> LINK NAAR TEKSTVERSIE IN HTML

PBLQ

Buitenlandonderzoek Domeinnaambeleid

Eindrapport
project 006976
versie 1.0
27 november 2019

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

De directie Informatiesamenleving en Overheid van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) is door de staatssecretaris gevraagd om een verkennend onderzoek te doen naar de wenselijkheid en haalbaarheid van de invoering van een uniforme domeinnaamextensie voor de overheid. Dit onder andere naar aanleiding van eerder uitgevoerde onderzoeken en de behoefte om waar nuttig en mogelijk de herkenbaarheid, vindbaarheid en veiligheid van overheidsinformatie te vergroten.

Binnen de directie is een aantal onderzoekslijnen uitgezet. Eén daarvan is een verkenning naar de situatie inzake het domeinnaambeleid bij buitenlandse overheden, met de gedachte erachter om te leren van hun overwegingen en ervaringen bij het al dan niet toepassen van een domeinnaambeleid.

Aan PBLQ is gevraagd dit onderzoek uit te voeren.

1.2 Opdrachtformulering

De opdracht voor het buitenlandonderzoek is als volgt:

Voer een survey uit naar de wijze waarop buitenlandse overheden al dan niet invulling geven aan een domeinnaambeleid en geef op basis van de resultaten antwoord op de volgende vragen:

1. *In welke mate maken buitenlandse overheden gebruik van een domeinnaambeleid? Wat is het werkingsgebied? In welke mate heeft het beleid een verplicht karakter en, zo ja, hoe wordt daarop gehandhaafd?*
2. *Welke overwegingen hebben een belangrijke rol gespeeld bij de keuze voor het hebben en invoeren van een domeinnaambeleid of juist het niet hebben en niet invoeren daarvan?*
3. *Wat zijn de te leren lessen als het gaat om de implementatie van een domeinnaambeleid?*
4. *In welke mate zijn er evaluaties uitgevoerd op het effect van een domeinnaambeleid op bijvoorbeeld de herkenbaarheid en veiligheid van overheidsinformatie op het internet?*

Geef op basis van de onderzoeksresultaten een korte samenvatting of en hoe buitenlandse overheden een domeinnaambeleid inzetten en welke kritische succesfactoren daaruit gehaald kunnen worden waar de werkgroep haar voordeel mee kan doen.

Opdrachtgever voor deze onderzoeksopdracht is de directie Informatiesamenleving en Overheid van het ministerie van BZK. Het onderzoek is begeleid door de werkgroep ‘Herkenbare en Betrouwbare Digitale Overheid’, onder projectleiderschap van de heer R. Ramdjielal.

1.3 Werkwijze

Het onderzoek is uitgevoerd door Piet Hein Minnecré, Matthijs Kerkvliet, Jinne Samsom en Marcel Bom, allen adviseur/onderzoekers van PBLQ. Het onderzoek is uitgevoerd in de periode augustus/

november 2019. Een werkgroep met daarin vertegenwoordigers vanuit verschillende bestuurslagen (Rijk, provincie, gemeenten, waterschappen, alsmede experts vanuit Forum Standaardisatie en het Nationaal Cyber Security Centrum) is nauw betrokken geweest bij de opzet van het onderzoek en de bespreking van de resultaten.

In gezamenlijk overleg met de werkgroepleden is gestart met het formuleren van de relevante onderzoeksvragen (zie bijlage B). Deze vragen zijn de basis geweest voor het opstellen van een tweetal surveys. Beide surveys bevatten een ingekorte set van de onderzoeksvragen, om daarmee de respons zo hoog mogelijk te maken. De ene survey is via CENTR (**C**ouncil of **E**uropean **N**ational **T**op-Level Domain **R**egistries) uitgezet bij haar leden, waar de Nederlandse SIDN (Stichting Internet Domeinregistratie Nederland) lid van is. De andere survey is uitgezet via het Europese netwerk van het ministerie van BZK bij buitenlandse overheidsorganisaties.

Daarnaast is op basis van deskresearch door de onderzoekers een verkenning gedaan naar relevante informatie over domeinnaambeleid bij buitenlandse overheden op het internet.

Op basis van de eerste surveyresultaten en de deskresearch is in overleg met de werkgroep een lijst van acht landen opgesteld voor nader onderzoek om zo ook antwoorden te krijgen op een aantal verdiepende vragen. Het verdiepend/nader onderzoek is gedaan aan de hand van telefoongesprekken. Voor nader onderzoek in aanmerking komende landen waren: Canada, Estland, de Europese Commissie, Italië, Oostenrijk Nieuw-Zeeland, Portugal, Verenigd Koninkrijk (VK), Verenigde Staten van Amerika (VS) en Vlaanderen[1]. Uiteindelijk is met zes landen uitvoerig telefonisch contact geweest. Vertegenwoordigers van de Europese Commissie en de landen Portugal en Nieuw-Zeeland hebben via e-mail een uitgebreide reactie gegeven. Gespreksverslagen hiervan zijn opgenomen onder bijlage D. Het leggen van contact met Estland bleek binnen de onderzoeksperiode niet haalbaar.

Alle onderzoeksresultaten zijn bij elkaar gebracht, geordend naar kwantitatieve (meetbare) informatie en kwalitatieve informatie, geanalyseerd en verwerkt in deze rapportage. Voorts zijn de onderzoeksresultaten input geweest voor de gevraagde samenvatting inclusief de verzamelde kritische succesfactoren als advies voor de werkgroep.

1.4 Indeling rapport

Het rapport is als volgt ingedeeld. Hoofdstuk 2 bevat een overzicht van de onderzoeksresultaten. Waar mogelijk is gebruik gemaakt van overzichten om tot generieke inzichten te komen. Hoofdstuk 3 gaat middels een aantal grafieken in op een aantal onderwerpen die op basis van deze studie naar voren komen als belangrijk in de keuze voor een eventueel domeinnaambeleid. Hoofdstuk 4 bevat de samenvatting en de kritische succesfactoren.
Daarnaast bevat deze rapportage een aantal bijlagen met daarin onder andere de gebruikte vragenlijsten, de ontvangen reacties uit de uitgezette surveys en de gespreksverslagen van de telefonisch afgenomen interviews.

[1] Strikt gezien zijn de Europese Commissie en Vlaanderen natuurlijk geen land, maar voor de eenvoud in schrijfwijze zullen wij ze in het vervolg van dit rapport wel zo betitelen

2. Bevindingen

Dit hoofdstuk bevat de resultaten van het uitgevoerde onderzoek. De resultaten zijn geordend naar de vier hoofdthema's zoals die ook bij het formuleren van de vragenlijst naar voren kwamen, te weten:

- De inhoud van het beleid;
- De rationale achter het beleid;
- Implementatievraagstukken;
- Effect van het beleid.

Daar waar zinvol en mogelijk zijn de resultaten schematisch weergegeven. De ruwe informatie is deels opgenomen in de bijlagen. Het volledige pakket aan ruwe data wordt bij oplevering van de definitieve rapportage overgedragen aan de opdrachtgever.

2.1 Inhoud van het domeinnaambeleid

2.1.1 Functionele scope

Uit het onderzoek blijkt dat er verschillen zijn in de functionele scope van het beleid. Grofweg valt deze uiteen in drie delen:

1. In de meeste gevallen is er sprake van een generiek domeinnaambeleid dat gericht is op het ondersteunen van herkenbare en betrouwbare overheidscommunicatie op het internet. Het beleid richt zich vooral op de naamgeving van de websites die informatie van de overheid verstrekken.
2. Daarnaast wordt in enkele gevallen ook digitale dienstverlening onder het beleid opgenomen. Daarbij wordt wel aangegeven dat de technische complexiteit hiervan hoger is.
3. In het onderzoek zijn we nauwelijks partijen tegengekomen die structureel gebruik maken van de uniforme domeinnaam voor e-mail overheidsbreed. De reden die hiervoor aangedragen wordt is dat dit de technische complexiteit sterk zou verhogen, onder meer omdat e-mailadressen ook gebruikt worden als autorisatie voor diverse applicaties en systemen en e-mailadressen tot in de 'haarvaten' van operationele informatieprocessen zijn opgenomen.

Daar waar een overheid inzet op één generieke website voor overheidscommunicatie (en soms ook digitale dienstverlening) is er eigenlijk sprake van een beleid om de overheidscommunicatie te concentreren via een centraal platform. De website GOV.UK is hier een goed voorbeeld van. Overigens komen we deze oplossing vaker – en met een groeiende belangstelling – tegen. De aangetroffen voorbeelden in Vlaanderen, het VK, Zweden, Noorwegen, Slovenië, Portugal, Polen, alsook Canada, zijn hier representanten van.
In deze gevallen leidt de platform-oplossing eveneens tot aanpassingen van de eraan verbonden domeinnamen. Voor de aanpassing van domeinnamen wordt dan doorgaans wel de benodigde tijd gereserveerd. In Vlaanderen wordt hiervoor vier jaar uitgetrokken, Canada bevindt zich in een transitieperiode sinds 2013. Kijkend naar GOV.UK als platform zien we op dit moment nog steeds een aantal gerelateerde websites actief onder hun eigen 'vertrouwde' naam, terwijl het programma om tot de centrale website te komen liep tijdens het kabinet Cameron.

In een groter aantal gevallen richt de overheid zich op een generiek domeinnaambeleid, waarbij het gebruik van een second-level domain wordt nagestreefd. Voorbeelden hiervan zijn Italië, Frankrijk,

Oostenrijk, Nieuw-Zeeland, Australië, Japan, VS, alsook het VK. Deze lijst is niet uitputtend. Het geeft wel een beeld dat een behoorlijk aantal overheden een uniform domeinnaambeleid inzetten om vooral de betrouwbaarheid en herkenbaarheid van overheidscommunicatie te verbeteren. Hierbij geldt in de meeste gevallen dat het uniforme domeinnaambeleid 'vrijwillig' is, en de adoptie ervan toeneemt naarmate er meer diensten rondom worden aangeboden (denk aan eenvoudige en soms ook betaalde registratie, beveiligingsmaatregelen, vertaalservices, etc.).

Een beleid gericht op het gebruik van uniforme e-mailadressen door de gehele overheid heen, is niet of slechts in beperkte zin aangetroffen. In verschillende landen zijn voorbeelden aangetroffen waar een overheidsorganisatie gebruik maakt van een e-mailadres dat is afgeleid van de generieke domeinnaam. Bijvoorbeeld in het VK (*@justice.gov.uk) of Oostenrijk (*@stmk.gv.at). Hierbij moet echter een belangrijke reservatie worden gemaakt. Er is namelijk (nog) geen sprake van een consequente toepassing van naamgevingsbeleid voor e-mailadressen. Bij veel overheden zien we nog een diffuus beeld wat betreft toepassing van een uniform naamgevingsbeleid voor e-mailadressen. Zo zijn binnen de centrale overheid van het VK naast '.gov-adressen' ook *@officeforstudents.org.uk in gebruik en maakt het defensieapparaat gebruik van eigen e-mailadressen, etc. Onze ervaring uit directe communicatie met buitenlandse overheden is dat onder overheidsfunctionarissen geen consequent gebruik waarneembaar is. Dit laat onverlet dat in veel landen e-mailadressen zijn aangetroffen waarin een overheidsextensie is opgenomen.

Een uitzondering op het bovenstaande beeld troffen wij aan in Luxemburg. Hier worden alle organisaties uit de centrale overheid verplicht om gebruik te maken van het format first-name.surname@organization-abreviation.etat.lu. .etat (letterlijk: staat) geldt hier als overheidsextensie. De Luxemburgse respondent geeft aan dat het naamgevingsbeleid rondom e-mailadressen reeds bestaat sinds de jaren 90 en niet is geïntegreerd met domeinnaambeleid dat pas in 2002 werd gedefinieerd. Opvallend is dat de extensie .etat niet terugkomt in de websitedomeinen die door overheidsorganisaties worden gebruikt (.gouvernement). Er is bovendien geen poging ondernomen om deze twee extensies te uniformeren.

Uit de interviews en surveys maken we op dat het onderwerpen van alle e-mailadressen aan een uniform naamgevingsbeleid weerbarstig is. Als reden hiervoor wordt veelal de technische complexiteit genoemd. Omdat e-mailadressen veeltijds ook worden gebruikt als vorm van authenticatie en autorisatie (Identity Access Management) is het een veeleisend en moeilijk proces om ze te migreren naar uniforme e-mailadressen. Soms zelfs zo veeleisend, en kostbaar, dat landen (bijvoorbeeld Vlaanderen en Oostenrijk) expliciet ervoor kiezen om het e-mailbeleid niet te integreren in het domeinnaambeleid.

2.1.2 Organisatorische scope

Een tweede scope-aspect, en relevant voor het vraagstuk over de reikwijdte van het domeinnaambeleid, betreft het organisatorische werkingsgebied van het beleid: op welke overheden richt het beleid zich?

Centraal vs. decentraal
In veruit de meeste gevallen waar er sprake is van een domeinnaambeleid op landelijk niveau, geldt dat het beleid niet een-op-een wordt vertaald naar regionale en lokale bestuurslagen. Als er al sprake is van een landelijk dekkend beleid op dit punt, dan geldt dat regionale en lokale overheden de mogelijkheid hebben om gebruik te maken van voorzieningen die op landelijk niveau zijn/worden

ontwikkeld, maar dat er geen sprake is van een verplichting. Het domeinnaambeleid concentreert zich dientengevolge vooral op centrale overheden. Hieronder verstaan wij (federale) departementen en agentschappen en/of uitvoeringsorganisaties.

Bij navraag over de redenen hiervoor komt in de interviews naar voren dat de inrichting van het staatsbestel veruit de belangrijkste overweging is. In de meeste gevallen wordt het als een onwenselijke aantasting van de autonomie van de te onderscheiden bestuurslagen binnen een land gezien om eisen te stellen aan de (website)naamgeving van decentrale overheden.

Als het gaat om het toepassen van een domeinnaambeleid voor zowel centrale als lokale overheden, is het VK een goed voorbeeld. Daar maken de centrale, regionale en lokale overheden gebruik van *.gov.uk. De centrale overheid maakt aanvullend gebruik van een gezamenlijk platform, www.gov.uk/*. Ook Australië geldt als land waar het gebruik van het overheidsdomein (*.gov.au) voor zowel centrale als decentrale overheid kan worden aangemerkt als structureel hoog. Bijzonder is dat in geen van deze genoemde gevallen er sprake is van verplicht gebruik van het domeinnaambeleid op decentraal niveau. In het VK wordt strikt onderscheid gemaakt tussen het domeinnaambeleid enerzijds en de beleidsvoorschriften binnen de centrale overheid om tot één GOV.UK platform te komen anderzijds. Beide bestaan naast elkaar. Een verplicht domeinnaambeleid voor de gehele overheid, centraal en lokaal, troffen wij alleen aan in Italië. Het gebruik van de overheidsextensie ‘gov.it’ is echter structureel laag door decentrale overheden en wordt bovendien niet op gehandhaafd.

Kerndepartementen vs. overige centrale overheidsorganisaties
Bij centrale overheden wordt doorgaans onderscheid gemaakt tussen de kerndepartementen en agentschappen/uitvoeringsorganisaties. Sommige landen hebben het dan over de directe of indirecte overheden, en andere maken nadrukkelijk het onderscheid tussen beleidsorganisaties en uitvoerende organisaties. Grosso modo maakt iedere centrale overheid een onderscheid zoals wij dat in Nederland kennen: kerndepartementen vs. overige centrale overheidsorganisaties (waaronder agentschappen en ZBO’s).

