Rapport impactanalyse uniforme domeinnaamextensie

Versie: Definitief



Ministerie van Binnenlandse zaken en Koninkrijksrelaties
April 2026

Managementsamenvatting

Achtergrond en aanleiding

Jaarlijks worden naar schatting (tien)duizenden Nederlanders gedupeerd door organisaties die lijken op de overheid, maar het niet zijn.[1] Er bestaat behoefte aan verbetering van de herkenbaarheid van de digitale overheid, zodat meer zekerheid ontstaat over de echtheid (het afzenderschap) van overheidsinformatie en dienstverlening.

Een maatregel die de herkenbaarheid van websites helpt verbeteren is de invoering van een uniforme domeinnaamextensie, zoals *.gov.nl* of *.overheid.nl*. In 2023 is hiervoor op basis van veiligheidsoverwegingen en internationale best practices een principebesluit genomen, met *.gov.nl* als voorkeursrichting. Conform toezegging aan de Kamer is een impactanalyse naar de haalbaarheid en betaalbaarheid uitgevoerd. In de impactanalyse is *.overheid.nl* als alternatief meegenomen. Dit omdat een (beperkt) deel van de Rijksoverheidswebsites deze extensie al hanteert, uit publieksonderzoek blijkt dat het publiek een intuïtieve voorkeur heeft voor deze extensie én nog altijd geen definitief besluit voor een variant is genomen.

Invoering van een uniforme domeinnaamextensie raakt aan het bredere vraagstuk van digitale soevereiniteit. Door het publieke digitale gezicht van de overheid onder één herkenbare en centraal geregisseerd stelsel te organiseren, ontstaat meer grip op een belangrijk deel van de digitale basisinfrastructuur en kunnen eisen aan beheer, veiligheid en continuïteit meer robuust worden ingericht.

Tijdens het wetgevingsoverleg van 2 maart 2026 heeft de Tweede Kamer verzocht om voor het zomerreces een plan van aanpak inclusief tijdpad over het overgaan van overheidssites naar één domeinnaamextensie te ontvangen. In dat debat is toegezegd de impactanalyse inclusief een realistisch plan van aanpak en een tijdsplanning op hoofdlijnen vóór het meireces toe te sturen aan de Tweede Kamer.

Aanpak

De analyse is afgebakend tot een eerste invoeringsfase alleen gericht op de publiek toegankelijke domeinen (websites, applicaties) van departementen en uitvoerders binnen de Rijksdienst.

De impactanalyse is gebaseerd op eerder uitgevoerd onderzoek, aangevuld met verdiepingssessies met relevante stakeholders en een externe (hoogover) financiële doorrekening. Daarbij is gekeken naar de gevolgen voor organisatie, techniek, financiën en communicatie, alsook governance en beheer. Daarnaast zijn twee implementatiescenario's uitgewerkt, inclusief een planning op hoofdlijnen en een eerste aanzet voor een communicatiestrategie.

[1] Het gaat hier om commerciële organisaties die bijvoorbeeld diensten aanbieden die de overheid ook levert of bemiddelen voor overheidsdiensten en daar extra kosten voor rekenen. Denk aan kadaster gegevens, het regelen van toeslagen en subsidies, tenaamstellingen van auto's, etc.

Hoofdbevindingen

Een uniforme domeinnaamextensie draagt bij aan grotere herkenbaarheid, meer consistentie en meer grip op het digitale domeinlandschap van de (Rijks)overheid. Meerwaarde ontstaat niet door de extensie alleen, maar in samenhang met heldere governance, centrale regie, eenduidige spelregels, een actueel internetdomeinregister en een beheerste invoering.

De organisatorische impact is aanzienlijk. Het huidige domeinlandschap is versnipperd en kent verschillende beheersituaties, waardoor uniforme naamgeving, centrale sturing en structurele opschoning in de huidige situatie beperkt afdwingbaar zijn. Invoering vraagt daarom om duidelijke kaders voor beleid, uitgifte, beheer, uitzonderingen en toezicht.

Ook op het punt van governance en beheer is sprake van een wezenlijke opgave. Voor een nieuwe situatie ligt een model voor de hand waarin beleid, naamgeving, toelatingscriteria en toezicht centraler worden ingericht, met ruimte voor gedelegeerde uitvoering waar dat nodig is. Het rapport benoemt governance en beheer dan ook expliciet als randvoorwaarde voor een gecontroleerde, veilige en uitvoerbare invoering.

Technisch is invoering haalbaar, maar de impact reikt verder dan alleen de domeinnaam zelf. Onder meer koppelingen, redirects, certificaten, vindbaarheid en afhankelijkheden met andere systemen vragen aandacht. In de vergelijking tussen *.gov.nl* en *.overheid.nl* is het technische verschil beperkt, maar *.gov.nl* ligt meer voor de hand vanuit (internationale) standaardisatie en veiligheidsoverwegingen.

Communicatie is een bepalende randvoorwaarde. De maatschappelijke meerwaarde van een uniforme extensie zit immers in betere herkenbaarheid voor burgers en ondernemers. Die herkenbaarheid ontstaat alleen wanneer de betekenis van de extensie ook daadwerkelijk duidelijk is. Tegelijkertijd is de overgangsperiode kwetsbaar, omdat oude en nieuwe domeinen tijdelijk naast elkaar kunnen bestaan. Duidelijke publiekscommunicatie, centrale bewegwijzering en een actueel overzicht van officiële domeinen zijn daarom noodzakelijk.

Financieel is sprake van een meerjarige opgave. Naast investeringen in governance, ondersteuning, migratie en communicatie is de impact op het bestaande webportfolio bepalend voor de uiteindelijke kosten. Op basis van de kostenraming van Berenschot bedraagt de verwachte eenmalige investering voor de migratie van het huidige webportfolio binnen scope ongeveer € 49,6 miljoen, met een bandbreedte tussen de € 40,1 miljoen en € 59,2 miljoen. Daarnaast worden structurele governancekosten geraamd op ongeveer € 2 miljoen per jaar. Tegelijk laat het rapport zien dat de financiële impact sterk kan afnemen wanneer invoering wordt gecombineerd met sanering van het webportfolio. Omvang en spreiding van de kosten hangen direct samen met het gekozen scenario en de bijbehorende doorlooptijd.

