Een herkenbare en betrouwbare digitale overheid

Quickscan oplossingen en maatschappelijke effecten

Opdrachtgever: Ministerie van BZK

Rotterdam, woensdag 8 juli 2020

Een herkenbare en betrouwbare digitale overheid

Quickscan oplossingen en maatschappelijke effecten

Opdrachtgever: Ministerie van BZK

Walter Hulsker

Rotterdam, woensdag 8 juli 2020

ECORYS

Inhoudsopgave

1 Inleiding

Uit publieksonderzoek van het ministerie van BZK, directie Digitale Overheid, blijkt dat er op dit moment voor de gemiddelde burger weinig houvast is om te bepalen of een overheidswebsite of e-mail echt is en veilig kan worden gebruikt. [i] Uit het onderzoek komt naar voren dat herkenbaarheid en betrouwbaarheid van de digitale overheid gebaat kan zijn bij invoering van een uniforme domeinnaamextensie, zoals in verschillende andere landen al het geval is[ii]. Er zijn echter meerdere oplossingsrichtingen mogelijk die hetzelfde doel (deels) kunnen dienen.

1.1 Onderzoek

In dit onderzoek is een Quickscan verkenning uitgevoerd naar de maatschappelijke effecten van verschillende oplossingsrichtingen voor een herkenbare en betrouwbare digitale overheid (voor websites en e-mails).

1.2 Afbakening

De in dit onderzoek gehanteerde oplossingsrichtingen voor een herkenbare en betrouwbare digitale overheid zijn geïdentificeerd tijdens een workshop met professionals uit het digitale domein. De maatschappelijke effecten zijn kwalitatief in kaart gebracht. Wat betreft de effecten richten we ons primair op burgers en bedrijven (en indirect de overheid zelf).

Dit onderzoek is beperkt tot websites en e-mails van de overheid. Digitale communicatie van de overheid is aan verandering onderhevig, denk aan SMS, Facebook, later ook Whatsapp en Instagram. Dit zal blijven plaatsvinden. Deze veranderende wijze van communicatie is niet opgenomen in dit onderzoek. Het is aan te bevelen om in de toekomst ook andere vormen van communicatie te beschouwen. Op deze wijze ontstaat een integraal beeld van de herkenbaarheid en betrouwbaarheid van digitale overheidscommunicatie, wat een integrale aanpak mogelijk maakt.

MKBA als denkkader in deze Quickscan

Indien de belangrijkste effecten van een beleidsoptie niet goed genoeg kunnen worden gemeten of gemonetariseerd, dan kan een MKBA alleen schetsmatige informatie verschaffen met een beperkte betrouwbaarheid en relevantie. Wel kan het gedachtegoed van de MKBA dan als denkkader gebruikt worden om de besluitvorming te helpen structureren. Het gebruik van de MKBA als denkkader leidt echter niet tot een maatschappelijke kosten-batenanalyse en mag zo ook niet worden genoemd.

1.3 Leeswijzer

In het volgende hoofdstuk beginnen we met een korte schets van de problemen door de belangrijkste oorzaken en gevolgen op een rijtje te zetten. Vervolgens beschouwen we eerst de autonome ontwikkelingen, die relevant zijn indien wordt voorzien dat problemen in de toekomst al afnemen of worden opgelost door een ander project. Daarna komen de voor dit onderzoek geïdentificeerde oplossingsrichtingen aan bod. We geven een beknopte beschouwing van de belangrijkste maatschappelijke effecten en kostenindicaties. Het rapport sluit af met een samenvatting van de bevindingen en conclusies.

2 Probleemanalyse

De Raad van State constateert dat de omslag naar een digitale overheid, die momenteel gaande is, vergt dat we opnieuw overdenken wat wel en niet van de burger mag worden verwacht in het verkeer met de overheid[iii]. Zo blijkt bijvoorbeeld de digitale weerbaarheid van de Nederlandse samenleving niet overal op orde volgens het Nationaal Cyber Security Centrum[iv]. Zij geeft aan dat het vergroten van de weerbaarheid het belangrijkste instrument voor burgers, bedrijven en overheid is om risico's te verminderen. Een volledig en scherp beeld van digitale weerbaarheid en de omvang van (maatschappelijke) problemen die ontstaan door een gebrek aan deze weerbaarheid, ontbreekt. In dit onderzoek zijn kennis en inzichten over het onderwerp verzameld, wat vanzelfsprekend niet tot nieuwe informatie leidt.

2.1 Oorzaken

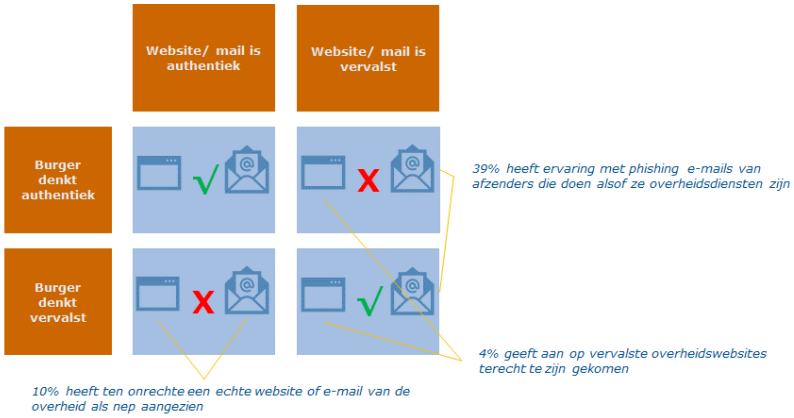
Om meer inzicht te verkrijgen in weerbaarheidsproblemen rond de digitale overheid heeft Kantar Public kwalitatief en kwantitatief onderzoek onder burgers uitgevoerd. In het onderzoek worden vier verschillende situaties onderscheiden die zich voor kunnen doen rond de herkenbaarheid van de digitale overheid bij burgers en bedrijven:

