de registry laten beheren. Een potentieel nadeel is wel dat deze derde partij alle domeinen en de (overheids)content daarop tot zijn beschikking heeft. Deze informatie is contractueel wel zwaar beschermd.

Met betrekking tot dit risico kan het volgende over de andere situaties gezegd worden:

- Huidige .nl situatie: Een voordeel van het .nl gTLD is dat ICANN hier geen beleidsmatige zeggenschap over heeft. Dit in tegenstelling tot de gTLDs, waaronder .overheidnl zou vallen, waar ICANN in grote mate het beleid bepaalt. De registry kan zelf met voorstellen komen maar heeft toestemming van ICANN nodig. Met andere woorden, een gTLD biedt minder vrijheid en het is verstandig om van tevoren goed na te denken over het vast te stellen beleid zodat dit in één keer aan ICANN kan worden voorgelegd. Ook .nl heeft escrow verplichtingen.
- .overheid.nl situatie: Hier kan de overheid zelf de spelregels (inclusief escrow) bepalen voor het second-level domein.

3 Samenvatting

De geïdentificeerde kansen en risico's per aandachtsgebied zijn samengevat in de onderstaande tabel. De tabel geeft tevens een inschatting van de meerwaarde van een gTLD t.o.v. de huidige .nl en .overheid.nl situaties.

Aandachtsgebieden	Kans of risico?	Meerwaarde t.o.v. huidige .nl situatie	Meerwaarde t.o.v. .overheid.nl situatie
Beveiliging			
Waarborgen van de echtheid van de websites	Kans	Geen	Geen
Toevoegen van additionele maatregelen	Kans	Geen	Geen
Meer controle	Kans	Beperkt	Geen
Veiligere registratie	Kans	Beperkt	Geen
Minder last van typosquatting	Kans	Beperkt	Beperkt
Toenemende complexiteit	Risico	Geen	Geen
Ontbreken van expertise	Risico	Geen	Geen
Browser blijft de zwakste schakel	Risico	Geen	Geen
Contractuele verplichtingen / beperkingen	Risico	Groot	Groot
Communicatie			
Imagoversterkend	Kans[41]	Beperkt	Beperkt
Aandachttrekkende gebeurtenis	Kans	Beperkt (tijdelijk)	Geen
Eenduidigheid en kwaliteitsverbetering	Kans	Beperkt	Geen
Betere vindbaarheid	Kans	Beperkt	Beperkt
Meer vrijheid in keuze domeinnaam	Kans	Beperkt	Geen
Verwarring bij burger	Risico	Groot	Groot
Te lange URLs	Risico	Groot	Geen
Kans op merkmisbruik	Risico	Beperkt	Geen
Overgangssituatie – legacy	Risico	Groot	Beperkt
Communicatieve transitiekosten	Risico	Groot	Beperkt
Acceptatie en draagvlak			
Greenfield situatie	Kans	Beperkt	Geen
Betere bescherming eigen merk	Kans	Beperkt	Geen
Weinig intuïtieve naam	Risico	Groot	Groot
Ontbreken van vertrouwen in de naam	Risico	Groot (tijdelijk)	Groot (tijdelijk)

[41] Mits goed uitgevoerd, anders wordt het een risico.

Onduidelijke meerwaarde	Risico	Groot	Beperkt
Efficiency en kosten			
Meer procesmatige uniformiteit	Kans	Beperkt	Geen
Hoge aanschaf- en beheerkosten	Risico	Groot	Groot
Hoge technische transitiekosten	Risico	Groot	Beperkt
Uitvoerbaarheid – beheer en inrichting			
Betrouwbare registry	Kans	Beperkt	Beperkt
Eén loket voor registratie	Kans	Beperkt	Geen
Ontbreken van governance	Risico	Beperkt	Groot
Starheid centrale registratie	Risico	Beperkt	Geen
Verkeerde uitvoering	Risico	Groot	Beperkt
Onder toezicht van ICANN	Risico	Groot	Groot