Scenario's

De analyse werkt twee implementatiescenario's uit. Het eerste scenario, *burger en ondernemer centraal*, geeft prioriteit aan de centrale aanlandplek en aan snelle zichtbaarheid voor burgers. In dit scenario bedraagt de doorlooptijd maximaal vijf jaar. Het tweede scenario, *bedrijfsvoering centraal*, kiest voor een meer geleidelijke invoering, met een gefaseerde omzetting van eenvoudige naar meer complexe websites en een doorlooptijd van vijf tot maximaal tien jaar. Het eerste scenario biedt sneller zichtbare publiekswaarde; het tweede scenario is vanuit uitvoerbaarheid en beheersbaarheid meer

geleidelijk van aard. Financieel laat scenario 1 sneller rendement zien: de terugverdientijd wordt geraamd op ongeveer twee tot drie jaar binnen een looptijd van vijf jaar. Voor scenario 2 wordt de terugverdientijd geraamd op ongeveer drie tot vijf jaar binnen een looptijd van tien jaar.

Conclusie en advies

Invoering van een uniforme domeinnaamextensie is haalbaar en inhoudelijk verdedigbaar, mits deze gefaseerd wordt ingevoerd en wordt ondersteund door heldere governance, duidelijke randvoorwaarden en een gerichte communicatieaanpak. Op basis van de analyse ligt het voor de hand om vast te houden aan *.gov.nl* als voorkeursrichting en de verdere besluitvorming daarop te richten. Daarbij is een programma-aanpak aangewezen, met een bestuurlijke keuze voor het gewenste tempo van invoering: een korter, meer publieksgericht traject van maximaal vijf jaar of een meer geleidelijke invoering in vijf tot tien jaar.

Inhoud

1 Achtergrond en aanleiding 7
1.1 Digitale soevereiniteit 8
2 Opzet impactanalyse 9
2.1 Projectbegrenzing 9
2.1.1 Binnen scope 9
2.1.2 Buiten scope 10
2.1.3 Beoogd resultaat 10
2.2 Aanpak 10
3 Uitkomsten impactanalyse 11
3.1 Desk onderzoek 11
3.1.1 Burger -en ondernemersperspectief 11
3.1.2 Extensie als deeloplossing 12
3.1.3 Aandachtspunten eerder onderzoek 12
3.1.4 Samenvattend 13
4 Impact op organisatie, techniek, financiën, communicatie en governance 13
4.1 Organisatie 13
4.1.1 Organisatie .gov.nl versus .overheid.nl 15
4.1.2 Samenvattend 15
4.2 Techniek 15
4.2.1 DNS-inrichting en robuustheid 16
4.2.2 Certificaten 16
4.2.3 Redirects, SEO en permalinks 17
4.2.4 (Functionele) E-mail (techniek en architectuur) 17
4.2.5 Technische aansluitvoorwaarden 18
4.2.6 Techniek *.gov.nl versus *.overheid.nl 19
4.2.7 Samenvattend 19
4.3 Financiën 19
4.3.1 Huidige situatie (nulsituatie) 20
4.3.2 Incidentele kosten 20
4.3.3 Saneringspotentieel webportfolio Rijksdienst 21
4.3.4 Governance kosten (incidenteel -en structureel) 23
4.3.5 Kansen voor structurele kostenbesparingen 24
4.3.6 Kosten *.gov.nl versus *.overheid.nl 25
4.3.7 Samenvattend 25
4.4 Communicatie 25

4.4.1 Publiekscommunicatie / campagne 27
4.4.2 Behoud van vindbaarheid in zoekmachines bij invoering van een nieuwe extensie 27
4.4.3 AI training en verificatie 28
4.4.4 Communicatie *.gov.nl versus *.overheid.nl 28
4.4.5 Samenvattend 29
4.5 Governance en beheer 29
4.5.1 Omvang en versnippering van het domeinportfolio 29
4.5.2 Rol van DPC en het huidige domeinnaambeleid 29
4.5.3 Decentraal DNS-beheer bij departementen, uitvoerders en leveranciers 30
4.5.4 Governance-niveaus: strategisch, tactisch en operationeel 31
4.5.5 PRO als gedeeltelijk gecentraliseerde platformvoorziening 31
4.5.6 Centraal uitgiftepunt, gedelegeerd DNS model 32
4.5.7 Aanvraag en uitgifteproces 32
4.5.8 Naamgeving, defensieve registraties en overgangsafspraken 33
4.5.9 Veiligheid 33
4.5.10 Governance *.gov.nl versus *.overheid.nl 34
4.5.11 Samenvattend 34
5 Implementatiescenario's 35
5.1 Scenario 1: Burger en ondernemer centraal (centrale aanlandplek krijgt voorrang + beperkte doorlooptijd) 35
5.1.1 Fasering / uitgangspunten 36
5.1.2 Financiële impact en terugverdientijd 37
5.1.3 Planning scenario 1 39
5.2 Scenario 2: Bedrijfsvoering centraal (klein beginnen, langere doorlooptijd) 40
5.2.1 Fasering / uitgangspunten 40
5.2.2 Financiële impact en terugverdientijd 42
5.2.3 Planning scenario 2 43
5.3 Doorkijk en bredere uitrol 44
5.4 Samenvattend 44
6 Aandachtspunten en risico's 45
6.1 Aandachtspunten 45
6.2 Risico's 45
7 Aanbevelingen 46
8 Bijlagen 48
8.1 Bijlage: Uitgangspunten en randvoorwaarden impactanalyse 48
8.2 Bijlage: Raakvlakken 50

8.3 Bijlage: Input communicatiestrategie uniforme domeinnaamextensie 51
8.4 Bijlage: Overzicht Rijksdienst – uitvoerders per departement 55
8.5 Bijlage: Samenvatting buitenlandonderzoek 56
8.6 Bijlage: Verdiepingssessies en gesprekken 59
8.7 Bijlage: Bronnenlijst 60

1 Achtergrond en aanleiding

Jaarlijks worden (tien)duizenden Nederlanders[2] gedupeerd door gebruik te maken van informatie en diensten die van de overheid afkomstig lijken, maar dat niet zijn. Enerzijds gaat het om websites van organisaties die qua look en feel een sterke gelijkenis vertonen met de overheid en die bijvoorbeeld tegen hogere kosten bemiddelen in overheidsdiensten.[3] Anderzijds zijn er overduidelijk kwaadwillende partijen die zich voordoen als overheid in de hoop geld of gevoelige gegevens in handen te krijgen. Een recent voorbeeld zijn de vele nepmails, zogenaamd van het CJIB, die hoogstwaarschijnlijk gerelateerd kunnen worden aan de recente hack van internetprovider Odido.[4] In dit kader worden regelmatig imitatiewebsites van bestaande Rijksoverheidsorganisaties gedetecteerd en uit de lucht gehaald.[5] Incidenteel worden ook websites van niet bestaande Rijksoverheidsorganisaties gedetecteerd en uit de lucht gehaald.[6] Uit publieksonderzoek blijkt dat behoefte bestaat aan verbetering van de herkenbaarheid van de digitale overheid, zodat meer zekerheid ontstaat over de echtheid (het afzenderschap) van overheidsinformatie en dienstverlening.[7]