1. Authentiek wordt beoordeeld als authentiek
2. Authentiek wordt beoordeeld als vervalst
3. Vervalst wordt beoordeeld als authentiek. In dit onderzoek krijgt, onder deze situatieschets, ook private communicatie die door burgers en/of ondernemers als authentiek publiek wordt beoordeeld een plek (enkele voorbeelden waarbij verwarring kan ontstaan zijn de commerciële websites kadasterdata.nl en huurtoeslag.nl)
4. Vervalst wordt beoordeeld als vervalst

In de tweede en derde situatie is sprake van een verkeerde beoordeling en ontstaan mogelijk problemen, met in veel gevallen als oorzaak:

- **Een authentieke website of e-mail van de overheid is onvoldoende herkenbaar als betrouwbare bron**
  Uit het publieksonderzoek blijkt dat 10% van de respondenten weleens ten onrechte een echte website of e-mail van de overheid als nep heeft aangezien.
- **Onbetrouwbare bronnen vervalsen digitaal verkeer van de overheid**
  39% van de respondenten blijkt ervaring te hebben met phishing e-mails van afzender die doen alsof zij overheidsdiensten zijn en 4% geeft aan op vervalste overheidswebsites terecht te zijn gekomen.

Figuur 2.1 Resultaten uit publieksonderzoek van Kantar



2.2 Gevolgen

Om de belangrijkste maatschappelijke of economische problemen te schetsen die uit de hiervoor geschetste situaties kunnen ontstaan, is een onderscheid gemaakt tussen informatieverstrekking en transacties.

Ongewenste gevolgen bij informatieverstrekking:

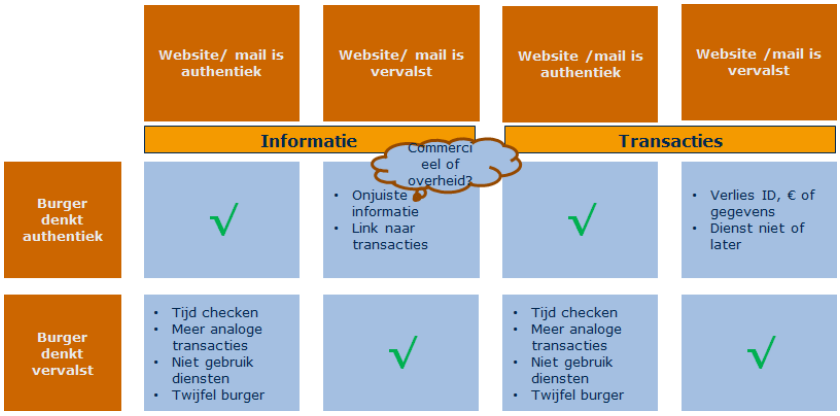
- Verspreiding van onjuiste informatie
- Extra tijd voor gebruiker ter controle
- Afzien van het gebruik maken van (digitale) diensten
- Meer analoge transacties

Ongewenste gevolgen bij transacties:

- Gewenste dienst wordt niet of later geleverd
- Verlies van ID, geld of gegevens

In volgend schema zijn deze ongewenste gevolgen per situatie voor informatieverstrekking en transacties overzichtelijk geschetst.

Figuur 2.2 Ongewenste gevolgen per situatie voor informatieverstrekking en transacties



2.3 Conclusie

In deze studie gaan we nader in op de gevolgen wanneer een authentieke website of e-mail van de overheid onvoldoende herkenbaar is als betrouwbare bron of wanneer onbetrouwbare bronnen digitaal verkeer van de overheid vervalsen. Dit leidt met name tot verspreiding van onjuiste informatie, extra tijdsbesteding van gebruikers van digitale overheidsdiensten en -informatie, het afzien van of later gebruik van digitale overheidsdiensten en eventueel verlies van persoonlijke- of zelfs identiteitsgegevens of geld.

3 Nulalternatief

In dit hoofdstuk beschouwen we de autonome ontwikkelingen, relevant indien wordt voorzien dat problemen in de toekomst al afnemen of worden opgelost door een ander project. "*Het nulalternatief is de meest waarschijnlijk te achten ontwikkeling […] in het geval de te beoordelen maatregel niet wordt uitgevoerd. Het nulalternatief wordt in de eerste plaats bepaald door de ontwikkeling van exogene factoren. Hiernaast omvat het nulalternatief bestaand beleid, voorgenomen maatregelen (althans, indien de uitvoering daarvan vrijwel onontkoombaar is) en kleinere ingrepen die het probleem deels oplossen of mitigeren maar geen zelfstandig beleidsalternatief vormen.*"
Voor deze definitie van het nulalternatief is aangesloten bij relevante leidraden[v] en werkwijzers[vi]. Een duidelijk beeld van het nulalternatief is bijvoorbeeld van belang in het geval problemen in de toekomst sowieso (fors) toe- of afnemen.