Voor veel van de onderzochte buitenlandse overheden geldt dat het domeinnaambeleid juist op de kerndepartementen van toepassing is. Voor agentschappen en uitvoeringsorganisaties zien we dat het gebruik van een overheidsdomein minder structureel en eerder vrijblijvend van aard is. Het bovendien integreren van daadwerkelijke diensten en/of voorzieningen via een centrale website zien we in nog minder gevallen terug.
Een goed voorbeeld waarbij de invoering van een centraal platform (lees: centrale website) uiteindelijk ook effect heeft op het gebruik van het domeinnaambeleid, is de centrale overheid van het VK. Sinds 2014 is er een verplicht gebruik van de centrale website GOV.UK waarmee ook het domeinnaambeleid wordt ondersteund. Vanaf dat moment geldt dat alle centrale overheidsdiensten, zowel de departementen als de uitvoerende diensten er gebruik van dienen te maken. Bij het feitelijke raadplegen van de website valt op dat een aantal diensten nog steeds ofwel in de transitie zitten, ofwel een uitzonderingspositie genieten.

Dit voorgaande laat onverlet dat een frequent aangetroffen implementatie van domeinnaambeleid door en bij buitenlandse overheden sterk lijkt op datgene wat op dit moment het vigerende beleid is binnen de Nederlandse Rijksoverheid (het platform Rijksoverheid Online met als onderdeel daarvan de website Rijksoverheid.nl). Een beleid waarbij de kerndepartementen hebben afgesproken om gebruik te maken van centraal ingerichte voorzieningen, met de toevoeging dat er altijd uitzonderingen

op de regel gelden. Van het Nederlandse beleid in dezen, ‘comply or explain’, gaat min of meer dezelfde werking uit.

2.1.3 Verplichten en handhaven vs. verleiden

Het onderzoek wijst uit dat de meeste overheden niet kiezen voor absoluut verplichten en handhaven van het gebruik van een uniforme domeinnaam. Deels heeft dat te maken met de inschatting dat een stevige verplichting een weinig succesvolle strategie is en juist weerstand opwekt. Daarnaast wordt aangegeven dat verplichte implementatie ook de nodige kosten en praktische drempels opwerpt.

Een voorbeeld waarbij verplichting niet per definitie leidt tot doorvoering en dus implementatie van het domeinnaambeleid is Canada. In 2013 werd daar vanuit de regering gestuurd op het instellen van een centraal platform, canada.ca. Alhoewel het beleid alle overheidsorganisaties op het centrale niveau voorschreef om hun website te migreren naar dit platform, bleek na vijf jaar dat lang niet alle organisaties hier gehoor aan hadden gegeven. Hierop is vervolgens besloten om naast de formele verplichting een verleidingsstrategie toe te passen. De door ons gesproken Canadese respondenten gaven aan dat het aanbieden van een zogezegde ‘carrot’ effectiever werkt dan het hanteren van een ‘stick’.

Praktisch betekent dit dat organisaties in niet langer verplicht zijn hun domeinnaam te migreren naar het centrale platform, maar ook gebruik mogen maken van canada.ca als second-level domein. Dit blijkt vooral voor uitvoeringsorganisaties die digitale services leveren een uitkomst te zijn. Daarnaast gaan medewerkers van de dienst ‘Digital Transformation Office’, verantwoordelijk voor de implementatie van het domeinnaambeleid, ook actief met organisaties die niet aan het beleid conformeren in gesprek om hen te overtuigen van de noodzaak van een uniform domein. Deze door hen genoemde ‘innovators’, webbeheerders die een afwijkend ontwerp hanteren van Canada.ca, worden zelfs uitgenodigd om plaats te nemen in een werkgroep waarin samen wordt nagedacht over de verbetering van de overheidsuitstraling en huisstijl. Al met al is de Canadese verwachting dat deze uitnodigings- of verleidingsstrategie veel beter werkt dan de vigerende verplichting.

Ondanks dat weinig landen verplichten beoordelen als succesfactor van het doorvoeren van een domeinnaambeleid, dient wel te worden opgemerkt dat hoog-bestuurlijke sturing van een nieuw of aangepast domeinnaambeleid (wel) effect sorteert. Het VK geldt hier als voorbeeld. Ten tijde van het kabinet Cameron is werk gemaakt van de Digitale Agenda met als gevolg dat nu alle centrale overheidsdiensten gebruik maken van beschikbaar gestelde voorzieningen (GOV.UK website) waarmee het domeinnaambeleid wordt geschraagd. Dat hiertoe een totaalpakket van maatregelen was getroffen om de overstap aantrekkelijk te maken, mag niet onvermeld blijven. Evenmin het feit dat de invoering van de Digitale Agenda kon steunen op politiek draagvlak.

Een ander voorbeeld waar centrale sturing leidt tot implementatie van een centraal domeinnaambeleid zijn onze zuiderburen. Niet België maar Vlaanderen. Binnen de Vlaamse overheid is recentelijk besloten om een stringent domeinnaambeleid in te voeren. Vanuit de centrale overheid wordt de implementatie gefaciliteerd en voor de implementatie is vier jaar uitgetrokken. Uit het interview met de Vlaamse vertegenwoordiger blijkt dat implementatiesstrategie gebaseerd zal zijn op een verleidingsstrategie.

Omdat veruit de meeste landen er niet voor kiezen om het domeinnaambeleid te verplichten, heeft het onderwerp handhaven weinig aandacht. Daar waar de verplichting wel geldt, althans dat blijkt uit de surveyresultaten van de door ons onderzochte landen, hebben de overheden gekozen voor strikte

centrale voorzieningen waardoor er kort geformuleerd voor de overheidsdiensten die onder de werking van het beleid vallen er geen ontkomen aan is. Zowel in het VK als in Vlaanderen is gekozen voor een platform-oplossing in plaats van een domeinnaam-oplossing.

2.1.4 Een overheidsplatform versus een domeinnaam

Als we kijken naar de technische wijze waarop overheden vormgeven aan hun domeinnaambeleid, komen twee oplossingen voor de technische inrichting naar voren:

1. De eerste inrichtingsvorm noemen wij het 'DNS-concept' en is meer cryptisch te omschrijven als **.gov.cc*. Het beleid bestaat uit het aanbieden van een second-level domain (in de VS een top-level domain).
2. De tweede inrichtingsvorm duiden wij aan als 'platform-oplossing'. De tweede vorm bestaat uit het gebruik maken van één centraal platform waaronder in ieder geval de departementen zijn geïntegreerd. De cryptische omschrijving daarvan is *gov.cc/*.*

Verreweg de meeste landen die een centraal domeinnaambeleid voeren, maken gebruik van het DNS-concept. Bijzonder is echter dat juist twee overheden – Vlaanderen en VK – waar al een domeinnaambeleid voor de centrale overheid van kracht was (alhoewel niet verplicht), aanvullend gebruik maken van de platform-oplossing waarbij het de ambitie is om ook diensten via het platform te leveren. In beide gevallen gaat een dergelijk gemeenschappelijk platform veel verder dan alleen het gebruik van de domeinnaam. Het is onderdeel van een veel breder pakket aan maatregelen met daarin onder meer aandacht voor:

- Richtlijnen voor toegankelijkheid;
- Het realiseren van een rijksbrede uniforme gebruikerservaring (designrichtlijnen, UX) en uitstraling (marketing);
- Centrale infrastructuur waardoor relatief eenvoudig gebruikt gemaakt kan worden van gedeelde voorzieningen/modules voor onder meer authenticatie en autorisatie;
- Beveiliging;
- Privacy.

In het geval van het VK en Vlaanderen wordt het efficiënt aanwenden van budget voor online aanwezigheid en dienstverlening als belangrijke reden voor het gebruik van een centraal platform genoemd.

Sommige overheden die op dit moment het DNS-concept hanteren, zijn minder gecharmeerd van de platform-oplossing, met hierbij de redenatie dat de voltallige overheid wel erg afhankelijk zou worden van het functioneren van dat platform. De mogelijkheid van het offline gaan van het platform als single point of failure wordt als een groot risico en nadeel van de platform-oplossing beschouwd. Als ander bezwaar tegen de platform-oplossing wordt de relatieve autonomie van uitvoerders en agentschappen genoemd.

Ook in landen als Zweden, Noorwegen, Canada en Polen zien we de platform-oplossing terugkomen. Het verschil met de oplossingen in het VK en Vlaanderen is dat in deze gevallen de websites die te vinden zijn via het centrale platform vooral een informatieverschaffingsfunctie hebben. Digitale diensten zoals het aanvragen van subsidies, het doen van belastingaangifte, etc. zijn (nog) niet geïncorporeerd. Dit lijkt sterk op de huidige situatie in Nederland (de website Rijksoverheid.nl).

Waar een select groepje landen dus gebruik maakt van een platform-oplossing, zien we bij veel andere landen het bestaan en gebruik van een overheidsportaal. Op een dergelijk portaal is de contactinformatie van verschillende overheden en overheidsdiensten voor burgers op een overzichtelijke manier te vinden. Een overheidsportaal dient daarmee primair een 'wegwijs'-functie door simpelweg koppelingen te bieden naar andere overheidswebsites. Een voorbeeld van een overheidsportaal vonden wij onder andere in Italië, de *Indicepa*. In Nederland kan overheid.nl worden gezien als voorbeeld van een overheidsportaal.

2.1.5 Naamgevingsbeleid

Uit alle gevoerde diepte-interviews met buitenlandse respondenten komt naar voren dat een effectief naamgevingsbeleid van cruciaal belang is bij het neerzetten een domeinnaambeleid. Grofweg zijn er een aantal keuzes te maken ten aanzien van dit onderdeel van het beleid:

- De meeste overheden staan het gebruik van de naam van de instantie toe, bijvoorbeeld gov.uk/homeoffice. Daarnaast worden in sommige gevallen ook onderwerpen toegestaan, bijvoorbeeld https://www.gov.uk/brexit.
- De wijze waarop beslissingen over uit te geven namen worden genomen. Daarbij wordt vaak gewerkt met criteria en aanvullend een orgaan in de vorm van een naamgevingsommissie dat hierover besluiten kan nemen en zich ook kan uitspreken in situaties waar er sprake is van onzekerheid of ambiguïteit. Deze taak wordt vaak gedelegeerd naar een aparte registrar, omdat de procedures voor het registreren van een domein door een overheidsorganisatie meestal afwijken van de procedure voor particulieren of bedrijven. Een voorbeeld hiervan is dat niet langer geldt 'first come, first serve'. De naamgevingscommissie die verantwoordelijk wordt voor de uitgifte van overheidsdomeinen is in veel gevallen onderdeel van de overheid zelf (in Vlaanderen bijvoorbeeld het agentschap 'Informatie Vlaanderen') of nauwe banden onderhoud met de overheid (in Oostenrijk bijvoorbeeld de universiteit).
  In correspondentie met buitenlandse expert wordt veelal teruggegeven dat het instellen van een dergelijke naamgevingscommissie bijdraagt aan een succesvolle doorvoering van het beleid.

2.2 Doelen en overwegingen van het beleid

In dit onderzoek hebben we de nodige aandacht besteed aan het achterhalen van de doelen en overwegingen bij het beleid. In bijna alle gevallen wordt een combinatie van de volgende factoren genoemd:

- Herkenbaarheid;
- Vindbaarheid;
- Betrouwbaarheid;
- Veiligheid;
- Beheerbaarheid.

Lang niet alle onderzochte landen zijn binnen de beschikbare beleidsdocumenten of in hun informatievoorziening op overheidswebsites transparant over de redenen achter het beleid. In de aangetroffen beleidsdocumenten zien we veelal een combinatie van factoren waarmee een

domeinnaambeleid wordt gemotiveerd. Het is meestal onduidelijk welke van de vijf factoren het zwaarste weegt. De citaties hieronder dienen als korte impressies hiervan.

"The sites of the central administrations and deconcentrated services will be housed in [.gouv.fr] in order to allow an identification unambiguous specification of public sites, in which users can have trust."[2]

"Using a govt.nz domain name improves the trust and integrity of communications from government."[3]

"The establishment of a common public administration network requires (…) a structuring of the symbolic namespace. The policy aims to make the image of public administration appear uniform on the Internet and to guarantee compliance with various security and organisational requirements and applies in particular to government domains or " gv.at" domains."[4]

"The websites of the ministries and agencies will increase the transparency of the activities of administrative agencies and aim to realize open administration."[5]

Een kwantificatie van deze gegevens is uiteengezet in figuur 4 in hoofdstuk 3.
Algeheel valt op dat de factoren en beweegredenen eigenlijk niet verder geoperationaliseerd worden, laat staan dat ze meetbaar worden gemaakt. Het is voor overheden daarom ook niet te bepalen in hoeverre een uniform domeinnaambeleid daadwerkelijk aan bovengenoemde factoren bijdraagt. We komen hier later in dit hoofdstuk op terug.

Ten aanzien van vindbaarheid kwam uit het interview met de Vlaanderen een interessant punt expliciet naar voren. Zij anticiperen met hun oplossing op hetgeen dat bij internetgebruik al langere tijd aan de gang is: mensen surfen niet meer naar een specifieke website maar stellen een (gesproken) vraag aan een zoekmachine, zoals Google en Bing, of een digitale assistent, zoals Siri, die hen vervolgens leidt naar de meest waarschijnlijke plekken op internet waar zij hun informatie kunnen vinden. Door overheidsinformatie via een centraal kanaal of platform aan te bieden, zo is de

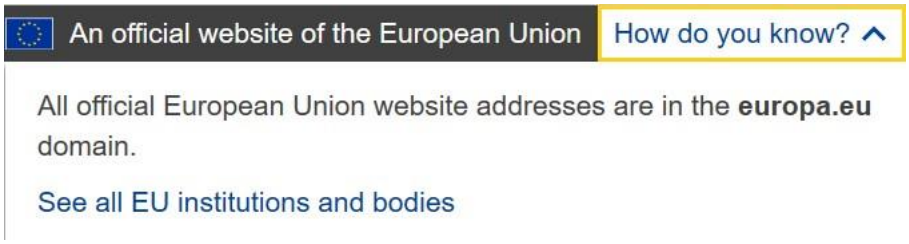
[2] Vrij vertaald van: https://www.economie.gouv.fr/files/files/directions_services/apie/marques/publications/Nom_de_domaine_affirmer_securiser_presence_internet.pdf
[3] https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/domain-names/government-domain-name-system-dns-service-overview/
[4] Vrij vertaald van: https://www.digitales.oesterreich.gv.at/domanenverwaltung-gv.at
[5] Vrij vertaald van https://cio.go.jp/sites/default/files/uploads/documents/domainguide-v2.0-20161201.pdf

verwachting, zal overheidsinformatie een hogere ‘ranking’ worden toebedeeld door een zoekmachine en daardoor beter vindbaar zijn.

Het vergroten van de herkenbaarheid van de overheid wordt ook vaak als motivatie achter het beleid genoemd. Een mooi voorbeeld troffen wij hiervan aan in Canada. Hierbij dient echter te worden opgemerkt dat het domeinnaambeleid slechts een van de maatregelen is die worden getroffen om de herkenbaarheid van de overheid als merk onder burgers te vergroten. Domeinnaambeleid wordt gezien als middel om een uniform overheidsmerk met daaraan gekoppelde huisstijl en gebruikerservaring neer te zetten. Herkenbaarheid bij de eindgebruiker wordt in het Canadese voorbeeld primair als maatstaf gebruikt.

Wat als te leren les naar voren is gekomen, is dat – indien een overheid kiest voor een centraal domeinnaambeleid – het helpt als een van de achterliggende doelen is om de centrale overheid als ‘merk’, met een aantal kenmerken (herkenbaar, betrouwbaar) neer te zetten. Een goed voorbeeld hiervan is onder meer de Oostenrijkse aanpak waar de implementatie van ‘gv.at’ is ondersteund met een stevige publiekscampagne in onder andere kranten en vormen van sociale media.