Vanuit de ministeries van BZK, AZ (communicatie) en diverse Rijksdiensten wordt onderzocht hoe de herkenbaarheid van de digitale overheid richting burgers en ondernemers kan worden verbeterd. Eén maatregel die veel landen in Europa hebben ingevoerd is een uniforme domeinnaamextensie voor (Rijks)overheidswebsites en e-mail. In Nederland zou het kunnen gaan om de standaard toevoeging *.gov.nl of *.overheid.nl aan websites (en op termijn e-mail) van de (Rijks)overheid. Aangezien alleen de overheid deze specifieke standaard toevoeging aan het adres van een website (ook wel domeinnaam genoemd) kan uitgeven, maakt een uniforme domeinnaamextensie aan burgers, ondernemers, zoekmachines en AI-systemen direct duidelijk dat een website (of domeinnaam) afkomstig is van de overheid. [8]

Op dit moment ontbreekt zo'n een uniek, betrouwbaar kenmerk voor overheidswebsites. Domeinnamen zijn vaak onduidelijk of onlogisch opgebouwd, exclusieve overheidscertificaten voor publieke Transport Layer Security (TLS) bestaan niet meer, en

[2] Voorzichtige schatting op basis van fraude en phishingcijfers van het CBS (zie o.a. https://www.cbs.nl/nl-nl/longread/rapportages/2026/veiligheidsmonitor-2025/6-online-criminaliteit) en de Fraudehelpdesk (https://www.fraudehelpdesk.nl/wp-content/uploads/2026/02/Terugblik-2025.pdf).
[3] Dit is een legale praktijk die kan bestaan dankzij de bestaande onduidelijkheid over het afzenderschap van overheidsinformatie- en dienstverlening.
[4] https://nos.nl/artikel/2607755-nepmails-van-cjib-in-omloop-verband-met-odido-hack-aannemelijk
[5] Via de Logodetectiedienst van SIDN wordt het .nl domein op basis van algoritmen gescand op het Rijkslogo. Vervolgens wordt onderzocht of het correct of incorrect gebruik van het Rijkslogo betreft.
[6] Voorbeeld: de gedetecteerde malafide website 'msdr.nl', zogenaamd van de 'Rijksdienst voor seksuele dienstverlening van het Ministerie van seksuele dienstverlening en registratie', bedoeld om de persoonsgegevens van (kwetsbare) sekswerkers in handen te krijgen om deze vervolgens te kunnen chanteren en/of exploiteren. Deze website is uit de lucht gehaald.
[7] Zie onderzoeken [3] Kantar , [10] Centerdata.
[8] Een voorbeeld: bij invoering van bijvoorbeeld .gov.nl als standaard domeinnaamextensie voor de Rijksoverheid, dienen (als eerste fase) alle publieke domeinnamen van de Rijksdienst te eindigen op .gov.nl. Denk aan "rijkswaterstaat.gov.nl" "aerius.gov.nl" "waarderingskamer.gov.nl" "donorregister.gov.nl", etc. Op die manier zijn voortaan ook minder bekende domeinnamen direct herkenbaar als afkomstig van de Rijksoverheid.

herkenningsmiddelen zoals het Rijkslogo (beeldmerk en woordmerk) zijn eenvoudig na te maken. Inmiddels maakt de Rijksoverheid gebruik van de Logodetectiedienst van SIDN om het .nl domein te monitoren op het gebruik van het Rijkslogo. Dit helpt misstanden aan te pakken, maar voorkomt deze niet. Met de opkomst van Artificiële Intelligentie (AI), dat steeds vaker zelfstandig websites interpreteert en doorzoekt én het genereren van nepwebsites steeds makkelijker maakt, neemt het belang van een eenduidige digitale identiteit alleen maar toe. Steeds meer landen, zoals recent (2024) nog Duitsland[9], nemen daarom initiatieven om overheidsdomeinen herkenbaarder en veiliger te maken via uniforme extensies (als betrouwbaar kenmerk in samenhang met bijvoorbeeld een uniform design, huisstijl en beeldmerk). In 2008 heeft de Rijksoverheid met de rijkshuisstijl een uniform design, huisstijl en beeldmerk ingevoerd voor de Rijksdienst. In 2024 is de rijkshuisstijl gemoderniseerd.

In 2023 nam de toenmalige staatssecretaris voor Digitaliseringsbeleid en Koninkrijksrelaties Van Huffelen een principebesluit voor de invoering van *.gov.nl op basis van internationale best practices en veiligheidsoverwegingen, met de toezegging dat een uitvoeringstoets (impactanalyse) op de haalbaarheid en betaalbaarheid zou volgen. In 2024 is het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) geraadpleegd over het impactonderzoek. Het OBDO heeft daarbij aangegeven behoefte te hebben aan meer inzicht in de organisatorische, financiële, technische en communicatie implicaties alsook scope en reikwijdte van mogelijke invoering als basis voor mogelijke vervolgbesluitvorming.

Tijdens het wetgevingsoverleg op 2 maart 2026 heeft de Tweede Kamer verzocht om voor het zomerreces een plan van aanpak inclusief tijdpad over het overgaan van de overheidssites naar één domeinextensie te ontvangen. [10] In dat debat heeft de huidige staatssecretaris van Koninkrijksrelaties en Slagvaardige Overheid toegezegd de impactanalyse inclusief een realistisch plan van aanpak en een tijdsplanning (op hoofdlijnen) vóór het meireces toe te sturen aan de Tweede Kamer als bijlage bij een Kamerbrief over belangrijkste onderzoeksbevindingen.