3.1 Relevante ontwikkelingen

Verschillende activiteiten en ontwikkelingen rond een herkenbare en betrouwbare digitale overheid zijn relevant voor en maken onderdeel uit van het nulalternatief. De volgende ontwikkelingen zijn hiervoor geïdentificeerd:

- De inwerkingtreding van de Wet digitale overheid[vii] met onder meer de uitrol van DigiD Substantieel en DigiD Hoog (met 2-stapsverificatie) en in het verlengde daarvan de uitfasering van DigiD Basis (met gebruikersnaam en wachtwoord).
- Samenwerking van de overheid met marktpartijen, zoals Google, om actief valse websites moeilijk vindbaar te maken of uit de lucht te halen.
- Burgers en bedrijven komen in toenemende mate via de zoekbalk en digitale assistenten, van bijvoorbeeld Google, op (overheids)websites terecht en niet door het invoeren van een domeinnaam in de browser.[viii]
- Toepassing van open standaarden zoals SPF, DKIM, DMARC voor e-mail en DNSSEC, HTTPS/HSTS en RPKI voor websites.[ix]

3.2 Autonome probleemoplossing

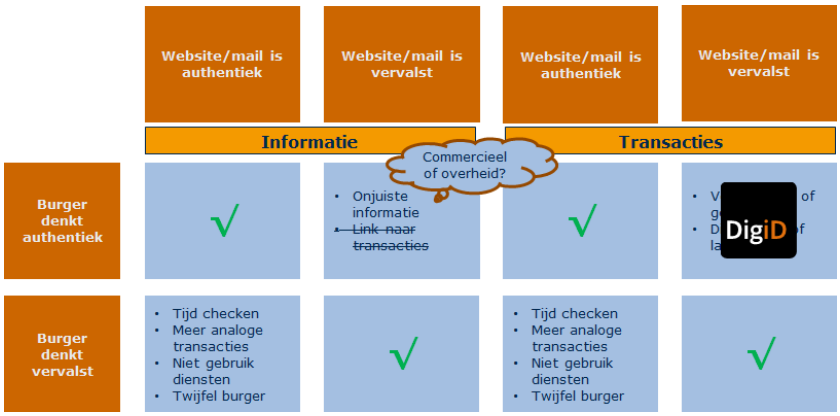
De ontwikkelingen in het nulalternatief zijn relevant indien een specifiek probleem bijvoorbeeld autonoom wordt opgelost (in het nulalternatief). Dan heeft een nieuw project (met de potentie om hetzelfde probleem op te lossen) geen meerwaarde meer voor het oplossen van dat specifieke probleem. Een simpel voorbeeld: wanneer iemand een paracetamol neemt waardoor de hoofdpijn weggaat, dan heeft het geen meerwaarde om na het nemen van de paracetamol ook nog een ander medicijn te nemen tegen dezelfde hoofdpijn.

DigiD 2-factorauthenticatie
Na de inwerkingtreding van de Wet digitale overheid zijn transacties op overheidswebsites op termijn alleen bereikbaar na inloggen met de DigiD app (met 2-factorauthenticatie op betrouwbaarheidsniveau substantieel of hoog). Indien een burger met de DigiD app probeert in te loggen op een vervalste website, dan krijgt deze bij 2-factorauthenticatie een foutmelding. Dat is een duidelijk signaal voor de burger dat de website vervalst is. De burger zal dan ook geen transacties verrichten waarbij mogelijk zijn identiteit, gegevens of euro's worden gestolen. Het risico van *verlies van identiteit, gegevens of euro's* wordt daarmee voor een zeer substantieel deel

opgelost. In dat geval heeft het geen nut meer voor fraudeurs om valse *links naar transacties* aan te bieden.

Deze geschetste ontwikkeling in het nulalternatief zorgt voor een oplossing voor de eerder geïdentificeerde maatschappelijke problemen '*verlies van identiteit, gegevens of euro's*', *'Overheidsdienstverlening wordt niet of later geleverd'* en *'links naar (vervalste) transacties'*. De overige geïdentificeerde problemen blijven zonder specifiek aanvullend beleid naar verwachting wel bestaan. In de volgende figuur is dit opgenomen.

Figuur 3.1 Overige geïdentificeerde problemen



De mate van gebruik van de DigiD app is afhankelijk van de adoptiegraad. Ofwel: hoeveel mensen hebben de mogelijkheden hiervoor (smartphone met NFC-lezer en identiteitsbewijs met NFC-chip[x]) en hoeveel daarvan maken ook daadwerkelijk gebruik van deze mogelijkheid? Het alternatief, wanneer mensen hier geen gebruik van kunnen of willen maken, kan dienstverlening op papier of aan een balie worden.

Continue ontwikkeling

Cybercriminaliteit blijft zich ontwikkelen. Zo wees het Nationaal Cyber Security Centrum in 2019 in Cybersecuritybeeld Nederland op de volgende, inmiddels opgeloste, ontwikkeling:
"Tweefactor-authenticatie voegt beveiliging toe aan traditionele gebruikersauthenticatie. Toch blijkt in de rapportageperiode dat criminelen ook hier op weten in te spelen. Dit bleek bijvoorbeeld uit de phishing aanval gericht op gebruikers van mijnoverheid.nl. Daarbij logden getroffenen in op een valse inlogpagina, waarbij de aanvallers ook de door de gebruiker ingevoerde sms-code misbruikten. Vervolgens werd geautomatiseerd ingelogd bij de persoonlijke MijnOverheid-pagina van de getroffene. Qua bredere trend lijken aanvallen gericht op het onderscheppen van sms berichten nog relatief zeldzaam, maar er is wel sprake van een toename."