Een andere vorm van publiekscampagne vinden we terug bij de Europese Commissie waar de betrouwbaarheid van het beschermde domein ‘europa.eu’ met burgers wordt gecommuniceerd door middel van een speciale banner aan de bovenkant van iedere webpagina van de Europese Unie en de Europese Commissie (zie voorbeeld hieronder). Het belangrijkste doel van deze banner is volgens een respondent burgers bewuster maken van de betrouwbaarheid van de websites van de Europese Unie. De banner wordt uitgegeven door een centrale softwarebibliotheek waar alle webmasters van verscheidende EU-instanties uit kunnen putten. Op dit moment wordt de banner nog niet op alle websites toegepast, maar het doel is om de banner voor het eind van 2019 op alle websites te tonen.



Een soortgelijke banner zijn wij overigens tegengekomen in de VS, maar hier verschijnt de banner niet consistent op alle websites onder het TLD .gov.

2.3 Implementatiestrategie en aanpak

Voor het invoeren van een nieuw domeinnaambeleid wordt doorgaans de tijd genomen. Er is eigenlijk altijd sprake van een lange overgangsperiode waarmee de betreffende organisaties de tijd krijgen om het nieuwe beleid in te voeren op een voor hen gelegen moment, bijvoorbeeld als er een nieuwe website/platform wordt ontwikkeld.

Verschillende respondenten hebben aangegeven dat de implementatie van een domeinnaambeleid zorgvuldig handelen vereist en zeker geen sinecure is. Het vergt bovendien een lange adem. Waar Vlaanderen een vaste doorlooptijd van vier jaar heeft ingesteld, zijn er ook landen waarbij de implementatie meer gradueel verloopt. Ondanks dat Italië bijvoorbeeld al sinds 2009 een strikt,

verplicht domeinnaambeleid voert, dat naar eigen zeggen via een ‘big bang’ werd ingevoerd, is de adoptie laag te noemen. Het daadwerkelijk registreren onder een uniform overheidsdomein door overheidsorganisaties, zowel centraal als decentraal, blijkt lang niet altijd te gebeuren. Hierdoor kan het zelfs voorkomen dat niet alle departementen hun website hebben geregistreerd onder het *gov.it-domein. Onze respondent heeft aangegeven dat het bij de centrale overheid aan middelen ontbreekt om het domeinnaambeleid af te dwingen en te handhaven en dat het bovendien niet als prioriteit wordt aangemerkt.

Zoals eerder gesteld, draagt een eventuele verplichting niet bij aan de mate van succes van een domeinnaambeleid. In het onderzoek is naar voren gekomen dat een effectieve implementatie meestal niet wordt bereikt door een verplichting, maar dat overheden andere, meer subtiele manieren van governance, de ‘verleidingsstrategie’ aanwenden om organisaties te overtuigen om over te stappen op een uniforme domeinnaam. Interne publiekscommunicatie en de daaraan gekoppelde strategie spelen hierin een centrale rol.

Een voorbeeld hiervan kan worden gevonden in de VS. Binnen de VS is het top-level domain (.gov) al vanaf 1985 in gebruik. Voor de federale overheid geldt een verplichting, voor de statelijke en lokale overheden geldt vrijwillig gebruik. Mede hierdoor is door de jaren heen een wirwar aan domeinnamen ontstaan (verschillende top-level domains naast .gov zoals .com en .org) met als gevolg dat de herkenbaarheid, betrouwbaarheid en veiligheid van overheidswebsites kwestieus werd. Dit heeft de federale overheid ertoe gebracht om in 2018 een programma te starten om alle statelijke en lokale overheden alsnog of opnieuw op het .gov-domein te krijgen. Vanwege de statelijke en lokale autonomie is nu een programma gestart, met DHS (Department of Home Security) als initiator waarbij er eisen gesteld worden aan de wijze waarop statelijke en lokale overheden kunnen communiceren met de federale overheid. Het afdwingen van een *.gov domein moet vooral effect sorteren op veilig e-mailverkeer. Zo heeft de FBI al laten weten dat zij e-mails van lokale overheden die niet voldoen aan de extensie .gov niet in behandeling nemen. Als een lokale overheid met een andere extensie communiceert dan zal de communicatie worden genegeerd.

Om dit proces te helpen c.q. versnellen worden de verkiezingen van 2020 gebruikt als drukmiddel om alle staten, counties en steden hiertoe te bewegen. De federale overheid hoopt dat met het afdwingen van eisen die gesteld mogen worden aan verkiezingen, lokale overheden de stap naar *.gov gaan maken.

2.3.1 Communicatie

Als het gaat om de introductie van domeinnaambeleid dan zijn er twee belangrijke doelgroepen te onderscheiden. Enerzijds het publiek, anderzijds de overheidsorganisaties die aan de lat staan om opvolging te geven aan het beleid. Kijkend naar de onderzoeksresultaten dan valt op dat in veel gevallen de publiekscommunicatie wordt overgelaten aan de overheidsdienst die een website of platform lanceert. In het geval van een nieuwe vorm van digitale dienstverlening, dan staat veelal die betreffende verantwoordelijke uitvoeringsdienst daarvoor aan de lat. De communicatie gericht op de (interne) overheidsdiensten die worden aangesproken op toepassing van het beleid, bestaat doorgaans uit veel uitleg en overtuiging waarom toepassing van het domeinnaambeleid zinvol is en een toegevoegde waarde heeft.

Deze laatste vorm van communicatie is intensief wanneer er sprake is van verplicht gebruik. In die gevallen gaat de communicatie veelal gepaard met het beschikbaar stellen van aanvullende

benodigde voorzieningen die het domeinnaambeleid ondersteunen. Denk aan het aanbieden van infrastructurele oplossingen, het faciliteren van allerlei diensten en het begeleiden bij de transitie. Het aanbieden of ondersteunen van de overheidsdiensten met het ‘volledige pakket’ is in veel situaties het ‘smeermiddel’ om de implementatie van het nieuwe domeinnaambeleid te effectueren. In enkele gevallen is er sprake van een expliciete interne communicatiestrategie, zoals de VS. Hier wordt gebruik gemaakt van een soort affiche om, met name decentrale overheden, te verleiden over te stappen. Dit affiche is opgenomen in bijlage C.

Een goed voorbeeld van een effectief, centraal gestuurde publiekcommunicatie over een uniform domeinnaambeleid van de centrale overheid is te vinden in Oostenrijk. Daar is de introductie van het gv.at-domein ondersteund met gerichte publiekscampagnes, zoals korte statements op openbaar-vervoertickets, in dagbladen, op reclamespots, via websites, etc.

Nogmaals, in veel gevallen blijkt een domeinnaambeleid niet verplicht maar optioneel te zijn. In die gevallen blijft de aandacht voor communicatie relatief beperkt.

2.4 Effect van het beleid

Belangrijk onderdeel van dit onderzoek was de zoektocht naar de effecten van het beleid. Tijdens de deskresearch en tijdens de interviews hebben we geen officiële evaluaties kunnen achterhalen en ook geen indicaties gekregen dat er evaluaties zijn geweest. Daarbij zijn een aantal zaken op te merken:

- Zoals onder 2.2 is aangegeven, zijn de doelen en overwegingen die hebben geleid tot de invoering van het beleid vaak redelijk abstract geformuleerd. Ze is in ieder geval niet specifiek en meetbaar gemaakt waardoor het achteraf lastig vast te stellen is of, en zo ja welke, voortgang is bereikt.
- Daarnaast geven respondenten aan dat het ontwikkelen en uitvoeren van een effectmeting op dit beleid complex is. In het geval dat een domeinnaam onderdeel uitmaakt van een breder pakket aan maatregelen dan is het effect van de invoering van de domeinnaam naar verwachting van de respondenten slecht te isoleren. In de interviews wordt consequent aangegeven dat het om een breder pakket aan maatregelen gaat.
- Tot slot valt op dat in veel gevallen een effectmeting of beleidsevaluatie nooit voorzien is.

Desondanks hebben de meeste respondenten een positief beeld van het gebruik van de domeinnaam, al heeft in veel gevallen het beleid (nog) niet geleid tot het gebruik van een uniforme domeinnaam door alle (centrale) overheden.
Het is daarmee een legitieme vraag in hoeverre de doelen bereikt worden als niet alle partijen gebruik maken van de uniforme naam of als er onvoldoende kritische massa bereikt is in het gebruik. Ter illustratie: een van de beoogde doelen van het beleid is dat de burger aan de domeinnaam van een website kan zien of het een legitieme overheidswebsite betreft. Bij onvoldoende gebruik van het uniforme domein roept dat de vraag op of de burger wel doorheeft dat de domeinnaam bijdraagt aan herkenbaarheid en betrouwbaarheid.

Binnen het VK heeft men het ‘oppoetsen’ van het domeinnaambeleid voor de centrale overheid aangegrepen om juist naar het grote publiek duidelijk te maken dat de regering de stap naar de ‘digitale wereld’ als een belangrijke en onontkoombare stap ziet. Door gebruik te maken van een centraal platform waarlangs alle digitale diensten en informatie van de centrale overheid beschikbaar zijn, is het merk GOV.UK als uithangbord van die ambitie van grote waarde.

Als onvoorzien, maar positief effect van het invoeren van het GOV.UK-platform wordt door de Britse vertegenwoordiger aangegeven dat een kostenbesparing van 63 miljoen pond per jaar is verwezenlijkt. Dit bedrag is voornamelijk opgebouwd uit het onderhoud van honderden separate overheidswebsites. Wel dient vermeld te worden dat, ondanks dat de adoptie onder centrale overheden relatief hoog op het platform is, er nog steeds tientallen uitvoerders en agentschappen niet onder gevonden kunnen worden en hun eigen website in stand houden.

Ten slotte kunnen vraagtekens worden gesteld bij de effectiviteit van een domeinnaambeleid als de benodigde implementatietijd lang is. Gedurende die gehele periode geldt dat het (al dan niet) beoogde effect slechts ten dele wordt gehaald. Een dergelijke hybride situatie, waarin het gebruik van een uniforme domeinextensie niet stelselmatig is, zou zelfs het aanvankelijke doel als herkenbaarheid en betrouwbaarheid van de overheid onderuit kunnen halen, aldus onze Canadese respondent.

3. Grafische weergaven

De bevindingen uit hoofdstuk 2 worden gestaafd door de uitkomsten van de twee surveys, de diepte-interviews en de deskresearch. Waar hoofdstuk 2 een meer kwalitatieve duiding bood van deze uitkomsten, worden de uitkomsten in dit hoofdstuk op een meer kwantitatieve manier gepresenteerd, in grafieken. De dualiteiten als beschreven in hoofdstuk 2 komen ook terug in de gepresenteerde figuren hieronder. De gegevens voor de grafieken zijn geenszins uitputtend en bieden daarom ook geen volledig of representatief beeld, maar dienen als indicatie van de buitenlandse praktijk.

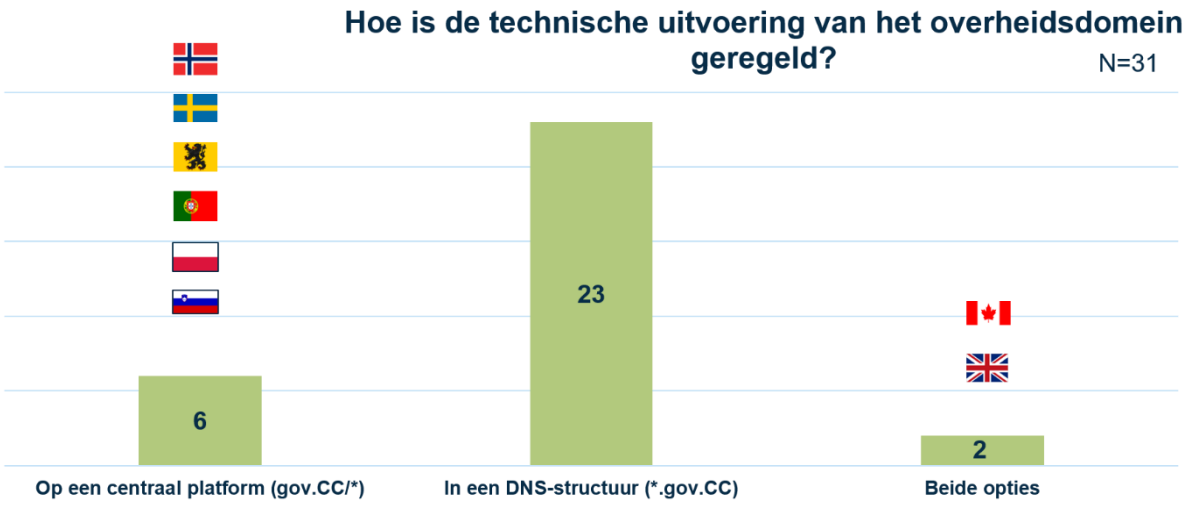
Figuur 1[6]

Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 30 observaties kunnen gebruiken voor het beantwoorden van de vraag of er een expliciet domeinnaambeleid bestaat voor de overheid. In 16 van de 30 geraadpleegde landen is dit het geval. Bij 14 landen is er geen expliciet domeinnaambeleid voor de overheid aangetroffen. Dit laat onverlet dat voor alle respondenten geldt dat er wel een algemeen domeinnaambeleid is, bijvoorbeeld om de rol van een landelijke 'registry' te formaliseren.

Daarnaast dient opgemerkt te worden dat het domeinnaambeleid voor de overheid – bij de 16 respondenten – per land kan verschillen qua inhoud en strekking. Zo geldt in het ene land een naamgevingsbeleid, het andere een registratieplicht, in weer een andere het gebruik van een centraal technisch platform, en zelfs in sommige situaties combinaties ervan.

[6] Deze vraag is toegespitst op het al dan niet expliciete karakter van het aangetroffen domeinnaambeleid, omdat wij, in met name de deskresearch, verschillende landen zijn tegengekomen die ondanks het gebruik van een overheidsdomein hierover weinig tot niks hebben opgenomen in beleid

Figuur 2[7]



Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 31 observaties kunnen gebruiken voor het beantwoorden van de vraag hoe de technische uitvoering van het overheidsdomein is geregeld.

In 23 van de 31 observaties wordt gebruik gemaakt van een DNS-structuur. In 6 gevallen is er sprake van een technisch centraal platform. Dit geldt voor Noorwegen, Zweden, Vlaanderen, Portugal, Polen en Slovenië. In 2 van de geraadpleegde landen, te weten het Verenigd Koninkrijk en Canada, geldt dat zowel gebruik wordt gemaakt van een DNS-structuur alsook een technisch platform.

Een observatie is dat de keuze voor een technisch centraal platform soms volgend is op het hebben van een DNS-structuur. Andersom is niet aangetroffen.

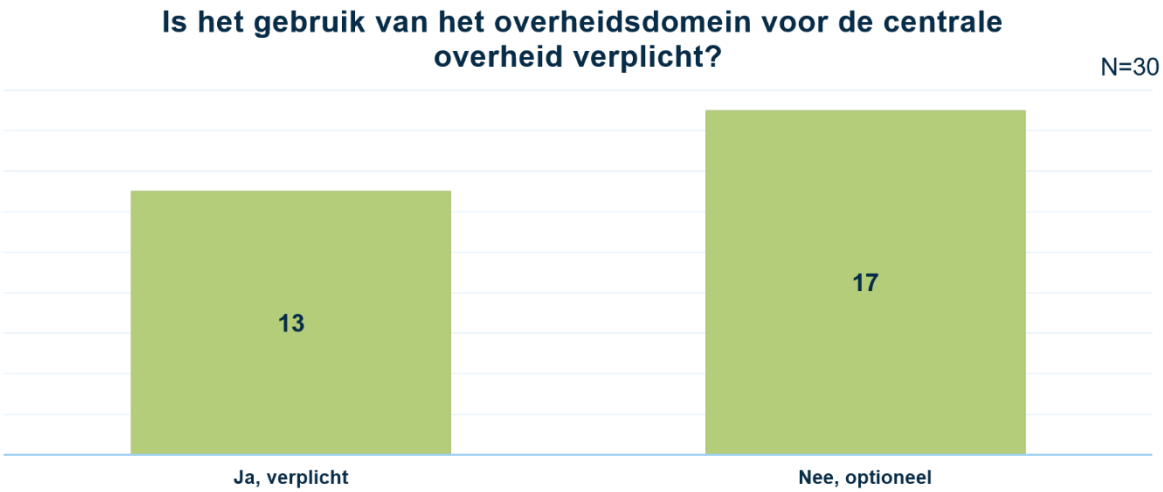
[7] Sommige grafieken zijn voorzien van inhoudelijke duiding door het toevoegen van landenvlaggetjes. Dit is alleen gedaan wanneer het, naar ons inziens, relevant bleek voor de context van dit onderzoek. Indien gewenst kunnen wij van alle grafieken aangeven welke landen in welke categorieën vallen

Figuur 3

Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 14 observaties kunnen gebruiken voor het beantwoorden van de vraag welke motieven ten grondslag liggen aan het hebben van een domeinnaambeleid voor de overheid.