Op basis van de bovenstaande tabel valt op dat de kansen en risico's van een gTLD ten opzichte van de huidige .nl of .overheid.nl situatie vanuit beveiligingsoogpunt nauwelijks verschillen. In technische zin kan met de huidige situatie ook veel worden bereikt (zo is het .nl domein al DNSSEC beveiligd en kunnen hier additionele maatregelen als DANE en DKIM aan toegevoegd worden). De grip op de beveiliging is echter voor de .nl situatie geringer en de middelen om in te grijpen zijn beperkter. De overheid is in de huidige situatie immers afhankelijk van relatief veel externe, al dan niet commerciële, partijen. Waar het aan ontbreekt zijn heldere afspraken en procedures over het aanvragen en beheren van domeinen en het toezicht erop. Tenminste als het een overheidsbrede context betreft. De Rijksoverheid registreert de domeinnamen voor alle ministeries via een centraal punt en voert hier beleid op uit middels richtlijnen. Voor alle situaties geldt dat met de introductie van DNSSEC de complexiteit toeneemt en daarmee de kans op fouten. Expertise is vereist voor een goed beheer van een DNSSEC beveiligd domein.

Samenvattend kan geconcludeerd worden dat het met een gTLD marginaal makkelijker is om een veilig registratieproces in te richten omdat men volledige controle heeft, maar dat hetzelfde ook gerealiseerd kan worden voor .nl domeinen mits goede afspraken worden gemaakt met SIDN en de registrars voor .nl of indien men opteert over een .overheid.nl situatie. Afspraken over het niveau van beveiliging van de DNS registratie- en beheerinfrastructuur dienen sowieso aangescherpt te worden als er beveiligingsmaatregelen in of via DNS gerealiseerd worden (zoals DNSSEC, DANE of DKIM).

Voor wat betreft de communicatie is er ten opzichte van de huidige .nl en .overheid.nl situaties een beperkte meerwaarde betreffende het imago en de eenduidigheid van de overheidscommunicatie richting de burger of bedrijven. Hieraan kleeft wel een prijskaartje dat vooral bepaald wordt door transitiekosten van communicatieve aard. Dit prijskaartje is gunstiger voor het consolideren van domeinen onder .overheid.nl.

Naast de transitiekosten, die niet alleen van communicatieve maar ook van technische aard zijn, kleven er nog eenmalige en beheerkosten aan een gTLD. Deze kosten zijn echter zo hoog in vergelijking met de kosten voor de

andere situaties dat het de vraag is of dit te rechtvaardigen valt.

De acceptatie en draagvlak onder burgers en bedrijfsleven betreffende een gTLD kunnen onder druk komen te staan door het ontbreken van een duidelijke meerwaarde voor hun en de weinig intuïtieve naamgeving van overheidnl. De (t.o.v. andere situaties) marginaal betere eenduidigheid van de communicatie, herkenbaarheid van de overheid en betere beveiliging zouden aangegrepen kunnen worden om de meerwaarde van een gTLD te 'verkopen' via bijvoorbeeld een communicatie-campagne.

Met een overheidseigen gTLD vallen efficiency-slagen te behalen betreffende de vindbaarheid, authenticiteit en de uniformiteit. De hoge kosten van het beheer wegen niet op tegen de kosten van de huidige of .overheid.nl situaties. De inschatting is dat de beheerskosten van de huidige situatie door de heterogeniteit van de systemen ook aan de hoge kant zullen zijn. Het behalen van procesmatige uniformiteit is niet direct gerelateerd aan een gTLD; het is ook goed mogelijk om domeinnaamaanvragen te centraliseren via een verbeterde huidige .nl of .overheid.nl situatie. Een beperkte meerwaarde van een eigen gTLD is dat dit een greenfield situatie creëert waarin er misschien meer draagvlak is voor centralisering.