Ongewenste gevolgen rond de digitale samenleving, zoals cybercriminaliteit, zullen altijd in ontwikkeling blijven. Oplossingen van vandaag worden op termijn achterhaald als gevolg van weer nieuwere en geavanceerdere ontwikkelingen (in onder andere cybercriminaliteit). Om schijnzekerheid te voorkomen moet worden onderkend en geaccepteerd dat hierdoor nieuwe risico's ontstaan waarop oplossingsrichtingen in deze studie geen antwoord bieden.

3.3 Randvoorwaarden en aandachtspunten

Bij deze oplossing zijn wel enkele randvoorwaarden:

- Er is uitgebreide publiekscommunicatie nodig over de DigiD app over een herkenbare en betrouwbare overheid (als onderdeel van de reguliere DigiD-communicatie).
- De burger moet een foutmelding begrijpen en beseffen dat de overheid altijd het gebruik van de DigiD app vereist voor digitale transacties op overheidswebsites. Indien een website vanwege 'gebruiksvriendelijkheid' aangeeft dat een burger voor een digitale transactie geen DigiD app hoeft te gebruiken, dan moet de burger direct weten dat dit geen overheidswebsite is.
- De adoptiegraad, het aandeel mensen dat gebruik maakt, van de DigiD app dient hoog te zijn.

Om aan deze randvoorwaarden te voldoen, is naar verwachting nog een forse inspanning van de overheid nodig. Het beleid is echter al ingezet, daarmee zal deze inspanning nagenoeg onvermijdelijk zijn. Een aandachtspunt blijft dat het man-in-the-middle probleem[xi] met de DigiD app niet wordt opgelost.

3.4 Conclusie

Als gevolg van het op termijn alleen nog maar toegankelijk maken van transacties middels de DigiD app (met 2-factorauthenticatie) neemt een zeer substantieel deel van de problemen in de toekomst autonoom af. Deze geschetste ontwikkeling zorgt voor een oplossing voor de eerder geïdentificeerde maatschappelijke problemen 'verlies van identiteit, gegevens of euro's', 'Overheidsdienstverlening wordt niet of later geleverd' en 'links naar (vervalste) transacties'. De overige geïdentificeerde problemen blijven zonder specifiek aanvullend beleid naar verwachting wel bestaan.

4 Oplossingsrichtingen

Op basis van literatuurstudie, wikken en wegensessies[xii] en verdiepende interviews zijn er vier mogelijke oplossingsrichtingen gedefinieerd: Uniformeren domeinnaamextensies, een register van overheidsdomeinnamen, een afsprakenstelsel en uniformeren notificatie. In dit hoofdstuk worden deze nader beschreven.

4.1 Uniforme domeinnaamextensies

De gedachte achter een uniforme domeinnaamextensie voor overheden is dat burgers, die digitaal contact hebben met een overheid, aan de extensie van een website en e-mailadres kunnen herkennen dat ze te maken hebben met een officiële overheidsinstantie. Hierdoor kunnen burgers beter beoordelen of de informatie, vermeld op websites of in e-mails, betrouwbaar is.

Deze oplossingsrichting bestaat uit het uniformeren van alle overheidsdomeinnamen op secondleveldomein (SLD) niveau[xiii]. Hierbij gaat het om het introduceren van een domeinnaamextensie vergelijkbaar met een domeinnaamextensie zoals in het Verenigd Koninkrijk wordt gehanteerd (**.gov.uk)*[xiv]. Alle overheidswebsites en e-mailadressen krijgen dezelfde extensie, bijvoorbeeld **.overheid.nl*. De inrichtingsvorm betreft het 'DNS- concept'[xv]. Hierdoor hoeven overheidsorganisaties hun domeinnaam niet te migreren naar een centraal platform.

Het uniforme domeinnaambeleid is beschikbaar voor alle overheden (lokaal en nationaal). Een overgangsperiode van verschillende jaren, waarin meerdere situaties naast elkaar bestaan, zal bijna onvermijdelijk zijn. Zeker wanneer meerdere overheidsorganisaties deelnemen en dit op vrijwillige basis plaatsvindt. Hierbij zullen deze organisaties wel geactiveerd moeten worden door middel van (communicatie)campagnes en ondersteuning.

4.2 Register van overheidsdomeinnamen

Deze oplossing betreft één centraal digitaal register waarin alle officiële overheidswebsites worden gepubliceerd. Bij twijfel of een website een overheidswebsite is of niet, kan een burger dit register raadplegen, waarin alle officiële overheidswebsites zijn gepubliceerd. Dit register zal uiteraard constant geactualiseerd moeten worden.

Burgers kunnen een website verifiëren door deze in bijvoorbeeld een zoekfunctie in het register op te zoeken en/of als add-on te installeren in een browser. In het tweede geval wordt bij het bezoeken van een website die geregistreerd staat als officiële overheidswebsite een waarborg gegeven dat dit het geval is.

4.3 Een afsprakenstelsel, één of enkele herkenbare en vertrouwde centrale platformen

Het voor burgers en bedrijven beperken van alle digitale informatie en procedures van de overheid tot één of enkele herkenbare en vertrouwde centrale platformen. Voorbeelden hiervan zijn MijnOverheid[xvi] en MedMij[xvii]. Deze platformen bieden de mogelijkheid om (na inlog met DigiD) transacties te doen en persoonlijke informatie in te zien. Uitgangspunt hierbij is dat burgers en

bedrijven generieke informatie anoniem in moeten kunnen zien, dus ook voorafgaand aan een eventuele inlog met DigiD.