Wat uit de response opvalt is dat vijf dominante redenen worden genoemd, te weten: beheersbaarheid, veiligheid, betrouwbaarheid, vindbaarheid en herkenbaarheid. Van deze redenen kwam herkenbaarheid het vaakst terug: 11 keer. Respondenten noemden beheersbaarheid en betrouwbaarheid 9 keer als motivatie achter het domeinnaambeleid. In mindere mate werden de redenen veiligheid (7 keer) en vindbaarheid (3 keer) genoemd. Voor deze vraag konden respondenten meerdere antwoorden geven.

Figuur 4



Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 30 observaties kunnen gebruiken voor het beantwoorden van de vraag of het gebruik van overheidsdomein (ofwel als DNS-structuur, ofwel als platform-oplossing) voor de centrale (federale) overheid verplicht is.

In 13 van de 30 gevallen is het gebruik van een centraal platform voor de centrale overheid verplicht. In 17 van de 30 gevallen niet. In geen enkel geval is het gebruik van een centraal overheidsplatform verplichtend voor decentrale (niet-federale) overheden.

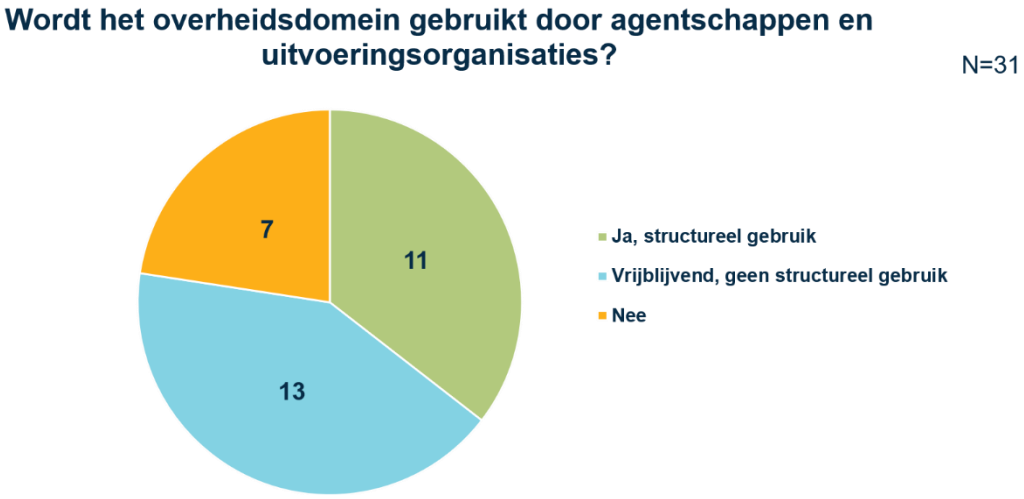
Wanneer de gegeven antwoorden op deze vraag vergeleken worden met het expliciet hebben van een overheidsdomeinnaambeleid (vraag 1), kan worden gesteld dat er in sommige landen wel een overheidsdomein beschikbaar is, maar dat er geen expliciet domeinnaambeleid geldt. Het niet hebben van een domeinnaambeleid sluit derhalve niet uit dat er geen overheidsdomein is voor digitale communicatie en dienstverlening.

Figuur 5

Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 31 observaties kunnen gebruiken voor het beantwoorden van de vraag in hoeverre het bestaande overheidsdomein ook daadwerkelijk wordt gebruikt door de departementen. De antwoordopties variëren tussen een structureel gebruik, een vrijblijvend gebruik, of geen gebruik.

Wat opvalt is dat als er sprake is van een centraal overheidsdomein dan maken de ministeries/kerndepartementen daar veelal gebruik. In 23 van de 31 gevallen wordt er door ministeries structureel gebruik van gemaakt, in 6 van de 31 gevallen niet structureel maar wel met een zekere frequentie. Slechts in 2 van de 31 gevallen wordt er dan geen gebruik gemaakt van het centrale overheidsdomein door ministeries.

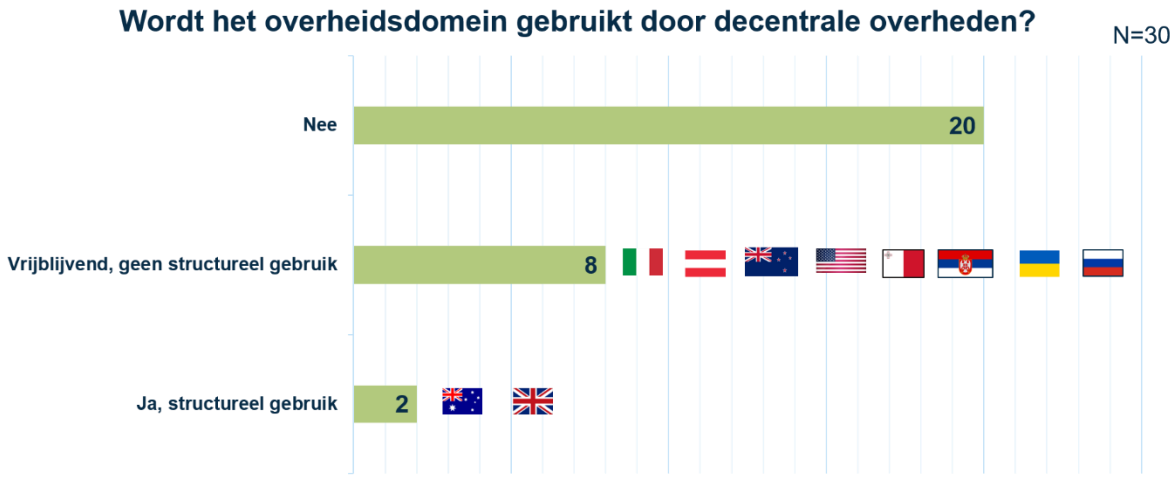
Figuur 6



Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 31 observaties kunnen gebruiken voor het beantwoorden van de vraag in hoeverre een het bestaande overheidsdomein ook daadwerkelijk wordt gebruikt door agentschappen en uitvoeringsorganisaties.

Door de 31 respondenten is aangegeven dat in 11 gevallen agentschappen en uitvoeringsorganisaties structureel gebruik maken van een centraal overheidsdomein, in 13 gevallen is het gebruik vrijblijvend is en in 7 gevallen wordt er geen gebruik van gemaakt door agentschappen en uitvoeringsorganisaties. Soms anticipeert het aanwezige domeinnaambeleid al op de noodzaak voor een agentschap/uitvoeringsorganisatie om gebruik te maken van een eigen platform door uitzonderingen toe te staan. Soms leidt de bekendheid van een merknaam zoals ‘Belastingdienst’ of de complexiteit om diensten van uitvoeringsorganisatie te koppelen aan een overheidsdomein tot de keuze om dat niet te willen/doen.

Figuur 7



Toelichting:
Op basis van het uitgevoerde onderzoek hebben wij 30 observaties kunnen gebruiken voor het beantwoorden van de vraag in hoeverre het bestaande overheidsdomein ook daadwerkelijk wordt gebruikt door decentrale overheden.

In 20 van de 30 gevallen is er geen sprake van doorwerking. In 10 van de 30 wel. Daarbij geldt vervolgens dat in 8 gevallen sprake is van vrijblijvende doorwerking cq. adoptie. Dit geldt voor de volgende landen: Italië, Oostenrijk, Nieuw Zeeland, VS, Malta, Servië, Oekraïne en Rusland.
In twee gevallen is er echt sprake van een doorwerking met structureel gebruik. Dit geldt voor het Verenigd Koninkrijk en Australië.

4. Samenvatting en kritische succesfactoren

4.1 Samenvatting

4.1.1 Domeinnaambeleid

Geen hard bewijs voor effectiviteit
Een wezenlijke onderzoeksvraag van het buitenlandonderzoek is of, en zo ja, in welke mate het invoeren van domeinnaambeleid bijdraagt aan de vijf achterliggende hoofdredenen die doorgaans in beleidsnotities worden aangemerkt als motivatie om een dergelijk beleid te willen hebben. Het gaat daarbij om de volgende beweegredenen: herkenbaarheid, vindbaarheid, betrouwbaarheid, veiligheid en beheerbaarheid. Uit het gevoerde onderzoek is noch in kwantitatieve zin, noch in kwalitatieve zin vast te stellen of het hebben van een overheidsbreed domeinnaambeleid een bijdrage levert aan deze punten. Daarvoor zijn er simpelweg geen evaluaties beschikbaar. Bij geen van de geraadpleegde buitenlandse overheden zijn hierover rapportages voorhanden.

Dit laat onverlet dat geraadpleegde respondenten een positieve mening en/of een verwachting hebben over het effect van domeinnaambeleid. Zo hebben respondenten van overheden waar actief het domeinnaambeleid wordt ondersteund met het aanbieden van generieke voorzieningen en diensten, het beeld dat het beleid echt bijdraagt aan alle vijf de genoemde redenen. Bovendien geven de respondenten van overheden die gebruik maken van een platform-oplossing terug dat een platform echt bespaart. Maar nogmaals, deze beelden zijn niet met harde feiten te onderbouwen.

Geen uniform beleid, maar wel 'rode draden'
Ondanks het feit dat er geen harde bewijzen zijn waarom een domeinnaambeleid effect sorteert op de genoemde aspecten, voert een behoorlijk aantal buitenlandse overheden toch een domeinnaambeleid.

Binnen landen treffen wij verschillende modaliteiten van domeinnaambeleid aan. Beleid dat als 'raadgeving' wordt gepropageerd, beleid dat verplicht is voor departementen maar waar geen sprake is van handhaving, beleid dat naast de departementen ook voorgeschreven is aan uitvoerende diensten, agentschappen en ZBO's, beleid dat vanuit een centrale organisatie wordt begeleid/ondersteund of juist ook weer niet, etc. Kortom, de wijze waarop centrale overheden invulling geven aan domeinnaambeleid is divers met een sterk wisselend gebruik tot gevolg.
Toch zijn een paar 'rode draden' te identificeren:

- Het beleid sluit aan op de grenzen en de inrichting van het bestuur van een land. Zo wordt overal rekening gehouden met de autonomie van verschillende bestuurslagen. Met uitzondering van Italië[8], treffen wij nergens een domeinnaambeleid aan dat is geïnitieerd en vastgesteld door de centrale overheid met een verplichte doorwerking naar de decentrale overheden. Als er al sprake is van een overheidsbreed beleid dan geldt dat beleid als optioneel, een raadgeving.
- Grofweg is er sprake van twee typologieën: het **DNS-concept** en de **platform-oplossing**.
  - Het DNS-concept houdt in dat er sprake is van 'naamgevingsbeleid', wel of niet gebruik maken van *.gov.cc bij domeinnamen voor de overheid. De platform-oplossing houdt in dat er

[8] Ondanks het verplichte karakter van het domeinnaambeleid in Italië voor 'alle publieke entiteiten' (zowel centraal als decentraal) kan de daadwerkelijke adoptie worden aangemerkt als vrijblijvend en laag

– al dan niet aanvullend op het DNS-concept – gebruik wordt gemaakt van een centrale website (gov.cc/*) voor overheidscommunicatie.
Van deze twee vormen komt het DNS-concept het meeste voor. Doorvoering c.q. toepassing van het beleid wordt het meest aangetroffen bij departementen en in mindere, vrijblijvendere mate bij uitvoeringsdiensten en agentschappen. In enkele gevallen is het beleid ook toegepast door decentrale overheden.

- Daarnaast kiest een aantal landen expliciet voor een platform-oplossing. Drie recente aansprekende voorbeelden hiervan zijn Vlaanderen.be, Canada.ca en GOV.UK. Wat bij het toepassen van de platform-oplossing opvalt is dat departementen (doorgaans verplicht) gebruik maken van zo een platform. Het betreft dan voornamelijk de ontsluiting van informatie richting burgers en bedrijven. Verder bestaat veelal de wens om ook uitvoeringsorganisaties erop aan te sluiten. Maar de eisen aan continuïteit van diensten en de technische complexiteit die schuilgaat achter een operationele elektronische dienst, inclusief digitale authenticatie en autorisatie en koppelingen met achterliggende systemen, maken dat tot op heden transities van uitvoeringsdiensten naar een centraal platform eerder uitzondering dan regel zijn.
- Een argument waarom een buitenlandse overheid ervoor kiest om een centraal platform neer te zetten voor haar overheidscommunicatie, naast of in plaats van een domeinnaambeleid, is dat juist een uniform overheidsplatform (zoals Vlaanderen.be of GOV.UK) zal bijdragen aan vindbaarheid en herkenbaarheid van overheidsinformatie. Zeker als gebruikers, nog meer dan nu al het geval is, hun informatie op het internet zoeken via zoekmachines.

- Ten slotte komt uit het gehouden buitenlandonderzoek naar voren dat een uniform domeinnaambeleid nauwelijks wordt vertaald naar een naamgevingsbeleid voor e-mail. Noch in de ontvangen vragenlijsten, noch in de gehouden interviews komt naar voren dat er een actief beleid is op dit vlak. Dit wil overigens niet zeggen dat er geen e-mailbeleid (inclusief regels omtrent etiquette, archivering, etc.) is, maar het is zelden expliciet onderdeel van het domeinnaambeleid. Dit wil ook niet zeggen dat er geen e-mailadressen met overheidsextensie bij buitenlandse overheden in gebruik zijn. Een inventarisatie leert dat dergelijke e-mailadressen wel degelijk worden gebruikt: in veel gevallen ten behoeve van een generieke overheidsorganisatie (info@organisatie.gov.uk), en in mindere mate door specifieke personen, maar bovenal niet consequent en overheidsbreed.

4.1.2 Positie Nederland

Als we de resultaten vanuit het buitenlandonderzoek vergelijken met de situatie aangaande domeinnaambeleid binnen de Nederlandse overheid, dan zien wij een aantal zaken.

Binnen de Rijksoverheid is een domeinnaambeleid van kracht. Dat beleid is primair gericht op het centraal registreren van domeinnamen die door de Rijksoverheid in gebruik zijn. Hiertoe is de Dienst Publiek en Communicatie (DPC) deelnemer van de SIDN (registrar), en houder (registrant) van alle domeinnamen van de Rijksoverheid. De DPC publiceert maandelijks een overzicht van alle publieke websites van de Rijksoverheid op www.websiteregisterrijksoverheid.nl.

Daarnaast verzorgt DPC ook het Platform Rijksoverheid Online (PRO) waarmee het voor organisaties binnen de Rijksoverheid mogelijk wordt gemaakt om een eigen platform te lanceren. Ondanks dat de content van ieder (uniek) platform niet door het DPC wordt aangeleverd, is het ontwerp of design van ieder platform hetzelfde. De techniek, doorontwikkeling, beheer en beveiliging van de platformen wordt wel door de DPC op zich genomen. De dienst die DPC hiermee levert is tot op zekere hoogte

vergelijkbaar met een ontwikkeling die in het VK is aangetroffen waar overheidsorganisaties op het centrale niveau worden ontzorgd in het onderhouden van hun domein. Bovendien is het toepassen van een consistent ontwerp van hoe de verschillende platforms eruitzien vergelijkbaar met de ambitie van Canada om de overheid neer te zetten als één herkenbaar merk.