Er zijn relatief veel risico's verbonden betreffende de uitvoerbaarheid van een eigen gTLD. Het mislukken ervan door de volledigheid van de uitrol ervan verkeert in te schatten kunnen desastreus zijn voor de gTLD eigenaar; een tweede kans zal er niet komen.

Belangrijk is te zorgen voor één centraal loket voor het aanvragen van domeinen. Een dergelijk loket is goed te verantwoorden en in te richten in alle situaties. Een cruciale beslisfactor hierbij betreft de scoping van het inzetten van een dergelijk loket voor registratie van domeinnamen onder een gTLD, .nl of .overheid.nl. Welke organisaties zullen via dit loket hun domeinnamen moeten aanvragen: de gehele centrale overheid, decentrale overheden en organisaties met een publieke taak haalbaar of voor slechts een deel hiervan? Hier dient, gegeven de autonomie van sommige overheidspartijen en de relatieve vrijheid die ze nu genieten betreffende het aanvragen van domeinnamen, met beleid mee omgegaan te worden om falen te voorkomen. Een gefaseerde aanpak van het uitrollen van een gTLD onder overheidsorganisaties kan hierbij helpen: begin klein met de Rijksoverheid en zoek daarna de verbreding op bij andere overheidsorganisaties. Een dergelijke scoping is ook van belang bij het succesvol uitrollen van een .overheid.nl situatie. In de huidige situatie beperkt de scope zich tot de Rijksoverheid, maar ook hier zal rekening gehouden moeten worden met het risico van verlies van autonomie bij verbreding van een strikter registratiebeleid naar mede-overheden.

Het toezicht op de gTLD door ICANN kan ook een belemmering zijn bij de uitvoerbaarheid ervan. Een gTLD biedt minder vrijheid en het is verstandig om van tevoren goed na te denken over het vast te stellen beleid zodat dit in één keer aan ICANN kan worden voorgelegd.

Tot slot adresseren we de onderzoeksvragen zoals gesteld in de inleiding.

Beveiliging	• Welke eisen moeten gesteld worden om de overheidscommunicatie te beveiligen? • Hoe het toezicht te regelen over deze beveiligingseisen en de handhaving ervan? • Wat is de toegevoegde waarde van een gTLD voor de beveiliging van websites? • Wegen de kansen en risico's van het inzetten van een gTLD als beveiligingsmaatregel op tegen die van de huidige beveiligings-maatregelen in het .nl domein?	• De eisen die gesteld moeten worden aan het beveiligingen van de overheidscommunicatie zijn bij een gTLD niet anders dan in de huidige, .nl, situatie. Alleen verschilt de uitvoering ervan in beide modellen. • In een gTLD situatie is de toezicht op het handhaven van de beveiliging makkelijker te regelen omdat er minder partijen bij betrokken zijn. • De toegevoegde waarde van een gTLD voor de beveiliging van websites is beperkt t.o.v. de andere situaties. • Vanuit beveiligingsperspectief zijn de voordelen van een gTLD t.o.v. de huidige situatie marginaal.
Communicatie	• Kan met behulp van een gTLD de echtheid van de overheidswebsites beter geborgd worden? • Kan er vanuit de overheid op een betrouwbare manier elektronisch met burger en bedrijfsleven gecommuniceerd worden via bijvoorbeeld portalen? • Hoe zit het met de schaarste aan domeinen?	• De echtheid kan marginaal beter geborgd worden omdat typosquatting lastiger wordt. • Dat kan zowel met een gTLD als in de huidige situatie. De authenticiteit van open (overheids)data kan marginaal beter gegarandeerd worden met een gTLD. • Er is sprake van schaarste aan domeinen maar dit mag geen excuus zijn voor de aanschaf van een gTLD.
Efficiëntie en kosten	• Wordt het met een gTLD makkelijker om overheidsinformatie te vinden? • Wegen de baten van een gTLD op tegen de kosten (inclusief benodigde infrastructuur, beheer, toezicht en migratie)? • Hoe zit het met de kosten waaronder het beheer van de gTLD, de jaarlijkse bijdragen aan ICANN ($25.000), voor de migratie, communicatie en marketing? Welke factoren zijn er nog meer die de kosten van een gTLD bepalen en hoe hoog zijn deze kosten? Wegen deze op tegen de huidige kosten van de overheidsdomeinen?	• De vindbaarheid wordt beperkt beter. Zoekmachines en mobiele platformen met apps maken dat de URL van een website minder belangrijk wordt. • De kosten zijn relatief hoog en de baten zijn daarbij moeilijk te kwantificeren. Anders dan publieke gTLDs staan er geen inkomsten tegenover via de verkoop van subdomeinnamen. • Een grote kostenpost is de migratie naar een gTLD model. De huidige situatie is te kenmerken als goedkoop. Een nieuwe situatie met eigen gTLD is ordegroottes duurder per jaar.
Maatschappelijke acceptatie	• Wat vinden burgers en bedrijven van een gTLD in het algemeen? • Wat vinden burgers en bedrijven van een overheidseigen gTLD in het bijzonder? • Wat is de meerwaarde voor burgers en bedrijven? • Wat is nodig om vertrouwen te winnen?	• Bedrijven zijn terughoudend. De vraag is of burgers om zullen kunnen (leren) gaan met de nieuwe gTLDs en de weinig intuïtieve naam van overheidnl dat indruist tegen de gebruikelijke taxonomie. • Veel burgers en bedrijven hebben geen mening over een overheidseigen gTLD. • De meerwaarde voor burgers en bedrijven is onduidelijk. • Een degelijke marketing campagne zal nodig zijn om het vertrouwen in de gTLD te winnen. Dit brengt ook kosten met zich