Om het mogelijk te maken dat meerdere overheidsorganisaties deelnemen aan een centraal platform is een helder afsprakenstelsel noodzakelijk. Een helder afsprakenstelsel draagt eraan bij dat gevoelige en vertrouwelijke gegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen burgers of bedrijven en de verschillende overheidsorganisaties. Deze uitwisseling vindt plaats in twee richtingen; burgers en bedrijven kunnen gegevens verzamelen en delen. In een dergelijk afsprakenstelsel worden afspraken gemaakt op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat burgers, bedrijven en overheidsorganisaties op een veilige manier gegevens kunnen uitwisselen.

4.4 Uniformeren notificatie, collectieve communicatieafspraken

Collectieve communicatieafspraken over de wijze waarop overheidsorganisaties communiceren met burgers en bedrijven, en deze afspraken eenvoudig en begrijpelijk uitleggen aan alle burgers en bedrijven. Een dergelijke oplossingsrichting is voornamelijk gericht op berichtenverkeer (zoals e-mail, sms, whatsapp, etc.) en in mindere mate op websites.

Dergelijke afspraken kunnen bijvoorbeeld bestaan uit de keuze om alle communicatie vanuit overheidsorganisaties uitsluitend via MijnOverheid te laten verlopen en/of dat overheidsorganisaties nooit links te laten opnemen in berichten. Hiervoor zijn dwingende afspraken noodzakelijk, zoals dat alle overheden volledig stoppen met links in alle berichten en/of volledig stoppen met communicatie in e-mails, sms, whatsapp, etc.

4.5 Overkoepelend

Voor elke oplossingsrichting is flankerend beleid aan te bevelen om daadwerkelijk effectief te zijn. Zo geldt dat een actief, helder en goed afgestemd domeinnaambeleid[xviii], bedoeld om het aantal actief gebruikte overheidsdomeinnamen te beperken en de gebruikte domeinnamen maximaal te benutten, bijdraagt aan de overzichtelijkheid en daarmee de efficiency van iedere oplossingsrichting. Ook een helder en breed communicatiebeleid draagt bij aan het bereik en daarmee de effectiviteit van iedere oplossingsrichting. Deze inspanningen zijn in dit onderzoek als randvoorwaarde aangenomen.

4.6 Conclusie

Voor dit onderzoek zijn vier (deel)oplossingsrichtingen voor de problemen geïdentificeerd: een uniforme domeinnaamextensie, register van overheidsdomeinnamen, afsprakenstelsels/herkenbare en vertrouwde centrale platformen en collectieve communicatieafspraken. Deze oplossingsrichtingen kunnen in samenhang worden gezien, ze vullen elkaar deels aan en sluiten elkaar niet uit. In deze Quickscan analyse beschouwen we de effecten echter apart per oplossingsrichting.

5 Effecten

In dit hoofdstuk wordt beschreven of en in hoeverre de oplossingsrichtingen bijdragen aan de oplossing van de geschetste problemen. In de tabel aan het einde van dit hoofdstuk zijn de oplossingsrichtingen en de problemen tegen elkaar afgezet. Hieronder wordt per probleem toegelicht of en in hoeverre deze wordt opgelost door de oplossingsrichtingen dan wel ontwikkelingen in het nulalternatief. Eerst wordt de informatie-kant behandeld, vervolgens de transactie-kant.

5.1 Informatie: Burger denkt authentiek, website/e-mail is vervalst

Link naar transacties
Doordat dit probleem al voor een groot deel wordt opgelost in het nulalternatief, wordt niet behandeld of en in hoeverre de oplossingsrichtingen bijdragen aan het oplossen van het probleem.

Verspreiding van onjuiste informatie
Bij uniforme overheidsdomeinnamen kan een gebruiker herkennen of een website van de overheid is of niet. Meer duidelijkheid over de afzender van informatie helpt de gebruiker bij zijn/haar inschatting van de juistheid en betrouwbaarheid van informatie.[xix] Deze oplossingsrichting draagt naar verwachting bij aan het terugdringen van de verspreiding van onjuiste informatie.

Een register voor overheidsdomeinnamen draagt naar verwachting beperkt bij aan het verspreiden van onjuiste informatie. Enkel op het moment dat een gebruiker twijfelt, zal hij/zij het register raadplegen. Wanneer een gebruiker niet twijfelt zal deze het register waarschijnlijk niet raadplegen en daardoor niet te weten komen dat de informatie niet wordt aangeboden door een overheidsorganisatie. Een add-on van het register in de browser van de gebruiker zal naar verwachting wel bijdragen. De mate waarin zal echter sterk afhankelijk zijn van hoeveel gebruikers de add-on toepassen. In de praktijk blijkt het erg lastig een breed publiek te bereiken met dergelijke oplossingen. Mogelijk zal de impact hiervan daarom beperkt zijn.

Bij één of enkele herkenbare en vertrouwde centrale overheidsplatformen is het voor de gebruiker eenvoudig om bekend te raken met deze betrouwbare overheidswebsites. Door het voorkomen van een veelheid aan onbekende en onherkenbare overheidsplatformen en -websites, kan deze oplossingsrichting bijdragen aan het terugdringen van de verspreiding van onjuiste informatie.

Uniformering van notificaties en collectieve communicatieafspraken zijn voornamelijk gericht op berichten en minder op informatie via websites. De impact hiervan op de verspreiding van onjuiste informatie zal daarom naar verwachting beperkt blijven.