1.1 Digitale soevereiniteit

De invoering van een uniforme domeinnaamextensie raakt direct aan het bredere debat over digitale soevereiniteit in Nederland en Europa. In recente visies op digitale autonomie en soevereiniteit benadrukt de rijksoverheid dat zij minder afhankelijk wil zijn van (niet-Europese) partijen en meer grip wil op kritieke digitale infrastructuur en processen.[11]Digitale soevereiniteit wordt daarin niet alleen opgevat als "waar data staat", maar vooral als zeggenschap, continuïteit en realistische exit-opties: de overheid moet zelf kunnen bepalen op welke infrastructuur haar kernsystemen draaien, onder eigen juridische en bestuurlijke controle, en zo nodig kunnen overstappen zonder dat diensten uitvallen.[12]

Een uniforme domeinnaamextensie voor rijkswebsites is in dat licht een belangrijke soevereiniteitsingreep op het niveau van de digitale basisinfrastructuur. Door het

[9] Digitale Verwaltung - Digitale Dachmarke (https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/digitale_dachmarke/digitale_dachmarke-node.html). Duitsland heeft gekozen voor een low-impact invoeringsmodel op basis van vrijwilligheid.
[10] Tweede Kamer (2025-2026), 36 800 VII, nr. 82.
[11] Rijksoverheid, 'Visie digitale autonomie en soevereiniteit van de overheid', 2025.
[12] Tweede Kamer, Kamerstuk over digitale autonomie en soevereiniteit, 2025.

publieke gezicht van de rijksoverheid onder één, door de Staat zelf beheerd second-level domein (bijvoorbeeld *.gov.nl*) te brengen, komt de inrichting, naamgeving en hosting van rijksdiensten gecontroleerd onder één governance-model. Dat maakt het mogelijk om DNS-voorzieningen expliciet als vitale infrastructuur te positioneren en de weerbaarheid daarvan te verhogen, in lijn met recente beleidskeuzes om DNS-dienstverleners en hun infrastructuur als essentiële/vitale aanbieders aan te merken[13]. Hierdoor kunnen open standaarden (zoals DNSSEC, TLS en IPv6) en beveiligingsmaatregelen rijksbreed worden afgedwongen en kan bij verstoringen of geopolitieke spanningen sneller en gecoördineerd worden gehandeld.

De invoering van een uniforme domeinnaamextensie sluit daarmee aan bij de Nederlandse Digitaliseringsstrategie (NDS), doordat het de domeinnamen en DNS-infrastructuur van de Rijksoverheid als één samenhangende, door de Rijksoverheid zelf geregisseerde voorziening organiseert – precies het type grip op cruciale digitale infrastructuur en afhankelijkheden dat in de NDS en bijbehorende uitwerkingen zoals het Nationaal Actieplan Webbeleid wordt nagestreefd.[14]

2 Opzet impactanalyse

2.1 Projectbegrenzing

In 2025 hebben Berenschot en PBLQ geadviseerd over de manier waarop het onderzoek naar invoering van een uniforme domeinnaamextensie het beste kan worden afgebakend. Mede op basis van dat advies is besloten de scope te beperken tot alleen de departementen en uitvoerders binnen de Rijksoverheid, als een mogelijke eerste invoeringsfase. Overweging is dat invoering, ook Overheidsbreed, alleen kans van slagen heeft wanneer de Rijksoverheid de extensie consequent adopteert én wanneer randvoorwaarden, zoals een centraal aanvraag en uitgifteproces en helderheid in de aansluitingsvoorwaarden door de Rijksoverheid zijn ingeregeld.

De scope van dit plan van aanpak richt zich op het uitvoeren van een impactanalyse om inzicht te krijgen op de impact van invoering van een uniforme domeinnaamextensie voor de websites van de departementen en uitvoerders die de rijkshuisstijl (met het Rijkslint) hanteren. In het onderzoek ligt de focus op *.gov.nl. Aangezien formeel nog geen definitieve keuze lijkt te zijn gemaakt voor een uniforme domeinnaamextensie wordt per onderzoeksthema aangegeven wat de impact is wanneer gekozen zou worden voor *.overheid.nl.

2.1.1 Binnen scope

- Alle publiek benaderbare domeinen (onder andere websites en inlogpagina's voor overheidsinformatie en dienstverlening) van departementen en uitvoerders binnen de Rijksdienst (dat wil zeggen een (groot) deel van de organisaties die de rijkshuisstijl met het Rijkslint voeren).[15]

[13] NCSC, 'Betrouwbaarheid DNS van Nederlandse overheden', adviesrapport, 2023.
[14] Digitale Overheid, 'Nederlandse Digitaliseringsstrategie (NDS)', beleidskader. Nationaal Actieplan Webbeleid.
[15] Zie bijlage: Overzicht departementen en agentschappen Rijksdienst.

2.1.2 Buiten scope

- Alle overige overheidsdomeinen (dat wil zeggen de overige organisaties binnen de Rijksoverheid, zelfstandige bestuursorganen (ZBO's), medeoverheden, publiek-private samenwerkingen, etc.).[16]
- E-mail.[17]
- Interne domeinen, of domeinen met andersoortige gebruiksdoelen dan publieksinformatie en dienstverlening (intra- en extranetten, beheerdomeinen, domeinen voor testdoeleinden, etc.).

2.1.3 Beoogd resultaat

De impactanalyse moet resulteren in een onderbouwd inzicht in de impact, haalbaarheid, betaalbaarheid en randvoorwaarden van de invoering van een uniforme domeinnaamextensie (.gov.nl of .overheid.nl) binnen een beperkte scope als mogelijke eerste fase voor bredere invoering. Onderdeel van het onderzoek is een scenarioverkenning of plan van aanpak (op hoofdlijnen) voor gefaseerde implementatie.

2.2 Aanpak

De impactanalyse is gebaseerd op eerder uitgevoerd onderzoek, aangevuld met informatie die in verdiepingssessies met relevante stakeholders[18] binnen de Rijksoverheid is opgehaald. Onderdeel van het onderzoek vormt een onafhankelijke kostenraming van omzetting van het huidige webportfolio binnen scope om een eerste inschatting te kunnen maken van de financiële impact.

Daarnaast worden de volgende inventarisaties uitgevoerd:

- Een inventarisatie van de huidige situatie binnen de Rijksoverheid aangaande het gebruik van domeinnamen en de wijze waarop die domeinnamen worden beheerd.
- Inventarisatie en classificatie van de publieke domeinnamen binnen scope.[19]
- Een verkenning van de benodigde centrale beheercomponenten zoals een centraal uitgiftepunt. Met aandacht voor:

[16] Zie onderzoek scope en reikwijdte uniforme domeinnaamextensie (Berenschot 2025): een verkenning naar overheden die in de toekomst gebruik zouden kunnen maken van een overheidsextensie.
[17] Wegens gebruik van e-mail als inlog identiteit in combinatie met single sign on toepassingen wordt de impact van aanpassing van e-mailadressen vele malen hoger ingeschat dan alleen aanpassing van domeinnamen van websites. Tegelijkertijd is het zo dat contact met de burger in toenemende mate plaatsvindt via chatfunctionaliteit en online formulieren. Het lijkt voor de hand liggend om in een vervolgfase wel functionele e-mail mee te nemen, zoals bulkmailings vanuit bijvoorbeeld mijn.overheid.nl en te onderzoeken of voor publiekscommunicatie gebruik kan worden gemaakt van alias adressen. Vanuit mijn.overheid.nl wordt er gewerkt aan een overheidsbrede e-mail notificatieservice. Met deze technische voorziening wordt het makkelijker voor publieke dienstverleners en medeoverheden om gebruik te maken van een uniforme domeinnaamextensie. Voor heldere communicatie naar burgers en ondernemers is het belangrijk dat website en e-mailadres op elkaar zijn afgestemd.
[18] De volgende stakeholders zijn bevraagd in verdiepingssessies en/of hebben specifieke onderzoeksinformatie aangeleverd: AZ (Dienst Publiekscommunicatie), AZ/DPC Team Domeinnaamregistratie, Bureau Forum Standaardisatie, BZK CIO Rijk en Digitaliseringsbeleid, BZK Publieke Dienstverlening en Digitalisering, Belastingdienst, Defensie, DICTU, Dienst Uitvoering Onderwijs, ICTU, Logius, NCSC, Rijksdienst voor Ondernemend Nederland, KVK Digitaal Ondernemersplein, Rijksdienst voor Volksgezondheid en Milieu, SSC-ICT.
[19] Onderdeel van de impactanalyse vormt een kostencalculatie door Bureau Berenschot ten aanzien van de financiële impact van omzetting van het huidige domeinportfolio (binnen scope). Hiervoor worden de domeinen op basis van verschillende criteria geïnventariseerd en geclassificeerd in de categorieën "laag complex", "gemiddeld complex" en "hoog complex".

    - De rollen en taken van het uitgiftepunt;
    - Een gedelegeerd dns-model;
    - De governance (o.a. beleid en uitvoering) waarmee het domeinnaambeleid wordt onderhouden;
    - De benodigde middelen en kosten van het centraal uitgiftepunt;
- Het opstellen van realistische invoeringsscenario's met een planning op hoofdlijnen;
- Een aanzet tot een communicatiestrategie die gedurende de looptijd van het programma.

3 Uitkomsten impactanalyse

In dit hoofdstuk worden de resultaten van de impactanalyse gepresenteerd. Beschreven worden achtereenvolgens: (1) de belangrijkste bevindingen uit eerdere onderzoeken en adviezen (o.b.v. desk onderzoek), (2) de relatie tussen een uniforme domeinnaamextensie en digitale soevereiniteit, (3) de impact van de invoering per thema: organisatie, techniek, financiën en communicatie, (4) de benodigde governance en beheer en randvoorwaarden om de extensie gecontroleerd, veilig en uitvoerbaar te kunnen invoeren en (5) een tweetal realistische implementatiescenario's met tijdslijnen.

3.1 Desk onderzoek

In het deskonderzoek zijn meerdere onderzoeken en adviezen geanalyseerd om op hoofdlijnen te begrijpen (1) wat de meerwaarde is van een uniforme domeinnaamextensie vanuit burgerperspectief, (2) welke aanvullende maatregelen nodig zijn om effect te bereiken, en (3) wat de belangrijkste randvoorwaarden en impactfactoren zijn voor mogelijke implementatie.

3.1.1 Burger -en ondernemersperspectief

Het Centerdata onderzoek (2023) [10] laat zien dat een uniforme domeinnaamextensie burgers (en ondernemers) kan helpen om overheidswebsites beter te herkennen en om frauduleuze look-alikes sneller als "niet overheid" te identificeren. Daarbij is een belangrijke uitkomst dat uitleg en bekendheid sterk bijdragen aan het effect: hoe beter mensen weten waar ze op moeten letten, hoe groter de herkenningswinst. Het onderzoek laat ook een nuance zien tussen "voorkeur" en "effect": respondenten vinden ".overheid.nl" op het eerste gezicht vaak logischer, terwijl ".gov.nl" in sommige tests rond look-alikes juist beter helpt bij het ontmaskeren van misleiding.

Het Kantar-onderzoek (2019) [3] bevestigt de noodzaak van zo'n herkenbaar signaal, omdat veel mensen te maken hebben (gehad) met phishing en vervalste websites. Kantar laat zien dat burgers (en ondernemers) vaak (onterecht) vertrouwen ontlenen aan het "slotje" (HTTPS), terwijl ook nepwebsites dat kunnen voeren. De domeinnaam is daarom een belangrijker anker, maar burgers (en ondernemers) kennen de "echte" domeinen niet altijd, waardoor ook legitieme overheidswebsites soms niet als echt worden herkend. Dit onderzoek laat zien dat er draagvlak is voor uniformering door invoering van een domeinnaamextensie. De voorkeur van respondenten neigt in dit onderzoek sterk naar ".overheid.nl".

3.1.2 Extensie als deeloplossing

Ecorys (2020) [6] plaatst een uniforme extensie nadrukkelijk in een bredere set van maatregelen om de herkenbaarheid van de digitale overheid te vergroten, zoals een publiek toegankelijk register van overheidsdomeinen, (meer) centrale platformen/standaardisatie en communicatie-afspraken. De kern is dat maatregelen elkaar kunnen versterken en dat je het effect van "URL-herkenning" in de praktijk niet moet overschatten, omdat veel gebruikers via zoekmachines en apps binnenkomen. Tegelijk blijft een uniforme extensie nuttig als consistent signaal, zeker in combinatie met een register/bron van waarheid en goede communicatie.

3.1.3 Aandachtspunten eerder onderzoek

3.1.3.1 Governance

Het adviesrapport internetdomeinbeleid (Bureau Forum Standaardisatie, 2022) [9] beschrijft dat het domeinportfolio versnipperd is en dat afspraken in de praktijk niet altijd worden nageleefd. De hoofdboodschap is dat uniformering alleen duurzaam werkt als er centrale spelregels, lifecyclebeheer (aanvragen, wijzigen, uitfaseren) en een actueel overzicht/register bestaan, en vooral: als er governance en toezicht is belegd (iemand die kan sturen en corrigeren).

3.1.3.2 Techniek

De technische impactanalyse van ICTU (2022) [8] maakt duidelijk dat de grootste technische impact vaak niet in DNS zelf zit, maar in alles wat eraan gekoppeld is: koppelingen en API's, hardcoded URL's (bijvoorbeeld in mobiele apps), security-instellingen en mogelijk browsergedrag (zoals public suffix). Daarnaast benadrukt ICTU dat de centrale voorzieningen voor aanvraag/uitgifte en DNS-beheer robuust en veilig moeten worden ingericht, omdat die in de praktijk kenmerken krijgen van een vitale bouwsteen.

3.1.3.3 Fasering

Het buitenlandonderzoek (PBLQ, 2019) [13] laat zien dat landen verschillende modellen hanteren (vrijwillig vs. verplicht, wel/geen handhaving) en dat adoptie in de praktijk vaak lang duurt. In veel landen ligt de focus primair op de centrale overheid en is verbreding naar alle organisaties minder vanzelfsprekend. Dit ondersteunt het belang van een realistisch transitiepad en het expliciet organiseren van uitzonderingen en adoptieondersteuning.