Een platform onder het PRO is Rijksoverheid.nl, het gedeelde platform van de departementen. In vergelijkend perspectief kan worden gesteld dat Rijksoverheid.nl op dit moment een voorbeeld van een platform-oplossing binnen domeinnaambeleid is. Zoals in hoofdstuk 2 is opgemerkt, varieert de functionele scope van de platform-oplossing aanzienlijk. Waar sommige platformen louter informatie aan een websitebezoeker verstrekken, gaan sommige overheden verder door ook functionele toepassingen als digitale services en diensten op het platform te integreren. Rijksoverheid.nl is een platform-oplossing die in dat opzicht binnen de eerste groep valt van puur informatie verstrekken. Bovendien is er ten behoeve van het gebruik van Rijksoverheid.nl aanvullend een domeinnaamconventie voor URL's op de website van kracht.

De organisatorische scope van Rijksoverheid.nl blijft beperkt tot de 12 ministeries. Van andere overheden staat er geen informatie op dit platform. Uitvoeringsorganisaties die onder de ministeries vallen onderhouden hun eigen websites, maar hebben wel de mogelijkheid om via het PRO een eigen platform, conform hetzelfde ontwerp als Rijksoverheid.nl, te onderhouden. Een voorbeeld hiervan is de Rijksdienst voor Identiteitsgegevens. De meerderheid van de uitvoeringsorganisaties (en ook ZBO's) onderhoudt echter een website die niet is verbonden aan het PRO.

4.2 Kritische succesfactoren

Naast een aantal beschrijvende observaties over het toepassen en gebruik van domeinnaambeleid door buitenlandse overheden, heeft het onderzoek ook een aantal lessen opgeleverd. Die lessen worden in het hiernavolgende gepresenteerd in de vorm van kritische succesfactoren.

Voorafgaand wordt gesteld dat de effectiviteit/bruikbaarheid van de onderstaande kritische succesfactoren – ook al is het misschien een open deur – afhankelijk zijn van de ambities die de werkgroep 'Herkenbare en Betrouwbare Digitale Overheid' nastreeft en hoe zij de definitie van succes daarbij definieert.

1. Politiek-bestuurlijk draagvlak is voorwaardelijk om de ambities van een verdergaand domeinnaambeleid waar te kunnen maken. Zonder dat draagvlak zal het zeer lastig worden om ofwel te komen tot een gezamenlijk beleid, inclusief implementatie en naleving, dat over de verschillende bestuurslagen heengaat, ofwel te komen tot een verdere uitbouw van het thans aanwezige website Rijksoverheid.nl als onderdeel van het PRO.

2. Ook al krijgt het beoogde domeinnaambeleid (wat de inhoud er ook van is) een verplichtend karakter, dan nog is het noodzakelijk om een pakket aan flankerende maatregelen te treffen dat het beleid ondersteunt en stimuleert tot enthousiast gebruik. Tegen deze achtergrond spreken wij graag van een verleidingsstrategie. In het kader van een verleidingsstrategie zijn de volgende aspecten tijdens het onderzoek naar voren gekomen:
   - beschikbaarheid van budget om (verplicht) deelnemende overheidsorganisaties te ondersteunen bij het werk dat voortvloeit uit de ambitie;
   - beschikbaarheid van doorlooptijd om te groeien naar de beoogde situatie;

- ontzorgen van (verplicht) deelnemende organisaties bij de implementatie;
- beschikbaar stellen van ‘tooling’ zoals kaders, richtlijnen, UX-labs (user experience ontwikkelomgevingen), promotiemiddelen, etc.;
- nadenken over en implementeren van een externe overheidsbrede communicatie.

3. Denk bij de implementatie van domeinnaambeleid goed na over de timing. Sluit aan bij reeds lopende ontwikkelingen en maak gebruik van zogenaamde ‘windows of opportunity’.

4. Het instellen van een naamgevingscommissie om te bepalen welke organisaties zich onder welke naam kunnen registreren op een eventueel uniform overheidsdomein in de vorm van een platform of als second-level domein. Een procedure als ‘first come, first served’ wordt in het geval van het toebedelen van overheidsnamen als onbevredigend beschouwd. De buitenlandse praktijk leert dat dit kan worden ondervangen door het instellen van een verantwoordelijk naamgevingscommissie.

Bijlage A Gegevensbronnen

A. 1 Respons uit SIDN-survey

#	Land	#	Land
1	Slovenië	14	Verenigd Koninkrijk
2	IJsland	15	Luxemburg
3	Polen	16	Frankrijk
4	Oekraïne	17	Oostenrijk
5	Slowakije	18	Georgië
6	Ierland	19	Japan
7	Noorwegen	20	Canada
8	Denemarken	21	België
9	Rusland	22	Kroatië
10	Italië	23	Portugal
11	Zweden	24	Servië
12	Tsjechië	25	Duitsland
13	Spanje		

A. 2 Respons uit BZK-survey

#	Land	#	Land
1	Oostenrijk	7	Letland
2	Luxemburg	8	Nieuw-Zeeland
3	Duitsland	9	Polen
4	Singapore	10	Portugal
5	Ierland	11	Verenigd Koninkrijk
6	Italië		

A. 3 Lijst van contactpersonen

#	Datum van interview	Naam	Organisatie
1	25 sept	Godfried Knipscheer	Vlaanderen
2	3 okt	Alessandro Ranellucci	Italië
3	7 okt	Gerhard Schwarz	Oostenrijk
3	11 okt	James Stewart	Verenigd Koninkrijk
5	17 okt	Marina Fox	Verenigde Staten
6	-[9]	Joël Bannister	Nieuw-Zeeland
7	-	Tiago Mendonça	Portugal
9	4 nov	Carlos Torrecilla-Salinas	Europese Commissie
9	5 nov	Laura Piper en Michèle-Renée Charbonneau	Canada
10	-	Michiel Henneke	SIDN
11	-	Patrick Myles	CENTR

[9] Met Nieuw-Zeeland en Portugal is geen telefonisch contact geweest, maar is de voltallige vragenlijst uitvoerig beantwoord in een e-mailwisseling

Bijlage B Vragenlijst

Onderstaande vragenlijst is opgesteld samen met de werkgroep en heeft als basis gediend voor zowel de survey via SIDN alsook de uitgezette survey via het Ministerie van BZK naar Europese overheden. Daarnaast heeft deze vragenlijst als leidraad gediend voor de aanvullend afgenomen diepte-interviews.

A. Current policy on ' Uniform Domain name extensions '

General

1. What is the policy on unified domain name extensions for your government?
2. Is the policy mandatory or optional? And are there any exceptions in case of ' compulsory ' compliance?
3. Is the policy laid down in laws and/or regulations? And if so, in what way?
4. For which government/governments does the established policy apply? (i.e. central government, local government, agencies, etc)
5. How is the monitoring of compliance with the policy organized?
6. Who makes the policy and who establishes it?
7. Has the policy changed over the years, and if so why?

Specific

8. Which uniform domain name extension (SLD, gTLD) – the exact naming- has been chosen, and if so why? Did the availability of a particular ' name ' also be played?
9. How specifically is the domain name policy elaborated? (i.e. Which sites are covered, which are not? For websites as well as e-mail? What does the application process look like, and what is the turnaround time? Do ' old ' domain names remain in use, are they quarantined, and are these domain names ever released again? Are there specific situations (think of Commonwealth, colonies, special state law positions of institutes) that have to be taken into account?)
10. What are the requirements for using unified domain name extensions?
11. To what extent is the public suffix list and HSTS preload used?
12. To what extent has attention been paid to the concrete elaboration of the domain name policy:
    a) recognizability
    b) findability
    c) reliability
    d) security
    e) manageability
13. How often, and in what way, are there derogations from the policy?

B. The rationale, the idea behind or the reason for the current policy

1. What are the main reasons for choosing the policy as described under ‘A’ and what were the intended goals and/or expected (ex ante) effects?
2. Have there been specific causes which resulted in formulating a uniform domain name extension policy? If so, what were these causes?
3. To what extent have the following aspects played a role in the consideration?

- recognizability
- findability
- reliability
- security
- manageability

4. Has a business case/cost-benefit analysis been part of the considerations and, if so, what influence did it have?
5. Have alternative scenarios been investigated for the application of a naming policy? And if so, which ones?
6. To what extent has the pre-estimated duration for the introduction of the policy – the transition phase – played a role in the policy choice made?
7. Have alternative deployment scenarios been investigated? And if so, which ones?
8. What were the considerations to oblige or not to require domain name policy?

C. The consequences/impact of the introduction of the policy

Governance

1. Who is the policy owner?
2. Who is responsible for the implementation of the policy (domain management)?
3. Who is responsible for monitoring & enforcement?
4. How is the policy of a unified domain name extension elaborated in:
    a) Issuance process (central/decentralised)
    b) Requirements/Frameworks
    c) Automated Checks
    d) Methods for impact measurements

5. How is it ensured that all parties for whom the policy applies participate? (‘Carrot’ or ‘stick’)
6. How is the policy for a unified domain name extension rolled out?
(Big bang, phased, gradually via new sites, etc.)

Finance

1. What were the introduction costs?
2. Were there financial incentives (needed) to implement the policy?
3. What are the multi-annual operational costs for managing domain names?
4. To what extent have the cost of managing domain names changed? (shift from decentralized to central or vice versa, an increase/decrease when all costs are taken together)

Communication

1. Which public communication has been deployed?
2. What internal public communication has been deployed?
3. What contacts have been established with ' communities ' in the country?

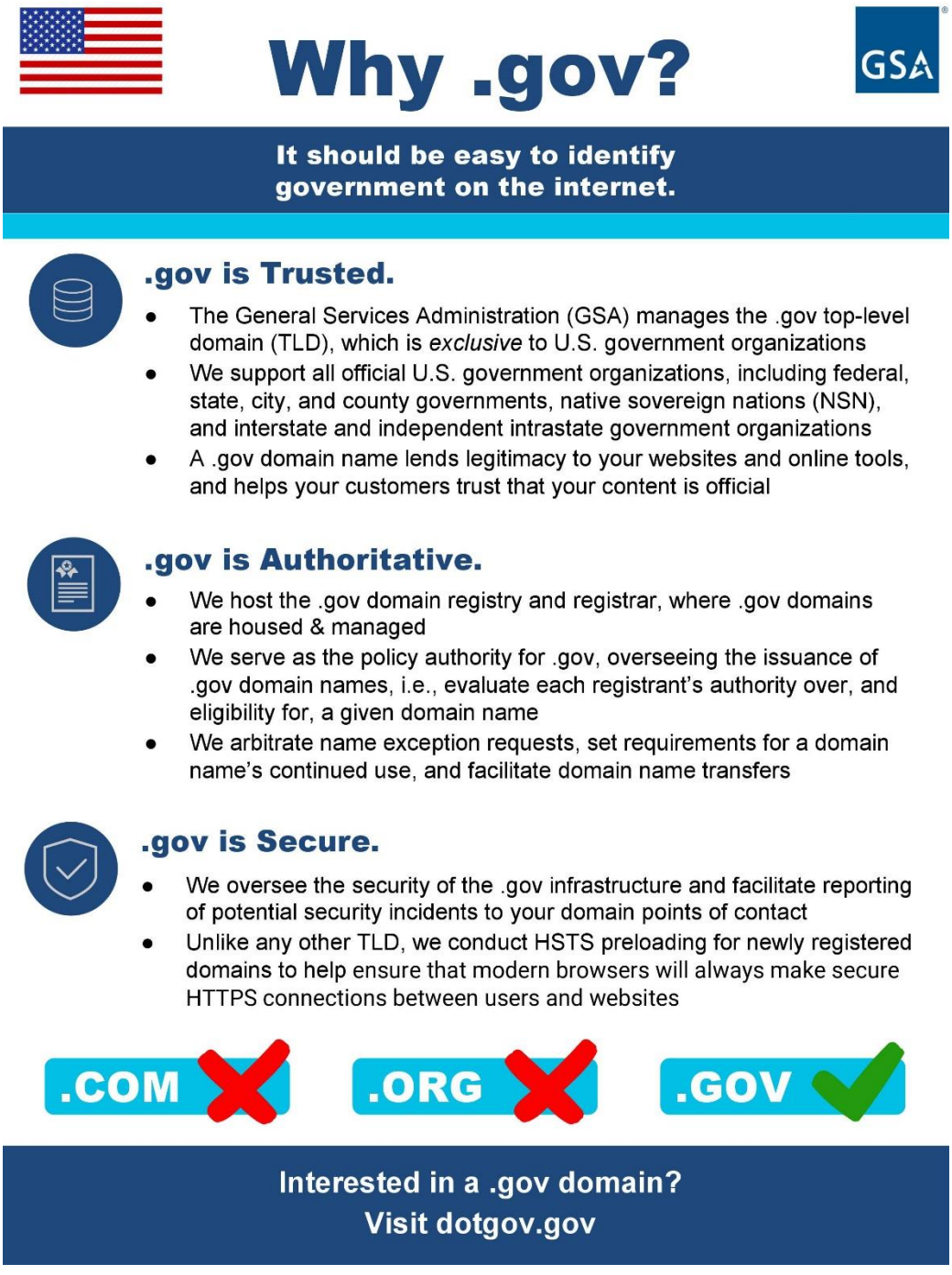
Technique

1. How is the 'registry function' of the domain technically implemented?
2. How is the (eventual) transition for e-mail domains technically addressed?
3. How is the (eventual) transition for websites technically addressed?
4. Does a unified domain name extension offer technical advantages compared to no unified domain name extension?

D. Effects of the policy

1. In relation to the questions under B: What where the effects? Have the (ex ante) expectations come out? Have the effects been achieved? Is it possible to make a subdivision in answering these questions to:
    a) recognizability
    b) findability
    c) reliability
    d) security
    e) manageability
2. To what extent have users and customers become accustomed to the domain name policy?
3. To what extent is there a citizen's acceptance?
4. What were the unexpected effects?
5. What are the lessons learned?
6. To what extent does the knowledge of today invite – if there is still no domain Name policy – to re-enter domain name policy?

Bijlage C Affiche VS



Bijlage D Informatie nader verkende landen

Van de diepte-interviews zijn korte gespreksverslagen opgesteld, die ook zijn teruggelegd bij de respondenten ter verificatie. Omdat de meeste interviews in het Engels zijn afgenomen, zijn de meeste gespreksverslagen ook in het Engels opgenomen. Van de landen waar een telefonisch interview niet mogelijk was, maar wel uitgebreid e-mailcontact mee is geweest, zijn de relevante antwoorden toegevoegd.