5.2 Informatie: Burger denkt vervalst, website/e-mail is authentiek

Extra tijd voor gebruiker ter controle
Bij uniforme overheidsdomeinnamen kan een gebruiker bij twijfel in theorie in een oogopslag controleren of de afzender een (erkende) overheidsorganisatie betreft. In het geval van een register zal de gebruiker wel zelf een handeling moeten verrichten om de website te controleren. In dat geval blijft er wel altijd een beperkte inspanning in tijd benodigd. Een add-on kan deze tijdsbesparing nog verder terugdringen.

Bij één of enkele herkenbare en vertrouwde centrale overheidsplatformen is het voor de gebruiker eenvoudig om bekend te raken met deze betrouwbare overheidswebsites. Door het voorkomen van een veelheid aan onbekende en onherkenbare overheidsplatformen en -websites, kan deze oplossingsrichting bijdragen aan het terugdringen van extra tijd voor controle.

Zowel een uniforme domeinnaam, een register als één of enkele herkenbare en vertrouwde centrale overheidsplatformen zullen daarnaast ook effectiever zijn dan de huidige controle door gebruikers. Uit het publieksonderzoek van het ministerie van BZK blijkt namelijk dat gebruikers slecht in staat zijn om echte websites van overheidsdiensten te herkennen en onechte websites te ontmaskeren. Communicatie en uitleg vooraf bleek hierbij weinig impact te hebben. Een uniforme domeinnaam of register kan dit probleem verhelpen.

Uniformering van notificaties en collectieve communicatieafspraken is voornamelijk gericht op de inhoud van berichten en minder op informatie via websites. Uit het publieksonderzoek bleek dat communicatie en uitleg vooraf weinig impact te hebben. De impact van het uniformeren van notificaties en collectieve communicatieafspraken op de controletijd voor de gebruiker, zal daarom naar verwachting beperkt blijven.

5.3 Transactie: Burger denkt authentiek, website/e-mail is vervalst

Doordat de problemen hiermee voor een groot deel al worden opgelost in het nulalternatief wordt niet behandeld of en in hoeverre de oplossingsrichtingen bijdragen aan het oplossen van het probleem.

5.4 Transacties: Burger denkt vervalst, website/e-mail is authentiek

Extra tijd voor gebruiker ter controle
De effecten van de verschillende oplossingsrichtingen op ‘extra tijd voor de gebruiker ter controle’ is voor transacties hetzelfde als omschreven in paragraaf 5.2.

Afzien van het gebruik maken van (digitale) diensten, meer analoge transacties
Bij uniforme overheidsdomeinnamen herkent een burger overheidswebsites beter. Hierdoor krijgen burgers naar verwachting meer vertrouwen en zullen ze minder snel afhaken bij de aanvraag/gebruik van digitale dienstverlening. Burgers zullen digitaal zelfredzamer worden en minder vaak een beroep doen op de analoge tegenhangers.

Hetzelfde geldt naar verwachting voor één of enkele herkenbare en vertrouwde centrale overheidsplatformen en het register, zij het in mindere mate omdat de burger zelf actie moet ondernemen. Deze drempel kan ervoor zorgen dat een deel alsnog afhaakt.

Uniformering van notificaties en collectieve communicatieafspraken is voornamelijk gericht op de inhoud van berichten. Indien een overheidsorganisatie in communicatie op uniforme en herkenbare wijze verzoekt een bepaalde digitale dienst te doorlopen, zou dit kunnen helpen. Deze oplossingsrichting heeft, doordat het is gericht op de inhoud van berichten, echter geen invloed op twijfel bij gebruikers over de authenticiteit van websites. De impact van het uniformeren van notificaties en collectieve communicatieafspraken zullen daarom naar verwachting beperkte impact hebben op het afzien van de digitale diensten.

5.5 Maatschappelijke effecten

Zoals volgt uit de voorgaande paragrafen leiden oplossingsrichtingen mogelijk tot het voorkomen van extra tijdbesteding door gebruikers voor de controle van de authenticiteit van websites en e-mails. De omvang hiervan lijkt beperkt, aangezien de meeste gebruikers hier naar verwachting niet veel meer dan enkele minuten aan besteden. Bij grote aantallen mails, aanvragen voor digitale dienstverlening of bezoeken aan informatiewebsites kan dit echter snel oplopen. Nader onderzoek naar de omvang hoe vaak dit plaatsvindt is hier echter voor benodigd.

Deze bevindingen sluiten aan bij bevindingen uit andere landen.[xx] Hierbij zijn de volgende beweegredenen geïdentificeerd: herkenbaarheid, vindbaarheid, betrouwbaarheid, veiligheid en beheerbaarheid. Uit het onderzoek is echter in kwantitatieve, noch kwalitatieve zin vast te stellen of een overheidsbreed domeinnaambeleid hieraan bijdraagt. Geen van de geraadpleegde buitenlandse overheden heeft een evaluatie hiernaar uitgevoerd.