		mee.
	• Is een marketing/promotie campagne noodzakelijk?	• Ja. Een dergelijke campagne zal zich ook moeten richten op het 'heropvoeden' van burgers om de juiste (niet intuïtieve) URL te gebruiken (.overheidnl i.p.v. overheid.nl).
	• Wat is de acceptatie van beveiligingsmaatregelen als DANE en DKIM in de internetgemeenschap, bijvoorbeeld onder browser vendors en makers van (mobiele) besturingssystemen?	• De verwachting is dat dergelijke aanvullende beveiligingsmaatregelen die gebruik maken van DNS in de nabije toekomst steeds meer gemeengoed gaan worden. DKIM wordt al gebruikt.
	• Kunnen webbrowsers en mobiele OSs en apps overweg met beveiligings-maatregelen als DANE en DKIM?	• Voorlopig nog niet.
Bestuurlijke acceptatie	• Wat vinden de verschillende overheidsinstanties van een overheidseigen gTLD?	• Door de beperkte meerwaarde geldt ook binnen de overheid enige terughoudendheid voor een overheidseigen gTLD.
	• Hoe ziet de regievoering van een overheidseigen gTLD eruit en willen bestuurders zich hier aan conformeren?	• Een centrale regie zou wenselijk zijn. Een gTLD opent de weg naar één centraal loket voor het aanvragen van domeinnamen.
	• Is het vanuit kansen- en risico-oogpunt wenselijk om de overheid regie te laten voeren op een overheidseigen gTLD DNS structuur met bijbehorende grip op beveiligingseisen en standaarden?	• Ja, dit is wenselijk en zorgt voor betere controle en toezicht en biedt uniformiteit.
	• Biedt de greenfield situatie kansen? Zoja, welke? Wat zijn de risico's?	• De greenfield situatie biedt kansen en kan bijdragen aan het creëren van draagvlak.
	• Hoe om te gaan met andere partijen die een gTLD hebben aangevraagd zoals de gemeente Amsterdam en de politie?	• Dit zijn open gTLDs met een andere insteek/motivatie. Voorlopig hoeft hier geen rekening mee gehouden te worden.
	• Scoping: Is het inzetten van een gTLD voor de gehele centrale overheid, decentrale overheden en organisaties met een publieke taak haalbaar of voor slechts een deel hiervan?	• Dit zal afhangen van het draagvlak en de kosten die ermee gemoeid zijn. Soms is het niet wenselijk om een website onder overheidsvlag te voeren. Hiervoor zal beleid moeten worden opgesteld. Het kiezen van een te brede scope kan risico's met zich meebrengen doordat de kans van slagen van het uitrollen van een gTLD ermee kleiner wordt (door gebrek aan draagvlak en/of hoge kosten). Verstandig is met een heldere en beperkte scope te beginnen.
Uitvoerbaarheid	• Hoe ziet een mogelijke inrichting van de bij een gTLD behorende functies op hoofdlijnen eruit?	• De inrichting geniet bij voorkeur een enkele registrar en een registry welke uitbesteed wordt.
	• Hoe ziet de governance structuur eruit?	• De overheid (MinAZ) houdt toezicht op de registratie van domeinen onder .overheidnl.
	• Wie zijn geautoriseerde registrars en hoe ziet het proces van domeinnaamregistratie er onder het overheidnl gTLD uit. Welke eisen moeten aan registrars gesteld worden? Wat zijn hierbij de overwegingen?	• MinAZ is een registrar. Een alternatief is om de huidige situatie te verbeteren door het aantal registrars te beperken en strengere beveiligingsmaatregelen te eisen voor registratie van overheidswebsites door de geselecteerde registrars. Dit betreft bijvoorbeeld sterke(re) authenticatie en strikte procedures voor het uploaden en verversen van (DANE) certificaten en (DNSSEC) encryptiesleutels.