3.1.3.4 Geïdentificeerde risico's

Berenschot (2025) [12] benadrukt dat uniformering aanzienlijke kosten en inspanning vraagt en dat een extensie niet op zichzelf alle veiligheidsproblemen oplost. Het rapport wijst er ook op dat verbreding naar e-mail doorgaans nog complexer en duurder is. De VNG-studie (2019) [4] onderschrijft dat e-mailmigratie een belangrijk effect heeft op de kosten en benoemt daarnaast aandachtspunten rond kwetsbaarheden zoals het risico op het ontstaan van een "single point of failure" bij centralisatie. Vraag die in algemene zin wordt gesteld is of de inspanning van een dergelijk omvattend traject (op gebied van kosten en capaciteit) opweegt tegen de verwachte baten.

3.1.3.5 Buitenland

Veel landen om ons heen hebben de afgelopen jaren al gekozen voor een uniforme domeinnaamextensie of een strak domeinnaambeleid voor hun centrale overheid. Het buitenlandonderzoek van PBLQ [5] laat zien dat een aanzienlijk aantal landen een

overheidsdomein volgens het zogeheten *DNS-concept* gebruikt (bijvoorbeeld *.gov.uk[20], *.gv.at, *.gov.it, *.gov.au, *.govt.nz, *.gov), vaak gecombineerd met een helder naamgevingsbeleid en een centrale rol van de nationale overheid in uitgifte en beheer. Daarnaast is er een duidelijke trend dat sommige landen (onder meer Vlaanderen, het Verenigd Koninkrijk, Canada, Noorwegen en Zweden) dit verder doortrekken in de vorm van een centraal platform (gov.cc/), waarbij herkenbaarheid, betrouwbaarheid, veiligheid en beheerbaarheid de belangrijkste drijfveren zijn. Herkenbaarheid voor burgers (en ondernemers) wordt daarbij het vaakst genoemd, gevolgd door betrouwbaarheid en beheersbaarheid; veiligheid en vindbaarheid spelen in de meeste landen eveneens een relevante, zij het iets minder uitgesproken rol.

3.1.4 Samenvattend

Over alle documenten heen ontstaat één consistent beeld: een uniforme domeinnaamextensie draagt bij aan herkenbaarheid van de digitale overheid en het verminderen van misleiding. Het effect hangt sterk af van communicatie en het combineren met andere bouwstenen zoals een domeinnaamregister en eenduidige spelregels. Implementatie vraagt expliciete governance (incl. toezicht). Technisch zit de impact niet alleen in DNS, maar (juist) ook in koppelingen, API's en verwijzingen in harde code die onder water moeten worden aangepast Een gefaseerde aanpak binnen een afgebakende scope is cruciaal om haalbaarheid en betaalbaarheid te borgen. Dit laat ook het buitenland onderzoek zien.

4 Impact op organisatie, techniek, financiën, communicatie en governance

4.1 Organisatie

De invoering van een uniforme domeinnaamextensie raakt organisaties primair op de as governance, eigenaarschap, webportfolio-beheer en ketenverantwoordelijkheid. Onderzoeken beschrijven het probleem vaak als "herkenbaarheid" voor burgers (en ondernemers), maar in de uitvoering blijkt dat de extensie vooral een sturingsinstrument wordt dat ingrijpt in de manier waarop organisaties domeinen aanvragen, beheren, uitfaseren en verantwoorden. Het adviesrapport internetdomeinbeleid (Bureau Forum Standaardisatie) [9] concludeert dat internetdomeinbeheer zowel decentraal als centraal nog onvoldoende volwassen is ingericht en dat daardoor een effectief sturingsinstrument ontbreekt om grip te krijgen op het portfolio aan overheidsdomeinen. Door gebrek aan grip is een wildgroei van domeinnamen ontstaan met bijvoorbeeld websites die (ongeveer) dezelfde informatie bevatten, niet voldoen aan de wettelijke eisen (en overige richtlijnen), soms buiten beeld zijn geraakt terwijl de beheerkosten ieder jaar worden afgeboekt.[21] Het rapport positioneert een herkenbare overheidsextensie nadrukkelijk als één van de samenhangende oplossingen om in control te komen, naast het Register

[20] In het Verenigd Koninkrijk wordt vooral gebruik gemaakt van zowel een centraal platform https://www.gov.uk/ als decentrale platforms, bijvoorbeeld https://www.manchester.gov.uk/. Daarnaast komt gebruik van de extensie .gov.uk ook voor.
[21] Op dit moment loopt een verkenning om boven water te krijgen welke verkeerd geregistreerde domeinen mogelijk van de overheid zijn.

Internetdomeinen van de Overheid, centrale registrar, lifecycle-afspraken, toezicht/handhaving en rolbelegging.

Die conclusie wordt in de verdiepingssessies vrijwel één-op-één bevestigd. DPC en Bureau Forum Standaardisatie (BFS) schetsen dat het beheer in de huidige situatie "valt of staat" met domein-liaisons bij rijksorganisaties, die vaak onvoldoende kennis hebben, de rol als corvee zien en daardoor beperkt bijdragen aan kwaliteit en actualiteit van registratie- en beleidsafspraken. Ook wordt "wildgroei" als structureel probleem benoemd en blijkt dat er beperkte mogelijkheden zijn om af te dwingen dat organisaties eerst saneren, hergebruiken of onderbrengen op bestaande domeinen in plaats van steeds nieuwe domeinen te registreren.

De verdiepingssessies maken bovendien concreet waarom dit organisatorisch zwaar is: grote uitvoerders en stelselpartijen (zoals Logius) hebben doorgaans meerdere teams per platform/omgeving, terwijl de "domeinlogica" door alle ketens heen loopt. De Belastingdienst beschrijft een keteninrichting waarbij wijzigingen per keten worden gepland en beoordeeld, en waarbij meerdere teams tegelijk worden geraakt (HCL, WordPress, OpenShift, Pleio, etc.) plus het Network Operations Center (NOC) als bottleneck voor netwerk-, firewall- en monitoringwijzigingen. Organisatorische randvoorwaarde is daarom dat een extensietraject niet als losstaande actie voor een enkele website moet worden behandeld, maar als ketenwijziging met vroegtijdige betrokkenheid van NOC en ketenverantwoordelijken.