D. 1 Vlaanderen

- Het domein ‘vlaanderen.be/naam’ is een bestaand domein voor centrale overheidsorganisaties, maar werd eigenlijk matig gebruikt. Verschillende overheidsorganisaties gebruikten hun eigen domeinnaam dus het oude beleid was een beetje verwaterd.
- In de nota van 21 december 2018 is het nieuwe beleid omtrent het domeinnaam ‘vlaanderen.be/naam’ uitgewerkt. Een belangrijke reden voor de Vlaamse regering om dit domein nieuw leven in te blazen was de vindbaarheid van de Vlaamse overheid. Met name werd er geconstateerd dat er tegenwoordig steeds minder direct wordt gezocht naar url’s. In de plaats daarvan bereiken steeds meer burgers overheidswebsites via zoekmachines als Google en Bing (en in de toekomst ook met spraakgerichte zoekopdrachten). Met oog op het feit dat de Vlaamse overheid door de ‘wildgroei’ in verschillende domeinnamen niet meer noodzakelijkerwijs als eerste zoekresultaat verschijnt op Google, is het uniforme url-beleid ingesteld. Naast vindbaarheid zijn herkenbaarheid (hét merk de overheid) en betrouwbaarheid ook belangrijke aspecten geweest om de url-strategie in te voeren.
- Het gebruik van vlaanderen.be wordt verplicht voor de in de nota genoemde organisaties, maar men is zich er zeer van bewust dat deze verplichting niet kan worden afgedwongen. Er worden daarom stimulerende maatregelen getroffen om organisaties te verleiden zich te registreren onder één domein of portaal. Een voorbeeld daarvan is het recentelijk herinrichten van het centrale portaal tot één (huis)stijl waarvan gebruik gemaakt kan worden.
- De stuurgroep Vlaamse Informatie en ICT Beleid is verantwoordelijk voor de toewijzing van de url’s (de namen achter de slash). De ambitie hierbij is om dat binnen twee dagen te doen, waarbij geldt dat dit in het eerste jaar als ‘best effort’ wordt beschouwd. Als organisaties zich niet wensen te registreren dan moeten zij via de stuurgroep een uitzondering afdwingen. De stuurgroep monitort ook de voortgang van de uitrol.
- Er is bewust voor gekozen de uniforme url-strategie niet te verplichten voor decentrale overheden. Zij staan – zo is de inschatting - te veel op hun eigen autonomie. Bovendien zou de gehele operatie qua omvang te groot en daarmee onbeheersbaar worden.
- Loketten en complexe applicaties zijn uitgezonderd van het registreren op vlaanderen.be/naam. Dit komt met name door de technische complexiteit die erbij komt kijken (bijvoorbeeld authenticatie via eID).
- Het aansluiten van alle agentschappen (met of zonder rechtspersoon) op het uniforme domein wordt nog lastig, want sommige van deze agentschappen doen aan een sterke eigen profilering. Vanuit het politieke niveau is echter gestuurd op hun insluiting binnen het vlaanderen.be domein.
- De url-strategie heeft niet zijn weerslag op de e-mail-accounts van de overheid, want deze operatie zou te duur uitpakken. Er zijn bovendien veel koppeling van accounts met andere applicaties.

- De invoeringskosten bestaan uit technische kosten (tussen de 150 en 170.000 euro per jaar, afhankelijk van het aantal nieuwe aansluitingen en het verkeer dat daaroverheen gaat) en begeleidingskosten (manuren). De begeleidingskosten zijn op dit moment minder dan 1 fte en kunnen afhankelijk van nieuwe aansluitingen oplopen naar 2 of 2,5.
- Er is geen expliciete communicatiestrategie rondom het invoeren van vlaanderen.be. Het wordt allereerst intern gecommuniceerd via de stuurgroep waarin verschillende mensen vanuit de administratie zijn vertegenwoordigd, en via intern gerichte websites. De noodzaak voor externe communicatie wordt niet gevoeld, omdat de meeste mensen overheidswebsites bereiken via zoekmachines.
- Het herinvoeren van Vlaanderen.be is gestoeld op gebruikersonderzoeken, maar er is nooit gekeken naar de effecten van een uniform beleid. Er wordt onderkend dat dit trouwens lastig te meten zal zijn. Voor de toekomst wordt er nagedacht over het meten van effecten van een uniform domein. De middelen ontbreken echter op dit moment om concrete plannen hiertoe te ontwikkelen.
- Over welke dingen moet Nederland absoluut nadenken bij een eventuele implementatie van een uniforme domeinnaam strategie?
  - Technologische inrichting van één generiek domein. Daar komt meer bij kijken dan vooraf wordt gedacht.
  - De kans bestaat op conflicterende url's; welke namen kunnen door welke organisaties worden geclaimd?
  - Hoe richt je dingen in als een cookie-consent?

D. 2 Italië

- The Italian government domain (gov.it) was established in 2009. At that time, the decision was being made that the .gov domain had to be exclusively reserved for public entities. The *Agenzia per l'Italia Digitale* (AGID) serves as registry.
- The migration to the uniform government domain was organized by a 'big bang': from 2009 onwards, all public entities were expected to register their domain names under gov.it.
- The Italian government has deliberately chosen for *name*.gov.it instead of gov.it/*name* (=website in the form of a single platform). The main reason for this is the high independence enjoyed by regional and local governments like municipalities. They hold on to their own autonomy and are therefore not willing to register under a single government platform. Moreover, registration under a single government platform brings difficulties in the allocation of names and the expectation is that there will arise technical problems with the different e-mail addresses.
- The registration at the gov.it-domain is mandatory to all public entities. All public entities include the central and local administration and also agencies and executive organizations. However, there are no formal sticks or sanctions to enforce this policy. Instead, the Italian government tries to tempt public bodies to register on the domain by reducing the costs and offering a clear and understandable framework for website design. This is in accordance with the UX Guidelines.
- An exemption has been made for educational institutions like schools and universities. They can register on the reserved .edu.it-domain. Right now, educational institutions are in the middle of the transition to this specific domain.

- In some cases, public entities register websites under .italia.it. This second-level domain is used for special government projects (for instance io.italia.it), but is not really well maintained. According to Alessandro, there is no clear policy for the .italia.it-domain.
- The main reason for introducing a uniform government domain (gov.it) has been recognizability by citizens. The government deems it relevant that citizens can trust the government and it is believed that maintaining a uniform domain is contributing to that goal. It is one of the measures to take to enlarge trust. Furthermore, having a uniform domain allows the government to prevent name clashes between different public entities which are willing to register websites under the same names. Lastly, keeping a gov-it-domain allows for safer manageability of the domain. It is easier to perform security scans.
- Although the registration of public entities at the gov.it-domain is mandatory, not all organizations are actually registering their websites on this domain. The ministries of justice and foreign affairs are examples of departments that are not yet registered at the gov-domain. Alessandro confirmed that they indeed do not comply with the directive, but that this can be mainly attributed to technical difficulties in transiting. Nevertheless, his guess would be that 90 percent of the public entities are registered under the gov.it-domain.
- Although not all public entities adopted the gov.it-domain, it is not really a top priority of the Italian government to make them do.
- There was no public communication strategy employed for the gov.it-domain. According to Alessandro, it was not needed, because people are not very interested in the specific name of government websites. Instead, it is more important that they can have the certainty that ones they are on a government website they know that it is authentic. The uniform government domain contributes to this.
- Alessandro is not aware of any policy evaluations to the effects of the introduction of a uniform government domain. He nevertheless mentioned that there is a national database (*Indicepa*) in which information about all Italian public entities is accessible for citizens. This website also collects lots of public data about the administration.
- There are no records about how much the migration to the gov.it-domain has costed so far. This depends on the number of already existing platforms for government organizations before the transition took place.
- Lastly, we asked whether Alessandro could provide us with lessons learnt from his country. He named the following things:
  - Focusing more than Italy did on naming conventions. That means: how do you organize the allocation of names and what are preferable names for public entities? For instance, how may a municipality call its website? City of Rome or municipality of Rome? You must carefully think about these things.
  - Although not all public entities are living up the obligation to register under a government domain, making your domain name strategy mandatory is a good thing. Optional domain choices will end up in messy situations.
  - Think carefully about how you arrange the transition period. This includes choices on how long old website names may stay and for how long old e-mail addresses may be used.
  - Be aware of good technical guidance in the migration and integration (for instance, the SSL).

D. 3 Oostenrijk

- Although the gv.at-domein has existed since the 90s, the first official policy document regarding the government domain was written in 2005. This original policy document was amended in 2007. You will find the documents on https://www.ref.gv.at.
- The policy owner is the BLSG-board (Bund, Länder, Städte, Gemeinden). This board is responsible for the e-government regulations and defines e-government strategies.
- Last year, a new version of the policy was released in which a less stricter use of the gv.at-domain is prescribed. The most important change was the moderation on accepting not just the formal Austrian governmental organizations on the gv.at-domain, but also organizations with a public goal. Now, also companies and foundations that provide public services are invited to register under the government domain. According to Gerhard, the current policy is more service oriented.
- The Austrian policy is strongly recommended to all public entities, but is not mandatory. The Ministry of Digital and Economic Affairs do not have the legislative power to enforce the government domain strategy. This can be mainly attributed to the relatively autonomous position of governmental organizations in Austria.
- Nevertheless, the policy is well adopted by various public entities. Gerhard's guess would be that over 1700 state organizations are registered under the gv.at-domain (those include departments, agencies, länder, cities and municipalities). However, the total number of websites registered under gv.at is probably much higher, because of the use of subdomains. Moreover, because of the newly released policy version the number of participating organizations will also increase.
- The high adoption can be mainly attributed to a good internal communication strategy through which awareness was created. And the timeline was helpful as well. When starting with the policy a lot of projects were at a certain point, what led to a wide-spread use of the 'gv.at' domain. Another key-success factor is the service-orientation.
- There are several (approximately less than 10) exemptions being made, mainly for technical and security reasons.
- The rationale behind the policy is mainly security and trustworthiness. Citizens can rely on the 'gv.at' domain. Gerhard also named the advantage of keeping control of entities that wish to claim public names. With an explicit policy on government domains those names can be reserved for government organizations.
- Many public entities (municipalities for instance) (still) think that it's important for the findability to have a short domain name. Thus, without an additional second-level domain (.gv). The need for explaining that this is not the case, remains. It is the ongoing duty of the central government to raise awareness of the importance of maintaining a uniform government domain.
- The formal domain registration process for gv.at is done by Gerhard, the WHOIS database operation is outsourced to the university of Vienna. Within the years, the Ministry responsible for the maintenance of the government domain has shifted to the Ministry of Digital and Economic Affairs, but this was purely because of bureaucratic reasons.
- The Austrian government has deliberately chosen for *name*.gov.at instead of gov.at/*name* (=website in the form of a single platform). The main reason for this is the vulnerability of maintaining a single platform. Ones keeping a single platform, the government will be much more vulnerable to possible cyber-attacks that could paralyze the government website. Moreover, because of technical difficulties Austria uses her policy, based on a federate-concept.

- From the start of the domain policy there has been a communication strategy to inform a wider public. This has been done through internet and headers in e-mails, but also through newspapers and for instance communication on ‘visit-cards’.
- The costs for having a domain name policy (and WHOIS and name service infrastructure) are rather low for the public budget. The services are provided anyway by the partner-organizations. The extra costs for operating a ‘.gv.at’ domain name are taken care by the university of Vienna.
- When discussing and deciding about the policy, finance was never taken into account. Leading was in the decision process were the quality and security. About the total costs of the operation no numbers are available.
- The entry in the public suffix list was made by the national registration agency for security reasons. Only the top-level gv.at is listed. HSTS preload is not in use for gv.at, since there are no webservices directly under this domain. Other registrations of subdomains under gv.at are in the responsibility of the owner.
- Lastly, Gerhard advices the Dutch government to enforce the policy if it is legally possible.

D. 4 Verenigd Koninkrijk

- In the United Kingdom, the domain name strategy and establishment of the platform gov.uk has been part of a bigger online strategy for the entire government. This online strategy includes things like:
  - A uniform government infrastructure online
  - Security
  - Open standards and open sources
  - UX elements
  - Etc.

  Because the UK treated their domain name strategy as part of a broader strategy/program, James does not belief that the decisions the Dutch government is facing right now regarding a separate domain name policy are similar to the UK case. It is a different business case in his eyes.
- The relative success of the gov.uk-platform (the overall adoption by organizations from the central government is quite high) can be partly attributed to huge government support. During the first cabinet of Cameron, there was a strong belief that ‘going digital’ was going to be crucial in future online services and that focus on delivering great services to users was of key importance in that strategy. The respondent noticed that without such political backing the realization of the whole digital strategy would have been less effective.
- Although lots of government organizations at the central level are registered under the platform gov.uk, the overall adoption is not 100%. There are still numerous organizations that haven’t switched to the central domain. However, because the platform has been only established since 2014, the transition is still ongoing.
- Also some digital and electronic services are integrated on the gov.uk-platform (for example, filing tax returns). Our respondent told that the implementation of integrating such services on a single platform is quite hard and takes a lot of time. This also holds for the gov.uk-platform where the digital services were not immediately included from the start.
- Although independent government organizations like to maintain their own so called identity (or brand) in things like an own website, the identity is still guaranteed at the gov.uk-platform according to James. However, it may take some time to convince organizations about the advantages of the use of a single platform.

- Because of the autonomy of local governments, they are not registered under the central platform. Nonetheless, they are invited to use the second-level domain *.gov.uk. In the end, it is their own choice whether they use this government domain or not. Put differently: it is not obligatory for local governments to use the SLD .gov.
- There are no policy evaluations to the uniform domain name policy. Nonetheless, the gov.uk-platform has resulted in less operational costs for the maintenance of separate government websites.

Van een ander contactpersoon, Roy Slinger, ontvingen wij een ingevulde questionnaire, omdat hij op het laatste moment niet in de gelegenheid bleek om een telefonisch interview af te nemen.

- *What is the policy on unified domain name extensions for your government?*

  We have no formal policy on this. We control this through 2 pieces of guidance: - Apply for a .gov.uk domain name: step by step - Exemption guidance
- *Is the policy mandatory or optional? And are there any exceptions in case of ' compulsory ' compliance?*

  Guidance is developed in lieu of formal policy. However, meeting the guidance when requesting a .gov.uk domain is required.
- *Is the policy laid down in laws and/or regulations? And if so, in what way?*

  No.
- *For which government/governments does the established policy apply? (i.e. central government, local government, agencies, etc)*

  This applies to all .gov.uk domains. This includes central government, local government and agencies. All organisations that can use the .gov.uk domain name are set out in the guidance.
- *How is the monitoring of compliance with the policy organized?*

  Compliance is checked on application. Ongoing compliance is the responsibility of the individual organisations.
- *Who makes the policy and who establishes it? Guidance is developed in lieu of policy.*

  This is published and maintained by Government Digital Services (GDS), which is part of the Cabinet Office.
- *Has the policy changed over the years, and if so why?*

  Guidance is developed in lieu of policy. However, the guidance on what gov.uk applicants must follow has iterated. For example, we have moved as much as possible from ‘rules-based’ guidance to ‘objectives-based’ guidance to give the guidance a longer lifecycle and provide organisations with more choice about domain names.
- *Which uniform domain name extension (SLD, gTLD) – the exact naming- has been chosen, and if so why? Did the availability of a particular ' name ' also be played?*

  .gov.uk - No local knowledge or history of the how the decision was made.
- *How specifically is the domain name policy elaborated? (i.e. Which sites are covered, which are not? For websites as well as e-mail? What does the application process look like, and what is the turnaround time? Do ' old ' domain names remain in use, are they quarantined, and are these domain names ever released again? Are there specific situations (think of Commonwealth, colonies, special state law positions of institutes) that have to be taken into account?)*

Guidance shows naming criteria and eligible organisations. Issued domains are not type specific (no e-mail only or website only domains). Once a domain is issued organisations have control over what records are added. The process to apply for a .gov.uk domain name is relatively straightforward. 1. Organisations check they are eligible, get permission and then apply for a .gov.uk domain with a registrar. 2. This application is passed onto the registry who shares this with a Naming and Approval committee (NAC), which is chaired by GDS. 3. The NAC review the application and let the registry know whether the application was approved or rejected.

Turn around time on average is 5 days. Old domains are currently put back into the pool but this under review.

- *What are the requirements for using unified domain name extensions?*

  The requirements can be seen in the guidance.

- *To what extent is the public suffix list and HSTS preload used?*

  There are some entries in the PSL and there is HSTS guidance in place for gov.uk. Not required for other government websites.

- *To what extent has attention been paid to the concrete elaboration of the domain name policy: a) recognizability b) findability c) reliability d) security e) manageability*

  This is covered in the naming guidance.

- *What are the main reasons for choosing the policy as described under 'A' and what were the intended goals and/or expected (ex ante) effects?*

  The gov.uk domain denotes association with the UK government. Access to the .gov.uk domain is controlled through government, allowing a high degree of domain control, allowing structured and regulated use of the domain to be implemented. The exclusivity of the domain allows government to build trust and association with the domain. The availability of subdomains of the .gov.uk domain is high.