Interviews, expertsessie en reviewers

3.1 INTERVIEWS

Organisatie	Naam	Functie
vtsPN	Aad Koppenhol	Senior Architect
Gemeente Amsterdam	Egbert Wolf	Senior Communicatie Adviseur
Ministerie van Economische Zaken, Landbouw en Innovatie	Thomas de Haan	Beleidsmedewerker en ICANN vertegenwoordiger namens de overheid.
SURFnet	Roland van Rijswijk – Deij	Technisch Product Manager en DNS expert
Red Hat	Paul Wouters	DNSSEC en DANE expert
NLnetLabs	Matthijs Mekking	DNSSEC expert
ISC.org	Jelte Jansen	DNSSEC expert
Nominet UK	Roy Arends	Onderzoeksleider en DNSSEC expert
Ministerie van Algemene Zaken	Erik den Hoedt	Directeur Dienst Publiek en Communicatie
Ministerie van Algemene Zaken	Rob Klaassen	Senior Adviseur
Ministerie van Algemene Zaken	Marc van de Graaf	Media Adviseur
DNS.be	Philip du Bois	General Manager
ISOC.nl	Michiel Leenaars	Bestuurslid
ISOC.nl	Dick Kalkman	Bestuurslid

3.2 EXPERTSESSIE

Organisatie	Naam	Functie
Logius	Agnes de Wit	Hoofdredacteur overheid.nl
Gemeente Den Haag	Patrick Rancuret	Adviseur Communicatie
Belastingdienst / CKC	Dennis Boehmer	Proces- en projectmanager
Belastingdienst / CKC	Jan Langenberg	Communicatie Adviseur
RIVM	Liesbeth Rentinck	Communicatie Adviseur

3.3 EXTERNE EN INTERNE REVIEWERS

Organisatie	Naam	Functie
SIDN	Hubert Welleman, Esther Makaay & Marco Davids	New Business Manager, service architect & technisch adviseur
SURFnet	Roland van Rijswijk – Deij	Technisch product manager en DNS(SEC) expert
Novay	Maarten Wegdam	Managing advisor