Bij Logius/KOOP wordt dit nog scherper: zij spreken van een "stelsel van diensten" waarin interne en externe omgevingen met elkaar verweven zijn. Het portfolio bestaat niet alleen uit een extern overzicht, maar ook uit tientallen interne websites die soms publiek benaderbaar zijn en waarbij split-DNS en interne netwerken (bijv. Diginetwerk) een rol spelen. Organisatorisch betekent dit dat inventarisatie en volgordelijkheid randvoorwaardelijk zijn; er wordt voorgesteld een 'mindmap' te maken van afhankelijkheden om überhaupt een migratiestrategie te kunnen bepalen.

Rijkswaterstaat laat vervolgens zien hoe organisatorische portfolio-problematiek er in de praktijk uitziet: duizenden sites, dubbelingen, domeinen die niet allemaal zijn aangemeld of centraal gehost, externe bureaus die projectwebsites "in de lucht brengen" en beheer dat later bij RWS terechtkomt. In zo'n context wordt een uniforme extensie niet alleen een herkenbaarheidsmaatregel, maar ook een hefboom om intake, eigenaarschap, lifecycle en opschoning af te dwingen. Tegelijkertijd benoemt RWS dat dit alleen werkt als er een rijksbreed afwegingskader en mandaat is; anders blijven uitzonderingen en "geitenpaadjes" bestaan.

Het scope- en reikwijdteonderzoek van Berenschot [12] plaatst deze organisatorische spanning in een bestuurlijk kader: gesprekspartners erkennen het belang van herkenbaarheid, maar vragen of de investering (tijd, geld, capaciteit) in verhouding staat tot de baten, zeker gezien parallelle opgaven (informatiehuishouding, NIS2, digitale toegankelijkheid). Daarmee wordt organisatiecapaciteit expliciet als schaarste benoemd. Berenschot benadrukt ook dat scope (welke overheidsorganisaties) en reikwijdte (welke categorieën websites/diensten) geen detailkeuze zijn, maar bepalend voor uitvoerbaarheid, draagvlak en effectiviteit.

Randvoorwaarden op organisatieniveau komen in alle bronnen consistent naar voren:

- Het traject moet als programma/project worden ingericht, niet als regulier beheer. RIVM benoemt expliciet dat vooral communicatie en governance/coördinatie de grootste uitdaging zijn, en dat een dedicated projectmatige trekker nodig is.
- Er moet een afwegingskader komen voor: (a) welke sites in scope zijn, (b) hoe om te gaan met samenwerkingssites, campagnesites en regionale projecten, en (c) welke uitzonderingen noodzakelijk zijn. Rijkswaterstaat, Dictu en DPC/BFS leggen hier veel nadruk op.
- Een centrale "basishygiëne" moet worden geborgd: lifecycle-afspraken, periodieke checks, eisen richting leveranciers en centrale monitoring/toezicht, zoals ook het adviesrapport internetdomeinbeleid (Bureau Forum Standaardisatie) [9] bepleit.
- Fasering moet realistisch zijn, bij voorkeur gekoppeld aan natuurlijke momenten (bijv. LCM/certificaatverloop/platformvernieuwing). Logius/KOOP, RIVM en Ecorys [6] onderkennen het belang van overgangsperioden als bijna onvermijdelijk.

Het toenemende belang om in control zijn op het eigen domeinportfolio wordt expliciet gemaakt in de Cyberbeveiligingswet (CBW) die overheidsorganisaties verplicht hun domeinnamen te registreren wanneer zij zich registreren als overheidsentiteit.

4.1.1 Organisatie .gov.nl versus .overheid.nl

Organisatorisch is het verschil tussen .gov.nl en .overheid.nl niet groot, maar wel relevant. In beide gevallen blijft de hoofdopgave hetzelfde: organisaties moeten hun webportfolio in beeld brengen, bepalen welke websites in scope vallen en de migratie organiseren in samenhang met governance, lifecyclemanagement en ketenverantwoordelijkheid. Het verschil zit vooral in de impact op bestaande naamgeving. .overheid.nl sluit beter aan op bestaande centrale omgevingen zoals (rijks)overheid.nl en mijn.overheid.nl, waardoor voor een deel van het huidige landschap minder aanpassing nodig is. .gov.nl vraagt juist om herpositionering van dit soort centrale domeinen, maar sluit beter aan bij de lijn van veel landen om Nederland heen en bij het eerdere principebesluit om .gov.nl als uitgangspunt te nemen. In beide gevallen blijven duidelijke centrale kaders nodig voor naamgeving, toewijzing, uitzonderingen en mandaat. Zonder die sturing blijft het risico bestaan dat versnippering in stand blijft.

4.1.2 Samenvattend

Organisatorisch is invoering van een uniforme domeinnaamextensie kansrijk als zij wordt gepositioneerd als onderdeel van (rijks)overheidsbreed internetdomeinbeleid (met heldere kaders, inclusief toezicht en handhaving). Daarnaast is randvoorwaardelijk dat uitvoeringsorganisaties en departementen voldoende tijd en ruimte krijgen om hun portfolio op orde te brengen en ketens gecontroleerd te migreren binnen een gestructureerde programma-aanpak.

4.2 Techniek

Technisch gezien komt uit alle bronnen één rode draad naar voren: een uniforme extensie is technisch haalbaar, maar de impact wordt bepaald door ketenafhankelijkheden, DNS/infra-architectuur, redirects/SEO, certificaatbeheer en uitzonderingscategorieën (zoals linked data/permalinks). De ICTU technische

impactanalyse [8] benoemt dat DNS een internet-nutsvoorziening is en dat storingen vaak terug te leiden zijn tot DNS; de benodigde centrale voorzieningen (uitgiftepunt, DNS, publiek register) moeten daarom worden behandeld als (mogelijk) vitale infrastructuur. ICTU beschrijft tevens dat de dienstverlening het hele lifecycle management van domeinen moet ondersteunen en dat beveiliging van het uitgiftepunt essentieel is (functiescheiding, workflow, logging, sterke authenticatie/autorisatie, bescherming master DNS).

De verdiepingssessies maken concreet waar de technische pijn zit. De Belastingdienst is hierin het scherpst: een extensiewijziging is geen "alleen DNS", maar raakt DNS, loadbalancers, firewalls, applicatie- en platformlaag, content, logging en monitoring. Door de ketenorganisatie moet iedere wijziging per keten worden uitgewerkt en ingepland, en is planning/testlast het dominante risico.

Dit patroon zie je ook bij Logius/KOOP (stelsel van diensten / stacked services), RIVM (koppelingen zoals SAML/DigiD/eHerkenning vragen ketentesten) en Rijkswaterstaat (veel verschillende CMS/platformen; mix van hostingpartijen; grote redirectproblematiek (in het verleden)).