- draagt niet bij aan
- draagt enigzins bij aan
- draagt bij aan
- probleem wordt al opgelost in nulalternatief

	Informatie						Transactie					
	Burger denkt authentiek + Website/mail is vervalst		Burger denkt vervalst + Website/mail is authentiek				Burger denkt authentiek + Website/mail is vervalst		Burger denkt vervalst + Website/mail is authentiek			
	Onjuiste informatie	Link naar transacties	Tijd checken	Meer analoge transaties	Niet gebruik diensten	Twijfel burger	Verlies ID, € of gegevens	Dienst niet of later	Tijd checken	Meer analoge transaties	Niet gebruik diensten	Twijfel burger
Nulalternatief: doorontwikkeling DigiD (incl. communicatie)	●	●	●	●	●	●	●	●	●	●	●	●
Uniforme domeinnaam	●	●	●	●	●	●	●	●	●	●	●	●
Platform / afsprakenstelsel	●	●	●	●	●	●	●	●	●	●	●	●
Uniformeren notificatie	●	●	●	●	●	●	●	●	●	●	●	●
Register domeinnamen	●	●	●	●	●	●	●	●	●	●	●	●

Tijdens verschillende gevoerde gesprekken zijn over iedere oplossingsrichting ook twijfels geuit. Vooruitlopend op een conclusie benadrukken we dat er niet één breed gedragen oplossingsrichting is die alle problemen oplost en (de keuze voor) een definitieve oplossing nog veel inspanning vraagt.

5.6 Conclusie

Alle oplossingsrichtingen hebben een beperkte invloed op de problemen. Een goed overzicht van effecten vraagt om nader onderzoek naar de omvang van (huidige) problemen en de oplossingsrichting. Een uniforme overheidsdomeinnaam heeft mogelijk het grootste effect op de herkenbaarheid van de digitale overheid. Een register, centraal platform en collectieve communicatieafspraken zijn (deel)oplossingen die een deel van de problemen aanpakken.

6 Kostenindicaties

In dit hoofdstuk is op basis van een expertoordeel van de onderzoekers kwalitatief invulling geven aan kostenindicaties van de geïdentificeerde oplossingsrichtingen voor een herkenbare en betrouwbare digitale overheid.

6.1 Kostenindicaties

De kosten voor een uniforme domeinnaam zullen snel oplopen naar forse investeringen. Overheidsorganisaties moeten verschillende technische aanpassingen doorvoeren, zoals het aanpassen van de certificaten, re-directs van e-mailadressen. Ook moet worden geïnvesteerd in het installeren en testen van deze certificaten in de architectuur en bij leveranciers en ketenpartners. Daarnaast moet worden geïnvesteerd in communicatie rond de nieuwe domeinnamen en e-mailadressen naar burgers, ondernemers en betrokken ketenpartners en moeten communicatie-uitingen worden aangepast. Ook worden e-mailadressen gebruikt als gebruikersnaam om in te loggen op verschillende plekken, een aanpassing daarvan zal ook kosten met zich meebrengen.

Ten behoeve van een register van overheidsdomeinnamen en het uniformeren van de notificatie kan gebruik worden gemaakt van bestaande bouwstenen, zoals de Staatsalmanak[xxi] en ‘Uitgangspunten overheidscommunicatie’ of ‘Handreiking online communicatie rijksambtenaren’. Hierbij moet rekening worden gehouden met het maken van heldere afspraken met alle overheidsorganisaties, continue actualisatie en het communiceren over de oplossing, zodat deze ook effectief zijn.

Het opzetten van één of enkele herkenbare en vertrouwde centrale platformen kan voortborduren op bestaande platformen zoals MijnOverheid en MedMij. Hiervan zijn de initiële investeringen al gedaan. Additionele kosten kunnen echter nog omvangrijk zijn. Nader onderzoek naar wat additioneel benodigd is en de kostenomvang hiervan is hier echter benodigd voor een inschatting.

In volgend schema is op basis van een expertoordeel door de onderzoekers een kostenindicatie per kostensoort gegeven van de verschillende oplossingsrichtingen. Dit is een eerste voorzichtige indicatie in ordegroottes. Voor een goede kostenraming vraag de architectuur van oplossingsrichtingen nadere uitwerking.

+ = enkele tonnen *++ = enkele miljoenen* *+++ = enkele tientallen miljoenen*	Wet- en regelgeving	Afsprakenkader	Infrastructurele aanpassingen (IT)	Governance/ organisatorisch	Communicatie/ campagne	Totaal
Uniforme domeinnaamextensies	+	+	+++	++	++/+++	**+++**
Register van overheidsdomeinnamen	+	+	+	+/++	++	**+/++**
Afsprakenstelsel	+	++	++/+++	++	++	**++/+++**
Uniformeren notificatie	+	+	+/++	++	++	**++**

6.2 Conclusie

Alle oplossingsrichtingen zullen significante investeringen met zich meebrengen. Een uniforme domeinnaamextensie lijkt de meeste inspanning en investering van overheidsorganisaties te vragen. De overige oplossingsrichtingen borduren voort op deels bestaande oplossingen en vragen daardoor mogelijk om minder inspanning en investeringen, waarbij een register van overheidsdomeinnamen, afhankelijk van keuzes voor inrichting en organisatie, relatief lagere inspanning en investeringen vraagt van overheidsorganisaties.

7 Conclusies

In dit onderzoek is een Quickscan verkenning uitgevoerd naar de maatschappelijke effecten van verschillende oplossingsrichtingen voor een herkenbare en betrouwbare digitale overheid (voor websites en e-mails). De belangrijkste besproken bevindingen en conclusies zijn in dit hoofdstuk samengevat.

In dit onderzoek zijn we nader ingegaan op de gevolgen die ontstaan wanneer een authentieke website of e-mail van de overheid onvoldoende herkenbaar is als betrouwbare bron of onbetrouwbare bronnen digitaal verkeer van de overheid vervalsen. Dit leidt mogelijk tot verspreiding van onjuiste informatie, extra tijdsbesteding van gebruikers van digitale overheidsdiensten en -informatie, het afzien van of later gebruik van digitale overheidsdiensten en eventueel verlies van persoonlijke of zelfs identiteitsgegevens of geld.