- *Have there been specific causes which resulted in formulating a uniform domain name extension policy? If so, what were these causes?*

  The development of government sites (directgov, businesslink, and latterly GOV.UK). GOV.UK especially resulted in the establishment of domain structures, for example: service.gov.uk, campaign.gov.uk, api.gov.uk, data.gov.uk, along with guidelines for how sites and services on these domains would function.

- *Has a business case/cost-benefit analysis been part of the considerations and, if so, what influence did it have?*

  Not that we are aware of.

- *Have alternative scenarios been investigated for the application of a naming policy? And if so, which ones?*

  Not that we are aware of.

- *To what extent has the pre-estimated duration for the introduction of the policy – the transition phase – played a role in the policy choice made?*

  We're not aware of any pre-estimated duration for the introduction of the policy.

- *Have alternative deployment scenarios been investigated? And if so, which ones?*

  None that we are aware of.

- *What were the considerations to oblige or not to require domain name policy?*

There is an obligation (non-legislative) for us to track government sites, and maintain a degree of control over the government online estate. C. The consequences/impact of the introduction of the policy

- *Who is the policy owner?*

  Cross government responsibility.

- *Who is responsible for the implementation of the policy (domain management)?*

  Overall government domain name policy is the responsibility of the Department for Digital, Culture, Media and Sport.

- *How is it ensured that all parties for whom the policy applies participate? ('Carrot' or 'stick')*

  GDS owns the registration approval process. Applicants cannot register a .gov.uk domain without GDS approval.

- *How is the policy for a unified domain name extension rolled out? (Big bang, phased, gradually via new sites, etc.)*

  The policy for the GOV.UK website and associated domain name was launched in January 2012 using a 'Big Bang' approach.

- *Which public communication has been deployed?*

  Guidance is published on the GOV.UK website

- *What internal public communication has been deployed?*

  We publish step by step guidance for communities to adhere to when applying for a gov.uk domain name. This is available on the GOV.UK website.

- *What contacts have been established with ' communities ' in the country?*

  We publish step by step guidance for communities to adhere to when applying for a gov.uk domain name. This is available on the GOV.UK website. A contact e-mail address is provided for any queries

- *How is the ' registry function ' of the domain technically implemented?*

  The gov.uk registry is outsourced to a third party registry operator with a Registrar channel providing end user services.

- *How is the (eventual) transition for e-mail domains technically addressed?*

  Not applicable, most, if not all organisations that require a gov.uk domain are already using as gov.uk has been in place for over 20 years.

- *How is the (eventual) transition for websites technically addressed?*

  Not applicable, most, if not all organisations that require a gov.uk domain are already using as gov.uk has been in place for over 20 years.

- *Does a unified domain name extension offer technical advantages compared to no unified domain name extension?*

  Domain names are a valuable asset and require a long-term financial and operational commitment. The Government Digital Service (GDS) assigns approved .gov.uk domain names on a first come, first served basis on behalf of the Cabinet Office. This is according to strict eligibility requirements, outlined in the guidance.

- *In relation to the questions under B: What were the effects? Have the (ex ante) expectations come out? Have the effects been achieved? Is it possible to make a subdivision in answering these questions: a) recognizability b) findability c) reliability d) security e) manageability*

  All of the points above are key considerations in why we value the use of the gov.uk domain. Further information on the brand GOV.UK and use of the .gov.uk suffix is below.

- *To what extent have users and customers become accustomed to the domain name policy?*

  GOV.UK is an established brand as is the suffix .gov.uk. Central to the digital transformation of government has been the GOV.UK website.
  Launched in January 2012, GOV.UK replaced 1,882 separate legacy websites and has saved government £63m per year (the ongoing avoided annual cost of government having multiple sites and publishing platforms). It currently sits in the top thirty most-visited sites in the UK with 4.6 billion visits (3.6 million visits per day on average). It has delivered on Martha Lane Fox's recommendation that it should become "the government front end for all departments' transactional online services to citizens and businesses".
- *To what extent is there a citizen's acceptance?*

  Citizen acceptance is high GOV.UK is an established brand, as is the suffix .gov.uk
- *What were the unexpected effects?*

  GOV.UK has saved government £63m per year (the ongoing avoided annual cost of government having multiple sites and publishing platforms)
- *To what extent does the knowledge of today invite – if there is still no domain Name policy – to re-enter domain name policy?*

  Although there is no formal policy, the. gov.uk domain denotes association with the UK government. Access to the .gov.uk domain is controlled through government, allowing a high degree of domain control, allowing structured and regulated use of the domain to be implemented.

D. 5 Verenigde Staten

- The .gov-domain is in use since 1985. The US has been the first country to introduce a specific government domain and is also the only country to use a .gov as TLD instead of a SLD. The GSA was delegated the task of managing the .gov-domain from the federal networking group in 1997.
- Originally, the .gov-domain was destined for the federal government, but in 2003 it was decided that also states, cities, counties, tribes and native sovereign nations might use the .gov-domain.
- The use of the .gov-domain is mandatory for the federal government and optional for non-federal governments, following the constitution.
- In April 2019, approximately 20 percent of all US cities and counties were registered at the .gov-domain. This makes up 56 percent of the total use of the .gov-domain. The federal administration counts for 22 percent, the states for 20 percent and tribal groups for around 3 percent.
- However, it is the ambition of the GSA to migrate all local government institutes to the .gov-domain before the presidential elections of 2020 will take place. According to Marina, this can be seen as a real shift compared with the past, because the use of the .gov-domain is now far more heavily promoted by the federal administration for all government organizations.
- The necessity to have all government organizations on the same TLD (.gov) originates from at least two reasons. First, the federal administration wants to ensure a safe intergovernmental communication. Because of the increased complexity of state issues and the increased cyber threats (hackers, attempts of phishing), an safe and secure communication between government organizations at different levels is vital, according to Marina. This stance is also reflected by federal organizations like the FBI, which has plans to oblige direct communication merely through email-accounts which entail a .gov extension, otherwise, they say, they cannot verify whether the message is real or not. It is reasoned that if you are not registered on the .gov-domain, you are not a government.

- Second, in addition to internal security reasons, recognizability for citizens is also an impetus in the current efforts to migrate all government institutions to the .gov-domain. According to Marina, citizens get confused if for example counties are using other TLDs, such as .com or .org, than .gov. Moreover, there is a serious risk that fake government websites are registered (Marina had several examples of these) which spread fake news, but are nevertheless trusted by citizens because they look very similar to real government websites. The belief is that with a uniform .gov-domain citizens can really ensure whether they deal with true and sincere instead of false and untruthful government communication.
- Although a real urgency is felt to migrate all government organizations to the .gov-domain, the federal government cannot force this. It is therefore heavily promoted by the federal government. An example of this is that the GSA is actively helping counties in the, technical, migration to the .gov-domain by ensuring that the old website names are maintained and become HSTS-proof. Moreover, the GSA is actively tracking down cities and counties that are not yet using a .gov-domain and try to convince them of the importance of a single TLD for the entire government. One of the means to effectively spread this message is the so called one-pager or leaflet Marina sent us.
- In general, local authorities are relatively eager to register their domain names and email addresses at the .gov, especially the bigger ones. However, for the smaller counties and villages, the price tag of 400 dollars for a .gov-registration is a firm threshold. There are nevertheless plans to somehow bypass this in the near future. Another serious threshold consists of the branding, in the form of emails and social media, that has been performed by some counties that they are not really willing to give up overnight.
- The ambition of the GSA is to have at least 80 percent of all counties and cities registered under the .gov-domain in 2020. However, as said by Marina, they ‘don’t know how many dogs will bark’. The challenge of the GSA is to discover the websites that do not use .gov yet and convince them to use it.
- Most information (policy, directives, criteria) regarding the .gov TLD can be found at the website home.dotgov.gov.

D. 6 Nieuw-Zeeland

- *What is the policy on unified domain name extensions for your government?*

  The Department of Internal Affairs (DIA) maintains a moderated namespace of .govt.nz domain names for use by central and local government agencies. Under the moderation policy governing the namespace, agencies may apply to register new third-level domains under either of two rationales:
  a. Organisational domain names that reflect the name of the agency applying
  b. Domains used for ‘pan-departmental projects of national significance’, which are required to be ‘specific and descriptive’

Discretion under the policy has led in recent years to DIA granting registrations for a wider variety of reasons than the above. In practice domains are also granted for:

c. Projects and campaigns where the domain is appropriately aligned with a wider public presence
d. Technical purposes, such as cloud services or APIs
e. Translations of domains into the reo Māori

Decisions with impacts for local government are made in conjunction with the Association of Association of Local Government Information Managers (ALGIM). A much smaller moderated domain, .parliament.nz, is also maintained with Parliamentary Services for the use of Offices of Parliament.

- *Is the policy laid down in laws and/or regulations? And if so, in what way?*

  The moderation policy is documented in an agreement between DIA and the Domain Name Commission, a subsidiary of the non-government body, InternetNZ, which maintains the .nz Registry. This policy is also published for agencies' reference at Digital.govt.nz. The current version of the policy dates from 2009.

This policy document establishes:

a. The eligibility of agencies to apply for .govt.nz domains
b. The reasons domains may be applied for
c. DIA's authority to grant or reject applications and to exercise discretion in the application of the policy, and an appeals process

It does not require agencies to make use of a .govt.nz domain, or otherwise refer to the use of non-.govt.nz domains by government. There are no more general directions, mandates or regulations guiding agencies in this area.

- *What are the main reasons for choosing the policy as described under 'A' and what were the intended goals and/or expected (ex ante) effects?*

  The moderation policy was originally drafted with the intention of limiting new registrations within the namespace and restricting the proliferation of government websites. It envisioned a limited total number of government websites that mostly correlated with individual government agencies, or to major national projects.

- *To what extent have the following aspects played a role in the consideration?*

  - Recognizability
    Public recognition and trust in an authoritative, closely-moderated .govt.nz namespace in the eyes of the public was the primary goal of the policy; the number of domains held by each agency was intended to be limited partly in order to strengthen the recognisability of those domains.
  - Findability
    Clarity of domain names amongst users or issues such as search engine optimisation were not foci of the policy; e.g. the focus on organisational names meant many .govt.nz domain names were based on acronyms.
  - Reliability
    While the policy envisioned agencies using primarily organisational .govt.nz domains, whether or how members of the public could rely on encountering .govt.nz domains more broadly was not a major consideration.
  - Security
    The security of .govt.nz domains has been the focus of DIA's management of the namespace, e.g. by introducing DNSSEC to the namespace in 2015, and maintaining secure and resilient nameservers for hosting .govt.nz domains.
  - Manageability
    A limited, manageable government web domain was an intended outcome of the policy, however the mechanics of managing domain name policy were less considered.

- *How is the policy of a unified domain name extension elaborated in:*

- Issuance process (central/decentralised)
  Third-level domain name applications must be made to DIA, where they are considered by a team within the staff of the Government Chief Digital Officer. Once a third-level domain has been granted, agencies may utilise the fourth or subsequent levels at will.
- Requirements/Frameworks
  The moderation policy is supplemented by advice published or given out by DIA.
- Automated Checks
  A WHOIS check is carried out on application for new registrations.
- Methods for impact measurements
  The number of registrations or cancellations within the .govt.nz namespace can be assessed by DIA as the registrar; measurements outside the .govt.nz namespace are limited.

- *How is the policy for a unified domain name extension rolled out? (Big bang, phased, gradually via new sites, etc.)*
  New domains have been added to the .govt.nz namespace over time upon application.
- *What were the introduction costs?*
  The .govt.nz namespace has operated since the 1990s, while the existing moderation policy was introduced in the 2000s. Costs from this time are undetermined.
- *Which public communication has been deployed?*
  DIA publishes information about the .govt.nz namespace and moderation policy on Digital.govt.nz/DNS, however this is intended for agency consumption. Public marketing or communications for particular domains is carried out by agencies.
- *How is the ' registry function ' of the domain technically implemented?*
  DIA is an authorised registrar within the .nz Registry, and works with an external vendor to provide registrar services to agencies, including nameserver hosting and a DNS management portal.
- In relation to the questions under B: What where the effects? Have the (ex ante) expectations come out? Have the effects been achieved? Is it possible to make a subdivision in answering these questions to:
  - Recognizability
    The .govt.nz namespace is widely recognised and trusted by the public. However, a number of high profile government websites using other domain extensions – either by choice, or in, some cases, because applications for .govt.nz domains were declined under the policy – has meant a .govt.nz domain name is not synonymous with a government website in the eyes of the public.
  - Findability
    The policy defined acceptable domain names by a more bureaucratic (i.e. organisational structure or certain programmes) than user-oriented logic. This resulted in many domain names using terminology that was unfamiliar to the public, a high incidence of acronym-based domains, and domains that became out of date or needed to be replaced as agency structures changed. The policy also did not allow for the alignment of domain names with public branding if the domain was otherwise ineligible. In recent years, DIA has endeavoured to grant domain names that reflect what members of the public are expecting to find more closely, e.g. subject matter keywords or widely promoted terms.
  - Reliability
    The policy did not address the usage of non-.govt.nz domains by agencies – and in

some cases effectively encouraged it by declining .govt.nz registrations – leading to a very large number of government websites using other domain extensions (.co.nz, etc). As a result, while the public can rely on a .govt.nz domain indicating a legitimate government website, they cannot rely on a government website to have a .govt.nz domain.

- Security
  While the .govt.nz namespace has been operated securely and without incident, government domains registered in other namespaces have had a variable level of security. Registrations in commercial namespaces outside of the government registrar are also frequently made with incorrect registrant information technically granting ownership of agency domain names to agency employees, contractors or vendors, with potential security implications.
- Manageability
  The demand from agencies for new domain names has outstripped expectations at the outset of the policy, and the ability to use a restrictive registration policy as a lever against web proliferation was over-estimated. This has resulted in a higher number of .govt.nz domains than expected (roughly 1100), and many other government domains registered outside of the scope of the policy. The lack of a mechanism to track latter domains outside of the .govt.nz namespace has resulted in poor visibility over the total government web domain, impacting the manageability of domain name issues, but also the ability to assess and audit security, accessibility and other web standards across government.

Op basis van de antwoorden uit deze vragenlijst stelden wij een aantal vervolgvragen:

We understand that the use of .govt.nz is not obligated. Nevertheless we read that the use of .govt.nz is wide-spread. What then is the secret behind? In what way are the services you offer (for instance the translation into te reo Maori) helpful to tempt the use of the .govt.nz domain?

The .govt.nz domain is widely recognised by the public and considered an authoritative and appropriate indicator of a government website's authenticity. For this reason, many government departments voluntarily register a .govt.nz domain, at least for their primary corporate website (e.g. DIA.govt.nz for the Department of Internal Affairs).

However, for many other types of website more separate from the department's corporate identity – e.g. websites for tools, campaigns, particular subject areas or groups – government departments often register other commercial domain types, such as .co.nz. This can sometimes be down to the decision of an individual project team (or a vendor hired by that team, like a marketing agency or IT provider), who might want to separate their own identity from the government for branding reasons, be more familiar with other commercial domain types, or assume that registering a .govt.nz domain would be too difficult or time-consuming.

Additionally, where .govt.nz domains are registered for a website they may still be used alongside commercial domain types or to redirect to them (e.g. the Accident Compensation Commission's website is available at acc.govt.nz or acc.co.nz).

One service that was intended as an incentive is the government domain name hosting and management platform which was available exclusively for .govt.nz names. This management portal and nameserver system features a high level of security and features such as DNSSEC that are rare in commercial providers. However, this had the unintended consequence not of reducing commercial domain name registrations – which can have a lower level of security related to their registration and ownership – but causing them to be hosted on often-insecure and out-of-date

nameservers with a very low level of visibility. As a result, we have recently opened the government domain name hosting and management platform to commercial domain types, and this will no longer be an exclusive incentive to register .govt.nz names.

Can you give some figures (numbers, percentages) about the usage of the .govt.nz domain and or about its spread?

There are around 1086 registered .govt.nz domains. Of these, about 500 are hosted on the government name server infrastructure, while 600 use various commercial or custom platforms.

The total number of government websites using non-.govt.nz domains like .co.nz is not recorded.

In some countries we see a preference for 'govt.cc/… instead of '... .govt.cc', especially when they take into account the use of search engines like Google, Bing in future. Is this in NZ a topic of discussion as well? If so, can you tell something about your reasoning and your points of view on this?

As a broader digital strategy, the NZ government has generally left a high level of agency in the hands of individual departments as opposed to structuring web assets centrally; for instance, New Zealand has not consolidated a large number of websites into one central government website like gov.uk. For domain names specifically, individual third level registrations allow agencies to manage their domains largely independently.

A related issue is that due to the technical architecture of the .nz namespace, registering 'govt.nz' directly at the second level is not currently possible. We do have an all-of-government branded website www.govt.nz – but technically this is in fact a third-level registration of ***www***.govt.nz (i.e. it could be properly described as www.www.govt.nz). Due to the reasoning above, there hasn't been the appetite to re-architecture the namespace to allow for this.

And lastly: What are the lessons learned (pitfalls, critical success factors, do's and don't)?

One lesson is that once some domains have been ruled 'outside the fence', it is very difficult to regain visibility of them. The initial .govt.nz moderation policy was restrictive but did not have any formal mechanisms for preventing departments from registering other types of domains. Once these other domains were registered, central services were not provided for them. The net result was a large number of government domains registered that government now lacks a central view of – in many cases individual departments do not have a comprehensive list of their own domains either. There is a growing level of concern about the security, privacy, etc. positions of these websites and building a more comprehensive view of government domains for auditing purposes will now be an extensive task.

I'd also say our experience has shown that without a mandate to enforce compliance, it is difficult to achieve consistency across government. While uptake of .govt.nz domains on a voluntary basis is high, there are still many government websites using other domains, including some very high profile and major websites. The decision to not use a .govt.nz domain can be made for a variety of reasons, including the personal preference of the senior management of the day. Ultimately this means a less consistent experience for the public and impacts the level of trust the public can have in digital information and services from government.

We have spent a lot of our focus on building out the infrastructure side of domain management aside from registration policy – i.e. the nameservers and a DNS management portal – which is not something there is necessarily a government service for in many other jurisdictions (e.g. gov.au is now considering developing this service after acting purely as a registrar). This has increased the

appeal of .govt.nz domains, led to greater engagement with departments over domain name issues, and contributed to our team's broader goal of increasing security for web services across government. As the commercial market for DNS services in New Zealand is rapidly transitioning to off-shore cloud services, our DNS platform may soon be one of the only traditional on-shore DNS set-ups of its type. This dynamic is obviously playing out for web hosting services as well, but for disaster resiliency and national security purposes it's of particular interest for DNS in New Zealand.

D. 7 Portugal

- *What is the policy on unified domain name extensions for your government?*

  All bodies, services and structures of the direct administration of the State must register their website under the .gov.pt classifier domain.

  Exception may be made to State bodies, services and structures, including tripartite or ad hoc committees, which, by virtue of their statutes, mission or area of activity, should, for justifiable reasons, fit into other existing classifying areas, such as domains .org.pt and .edu.pt.

  On an optional basis, indirect administration entities, on their own initiative or in the execution of general guidance of the Government member responsible for the respective area, may request the registration of their website under the .gov.pt classifier domain.

- *Is the policy laid down in laws and/or regulations? And if so, in what way?*

  The policy described in the previous point is embodied in the Resolution of the Council of Ministers no. 34/2016, of 16 June, which establishes that all bodies, services and structures of the direct administration of the State must register their website under the domain .gov.pt., reserving the possibility for the indirect administration of the State to proceed to the same registration, on an optional basis.

- *What are the main reasons for choosing the policy as described under 'A' and what were the intended goals and/or expected (ex ante) effects?*

  To define an identity and image that unambiguously identifies specific websites as a public service.

- *To what extent have the following aspects played a role in the consideration?*

a) recognizability
b) findability
c) reliability
d) security
e) manageability

The Government Shared Services Entity's (eSPap) reasons to adopt current uniformed domain name extensions policy were: recognizability, findability, reliability and manageability.

- *How is the policy of a unified domain name extension elaborated in:*

a) Issuance process (central/decentralised)
b) Requirements/Frameworks
c) Automated Checks
d) Methods for impact measurements

For accessing the impact of introducing the current policy, eSPap use central issuance processes and several automated checks.

- *How is the policy for a unified domain name extension rolled out? (Big bang, phased, gradually via new sites, etc.)*

The adoption followed a soft scheduled calendar, continuously adapted during the project to business constraints.

- *What were the introduction costs?*

  The implementation of the current uniformed domain name extensions policy was made by eSPap's own staff (processes, IT, PM), so the only costs incurred were internal.

- *Which public communication has been deployed?*

  Each organization set up its own communication strategy. However, almost all the entities used the same tools based on their own communication channels (intranet, direct e-mails campaign, company website, etc.), and different timings and messages adapted to their specific stakeholders and businesses.

- *How is the ' registry function ' of the domain technically implemented?*

  The registration function was centralized at one specific entity, CEGER (IT center responsible for providing services, for example, to the prime minister cabinet. They own the technical administration of gov.pt domain and its DNS service.

- *In relation to the questions under B: What where the effects? Have the (ex ante) expectations come out? Have the effects been achieved? Is it possible to make a subdivision in answering these questions to:*

a) recognizability
b) findability
c) reliability
d) security
e) manageability

The adoption of the new policy concerning uniformed domain name extensions consolidated the strategy of delivering public services through the internet, helping the citizens and companies to easily find and use those services.
Considering the essential role that digital channels play in the functioning of contemporary Public Administration, the Government is now proposing the implementation of measures aimed at ensuring the reliability and security of government domains (gov.pt), avoiding thus the appropriation of these domain names by entities outside the Public Administration, for other purposes than administrative activity.
Considering that the .gov top-level domain is crosscutting and can therefore cover not only the central government but also all public entities of indirect administration, the measure is intended to apply generally to all public entities, with special focus on direct administration bodies.

Op basis van deze response stuurden wij een drietal vervolgvragen. Hierop volgde het volgende antwoord:

- *What is meant by direct and indirect administration? Can you try to explicitly name the state organizations that belong to each group? For example, government agencies, provinces and municipalities, under which group do these fall?*

  The direct administration of the State integrates all the organs, services and agents integrated in the State legal person that, directly, immediately and under the hierarchical dependence of the Government, develop an activity that tends to satisfy the collective needs.

  Not all services of the direct administration of the State have the same territorial competence, so they should be distinguished between:

  – Central Services, with competence across the national territory, such as Directorates-General organized in Ministries;

- Peripheral Services, with limited territorial competence, as with Regional Directorates.

The indirect administration of the State comprises public entities, distinct from the legal entity "State", which have legal personality and administrative and financial autonomy that carry out an administrative activity that pursues the State's own purposes. It encompasses:

- Personalized services - legal persons of an institutional nature with legal personality, created by the public power to, independently from the State legal person, carry out certain functions specific to the latter;
- Custom funds - legal persons governed by public law, instituted by an act of the public authorities, with a patrimonial nature;
- Public corporate entities - profit-oriented corporate entities, aimed at the provision of goods or services of public interest, in which the State or other state public entities own the entire capital.

Municipalities are part of a third group of Public Administration entities, that constitute the Autonomous Administration, and include both direct (central and peripheral) and indirect (public business entities) administration services.

- *We understood that the use of the gov.pt-domain is mandatory for the direct administration. Is this policy enforced, and if, how?*

  The Resolution of the Council of Ministers no. 34/2016, of 16 June, which establishes that all bodies, services and structures of the direct administration of the State must register their website under the domain .gov.pt., reserving the possibility for the indirect administration of the State to proceed to the same registration, on an optional basis.

- *In addition to the last question, you also wrote that there has been employed a soft scheduled calendar to let organizations migrate to the uniform government domain. However, at the same time, organizations are obliged to register. How do these two align?*

  Although the obligation exists, it applies only to direct administration of the State (as defined above) – the dead line established was 30th June 2017. Regarding indirect administration of the State, there was no obligation. However, those entities could as well request the registry of their name under the domain ".gov.pt". In these cases, there was no dead line and the adoption followed a soft scheduled calendar, as stated previously.

De vorige antwoorden volgden van Tiago Mendonça. Een ander contactpersoon, Nuno Brás Fernandes, stuurden ons ook nog het volgende mailtje over het Portugese beleid:

- The gov.pt has been widely adopted since then but it was up to each service to decide whether or not to use it;
- Circa 2016 we (CNCS-PT) produced a recommendation regarding the need to have a uniform approach regarding domain registration for the public sector;
- Then, a law came into effect in June 2016, stating that all the organs, services and structures of direct administration of the State should register their website under the gov.pt domain (please see the resume of this law below). This law was developed by other public entities, without our direct involvement;
- Apparently the effects of this law (whether its technical effectivity or other aspects such the ones you are more interested about) haven't been adequately monitored, publicly or through other mechanisms (e.g. academic research).

- Scope of the law:

  Since the .gov.pt domain is cross-sectional and can therefore not only cover the central administration of the State, but also all public authorities of the indirect administration, the measure is widespread and covers all organs, services and structures of the State Direct Administration and, optionally, the indirect State Administration.
- Main guidelines:
  - By June 30, 2017, all the organs, services and structures of direct administration of the State should register their website under the .gov.pt domain, without prejudice of the following paragraph
  - By joint dispatch of the member the Government responsible for the body, service or structure concerned and of the Government member responsible for the Presidency of the Council of Ministers, it may be exempt from the provisions of previous paragraph, the organs, services and structures of the State, including tripartite or ad hoc committees, which, by virtue of their statutes, mission or area of activity, should, for justified reasons, be included in other existing classifications, in particular the .org.pt and .edu.pt domains.
  - On an optional basis, the entities of the indirect administration, either on its own initiative or in general guidance of the Government member responsible for their respective area, may request the registration of domain names under .gov.pt, under the same conditions of the organs, services and structures covered by this resolution
  - If different registrations coexist for the same domain name, belonging to a body, service or structure covered by the 1st paragraph, the user response must always occur with the domain registered under .gov.pt.

D. 8 Europese Commissie

Aangaande het Europees beleid rondom het europa.eu-domein ontvingen wij van Carlos Torrecilla Salinas de volgende toelichting.

- Regarding the use of web domains, you need to know that all official European Union and European Commission websites are to be hosted on the europa.eu domain or on any of its subdomains (*.europa.eu). As the domain is owned and managed by the European Commission, we consider the use of this domain a proof of trustworthiness for the citizens and stakeholders. If a site is hosted on europa.eu, they can be sure the site is authentic.
- In order to ensure that our web visitors know it, we decided last year to introduce the “EU banner” in all European Union and European Commission websites. The main goal is to increase awareness about the use of the domain and reassure the visitors on the trustworthiness of the source they are visiting. We are currently in the process of rolling out the banner to all websites and we expect to finish by the end of the year
- The banner is provided by a centrally developed software library that webmasters can use and include on their website. The use of the library is limited to sites hosted on the europa.eu domain and its subdomains.

D. 9 Canada

- Initially, Canada used a reserved second-level domain for government communications (gc.ca). Fairly all government websites at the federal level were registered under the gc.ca-domain. The adoption can be therefore regarded as relatively high, although there were also organizations that

did not comply. In 2013, the government decided to move to a uniform platform, Canada.ca. At that moment, there was really political momentum for this move.

- The move to the central platform was presented by the rather conservative government as economically driven. According to Laura and Michèle-Renée, the most important reasons for establishing a central government platform were recognizability and manageability. Those two are very much related. First, when all government organizations are registered under the same domain (Canada.ca), it is much easier to manage your web contact from a central place. Moreover, it allows you as government to present yourself as unified brand. If all government communication look the same to the public, it is believed that it is easier for citizens to recognize and trust the government.
- All things considered, having a consistent look and using a consistent design as federal government contribute to recognizable and reliable government. In the whole move to the Canada.ca-platform the experience by the end user (=citizen) of digital government services was paramount. The operation can therefore not be disentangled from UX.
- The specification of content management at the Canada.ca-platform is described in the 'Content and Information Architecture Specification'. Here, one can find guidelines regarding the organization of content, the way URLs are build up and can be easily found and many more things. This web page cannot really be seen as a policy document, but rather as main internal strategy for government communication with the public at the federal level.
- Initially, it was aimed for that all government organizations (both departments and agencies) were to move to the central platform. It was even mandatory. However, after six years, the transition to the uniform platform was not yet completed. There were and are still non-compliers who wish to maintain their own website and brand. It is therefore very much believed by Laura and Michèle-Renée that enforcement is not effective.
- Instead, organizations are now also allowed to register a sub domain under Canada.ca. That means, Canada.ca is both a central platform and a second-level domain. Technically, two solutions for organizing a government domain are combined: the platform solution (Canada.ca/*) and DNS-solution (*.canada.ca), both with the same design and look. Most electronic applications and web services do use the second option, because it was technically too complex to register them under the central platform. Moreover, there was no real need to transit the existing and well-functioning applications to a different URL, with the additional risk that complications arise. In sum, it does not really matter how websites are technically organized (in DNS or at a central platform), it is much more important that they look the same and create the same UX.
- However, there are still 'outliers', organizations that are not (willing to) migrate to either the platform or to the DNS-solution. There are two groups to be distinguished within the outliers. First, there are the very small departments which simply lack the resources to invest in a migration to the platform. Second, there are the organizations that want to be distinguished, that want to contain their 'own brand' and as a consequence, are innovative in web design (e.g. Veteran Affairs). Especially this last group is problematic, given that they are employing a different look than other government websites. This goes contrary to the ambition of keeping a unified federal look.
- What do the Digital Transformation Office do with these non-compliers? As noticed, using a 'stick' (enforcing the policy) is appeared to be far from effective. Therefore, a different strategy is now employed. Instead of looking for confrontation, it is believed that persuasion by conversation is more effective. The Digital Transformation Office is pointing at the user testing that is being done with Canada.ca and its proven usability for citizens. Moreover, the so called innovators are invited

to share their ideas about web design in a special community. Try to harness their energy, creativeness, and use it for a more high-quality government look.

- March 2020 is used as target date to have all government organizations at the federal level be migrated to Canada.ca. It is realized that this date is rather optimistic, but at least there is more pace in the operation than before. It is the goal to move forward in the hybrid situation of today, because it is also believed that this hybridity may harm the trust of citizens in the federal government.
- The operation is exclusively focused on government organizations at the federal level. Government organizations at the regional (provinces) and local level (municipalities) are outside scope, because the central administration do not have the jurisdiction to enforce such a policy to decentralized governments.
- In addition to the rather extensive internal communication strategy, the central government is also employing a small public communication strategy to promote Canada.ca. This was done at the start of the central platform in 2013 and right now laterally on social media. Nevertheless, it is expected that such promotions will increase when the whole migration operation is completed.
- Lastly, I asked Laura and Michèle-Renée for advices for the Dutch government. What are things you must do and not do in the development of a central platform? In other words, what are the lessons learnt?
  - Do not try to control everything too tightly. Give organizations the space to be a little bit flexible in the way they like to organize their content.
  - Use realistic time frames. It was far too optimistic of us to think that 91 government organizations could be easily migrated to the central platform in less than five years.
  - Think carefully about the ultimate goal of the operation: what are you aiming for? In Canada this is very much having a uniform, recognizable government look, but this can be different for other countries. Subsequently, the ultimate goal determines the strategy you use. The measure to reach this, either by a platform or by a DNS-solution, are subordinate to that.