Na de inwerkingtreding van de Wet digitale overheid zijn transacties op overheidswebsites op termijn alleen bereikbaar na inloggen met de DigiD app (met 2-factorauthenticatie op betrouwbaarheidsniveau substantieel of hoog). Hierdoor wordt een deel van de problemen in de toekomst autonoom verholpen. Deze geschetste ontwikkeling zorgt voor een oplossing voor de eerder geïdentificeerde maatschappelijke problemen ‘verlies van identiteit, gegevens of euro’s’, ‘Overheidsdienstverlening wordt niet of later geleverd’ en ‘links naar (vervalste) transacties’. De overige geïdentificeerde problemen worden hierdoor zonder specifiek aanvullend beleid niet opgelost.

Voor dit onderzoek zijn vier (deel)oplossingsrichtingen voor de problemen geïdentificeerd: een uniforme domeinnaamextensie, register van overheidsdomeinnamen, herkenbare en vertrouwde centrale platformen en collectieve communicatieafspraken. Deze oplossingsrichtingen kunnen in samenhang worden gezien, ze vullen elkaar deels aan en sluiten elkaar niet uit. In deze Quickscan analyse beschouwen we de effecten echter apart per oplossingsrichting. Tijdens verschillende gevoerde gesprekken zijn over iedere oplossingsrichting ook twijfels geuit. Vooruitlopend op een conclusie moet worden benadrukt dat er niet één breed gedragen oplossingsrichting is die alle problemen oplost en (de keuze voor) een definitieve oplossing zal nog veel inspanning vragen.

Een goed overzicht van maatschappelijke kosten en baten vraagt om meer nader onderzoek naar de omvang van (huidige) problemen en de kosten van oplossingsrichting.

Alle oplossingsrichtingen hebben een beperkte invloed op de problemen. Een uniforme overheidsdomeinnaam heeft mogelijk het grootste effect op herkenbaarheid van de digitale overheid. Een register, centraal platform en collectieve communicatieafspraken zijn (deel)oplossingen die een deel van de problemen aanpakken.

Alle oplossingsrichtingen zullen significante investeringen met zich meebrengen. Een uniforme domeinnaamextensie lijkt de meeste inspanning en investering van overheidsorganisaties te vragen. De overige oplossingsrichtingen borduren voort op deels bestaande oplossingen en vragen daardoor mogelijk om minder inspanning en investeringen. Een register van overheidsdomeinnamen, afhankelijk van keuzes voor inrichting en organisatie, vraagt een relatief lagere inspanning en investeringen van overheidsorganisaties.

Eindnoten

[i] Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid, Kantar Public, januari 2019

[ii] Bekende voorbeelden zijn *.*gov.uk* (Verenigd Koninkrijk) en *.*gov* (Verenigde Staten), zie ook 'Buitenlandonderzoek Domeinnaambeleid' (PBLQ november 2019)

[iii] Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen, Raad van State, 31 augustus 2018

[iv] Cybersecuritybeeld Nederland 2019, Nationaal Cyber Security Centrum

[v] Algemene leidraad voor maatschappelijke kosten-batenanalyse, CPB & PBL (2013)

[vi] Werkwijzer voor maatschappelijke kosten-batenanalyse van de digitale overheid, SEO, Ecorys & Van Zutphen Economisch Advies (2019)

[vii] Dit wetsvoorstel is op 18 februari 2020 aangenomen door de Tweede Kamer en ligt op dit moment in de Eerste Kamer

[viii] Impactanalyse Uniforme Domeinnaam extensie, VNG november 2019

[ix] Zie https://www.forumstandaardisatie.nl/open-standaarden/lijst voor meer informatie

[x] Geschat wordt dat de theoretische dekkingsgraad (hoeveel mensen kunnen hiervan gebruikmaken), momenteel circa 65% van de burgers bedraagt. (Voortgangsrapportage Digitale toegang, september 2019).

[xi] Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Daarvoor bestaan overigens andere oplossingen.

[xii] https://www.crow.nl/wikken-en-wegen/methode

[xiii] In de Domain Name System- of DNS-structuur staat een secondleveldomein (SLD) onder die van het topleveldomein (TLD).

[xiv] In het voorbeeld van het VK is ervoor gekozen om bedrijven het domeinnaam *.*co.uk* te laten hanteren, universiteiten *.*ac.uk* en overige organisaties *.*org.uk*. Dit geldt niet voor de oplossingsrichting zoals beschreven in dit document.

[xv] PBLQ (2019). Buitenlandonderzoek Domeinnaambeleid.

[xvi] https://mijn.overheid.nl/

[xvii] https://www.medmij.nl/

[xviii] Voor vrijwel ieder nieuw initiatief wordt een nieuwe domeinnaam aangevraagd (recente voorbeelden: https://www.databronnencovid19.nl/ en https://www.bijzonderebijstandbuitenland.nl/)

[xix] Hiervoor is het belangrijk dat het gebruik van uniforme domeinnaam gemeengoed wordt. Als dit niet het geval is, en maar een (klein) deel van de overheidswebsites gebruik maakt van de uniforme domeinnaam, dan is deze inschatting niet te maken. Tevens moet dit bekend zijn bij burgers.

[xx] 'Buitenlandonderzoek Domeinnaambeleid' (PBLQ november 2019)

[xxi] https://almanak.overheid.nl/