4.2.1 DNS-inrichting en robuustheid

Meerdere bronnen waarschuwen expliciet voor het bouwen van een te centrale constructie die als single point of failure kan fungeren. Logius/KOOP stelt dat een robuust DNS-systeem cruciale randvoorwaarde is en dat vier nameservers onvoldoende wordt gevonden voor een nieuwe, zeer zichtbare overheidszone; er is behoefte aan meer redundantie, spreiding en diversiteit. Ook wordt gepleit voor delegatie van subdomeinen (bijv. digid.gov.nl), zodat organisaties afzonderlijk verantwoordelijk zijn en impact van storingen beperkt blijft.

DPC en Bureau Forum Standaardisatie benoemen dat de grootste verandering niet zit in "handjes" maar in infrastructuur: voorkomen moet worden dat met invoering van .gov.nl een potentiële single point of failure (SPoF) ontstaat. Van belang is dat DNS-infra robuust wordt neergezet conform de technische inrichting zoals SIDN die hanteert voor het .nl domein. Tegelijk wordt aangegeven dat DPC in de huidige situatie al Anycast DNS inzet met geografische spreiding en goed uit tests komt, maar dat er organisatorisch nog een verbeterslag te maken is.

4.2.2 Certificaten

Certificaatbeheer komt in vrijwel alle sessies terug als grote beheer- en risicofactor. Logius/KOOP stelt dat een root-certificaat voor alle .gov.nl-domeinen te risicovol is; compromittering zou de hele keten raken.[22] Gepleit wordt voor een gedelegeerd model met eigen certificaten per suborganisatie en spreiding over certificaatautoriteiten (CA's). NCSC onderschrijft dit volledig. RIVM geeft aanvullend aan dat certificaten vaak drie jaar geldig zijn en dat koppeling aan certificaatverloop logisch is om dubbele rondes te voorkomen. Ook geeft het aan RIVM dat niet alle organisaties dezelfde CA gebruiken en dat dit in de ontwerpkeuze moet worden ondersteund.

Bureau Forum Standaardisatie licht toe dat Publiek vertrouwde eindcertificaten per maart 2026 nog maximaal 200 dagen geldig zijn en dat de levensduur in de komende jaren teruggaat naar maximaal 42 dagen. Bureau Forum Standaardisatie geeft aan dat de

[22] N.B. Er zijn geen publieke rootcertificaten binnen de overheid.

keuze in CA onafhankelijk is van welk domein je gebruikt en dat voor certificaatvervanging gebruik gemaakt dient te worden van standaard geautomatiseerd certificaatbeheer (Automatic Certificate Management Environment, verder ACME).

RWS noemt expliciet de wens om ACME te gaan gebruiken, maar geeft ook aan dat beleidskeuzes rond CA's (bijvoorbeeld de vraag of Let's Encrypt expliciet verboden is) randvoorwaardelijk zijn.

4.2.3 Redirects, SEO en permalinks

In de praktijk is de grootste technische én publieksrisicozone: redirects en vindbaarheid. De Belastingdienst beschrijft redirects als noodzakelijk voor externe verwijzingen en voorziet problemen voor het aanpassen van papieren brieven (die lang in omloop blijven). De Belastingdienst illustreert een gecontroleerde aanpak aan de hand van de Douane-case[23]: In deze aanpak is gedurende een langere periode gebruik gemaakt van een redirectregister, monitoring en vervolgens afbouw van redirects op basis van gebruik.

De KvK (Programma Digitaal Ondemersplein) bevestigt vanuit eigen migratie (Ondernemersplein.overheid.nl) dat vindbaarheid vrijwel altijd (tijdelijk) afneemt en dat herstel weken tot maanden kan duren. Redirect-ketens moeten worden vermeden en het handhaven van URL-structuur voorkomt extra schade.

Het RIVM vraagt daarom om een centrale SEO/redirect-blauwdruk die organisaties kunnen toepassen.

Volgens de architecten van Logius/KOOP komt daar nog een aparte, technisch-semantische laag bij: permalinks en linked data (URI's). Hier kan het domeinonderdeel onderdeel zijn van de identifier zelf. Wijziging kan semantische breuk veroorzaken, terwijl onduidelijk is wie de URI's gebruikt. Daarnaast kan bij wettelijk verankerde URL's (zoals officielebekendmakingen.nl) zelfs wetgeving een rol spelen. Daarom worden scenario's geadviseerd waarin bestaande links/URI's blijven bestaan en alleen nieuwe links eventueel onder de nieuwe extensie worden uitgegeven, of waarin de bestaande extensie blijft.

4.2.4 (Functionele) E-mail (techniek en architectuur)

Het buitenlandonderzoek van PBLQ [5] laat zien dat overheden zelden e-mail overheidsbreed uniformeren, omdat e-mailadressen verweven zijn met autorisatie en operationele processen en daardoor technisch zeer complex zijn om te migreren.

In de verdiepingssessies komt dezelfde conclusie terug: hoewel e-mail vaak buiten scope wordt gehouden, is het communicatief niet los te zien van websites. RIVM benoemt risico's van denylisting door mailproviders en wijst op kritieke processen die geraakt kunnen worden. NCSC nuanceert dat blocklisting vaak op mailserver/IP plaatsvindt en ziet kansen voor allow-listing van *.gov.nl door grote providers, maar benadrukt tegelijk dat dit onderzocht moet worden en dat web en mail in samenhang consistent moeten worden benaderd. NCSC adviseert ten aanzien van e-mail op subdomeinen van gov.nl de standaarden SPF, DMARC en DKIM te implementeren en op gov.nl een default DMARC-policy zodat bij eventueel missende DMARC policies op subdomeinen het second level

[23] Douane-case: omzetting van websites met gebruik van redirects gedurende een langere periode.

domein voor een veilige policy kan zorgen en/of kan zorgen dat niet-bestaande domeinen niet gespoofed kunnen worden.

Op dit moment loopt vanuit BZK een separaat onderzoekstraject naar uniformering van e-mail van de Rijksdienst. Vanuit herkenbaarheid en transparantieoverwegingen zou het aan te bevelen zijn om te komen tot een uniforme e-mail extensie die hetzelfde is als de uniforme extensie voor websites. In dat kader kan worden verkend om alleen functionele e-mail (bulkmailings, notificaties, etc.) van een e-mailadres met de *.gov.nl of *.overheid.nl extensie te voorzien.

Functionele e-mail betreft e-mailadressen, zogenaamde Functionele Postbussen, die direct gekoppeld zijn aan functies van de website bijvoorbeeld info@weguitbreiding.gov.nl voor het aanvragen van extra informatie of no-reply@weguitbreiding.gov.nl voor herkenbaarheid van de afzender van de mail maar waarop je juist niet moet antwoorden. Het functionele e-mailadres staat hierbij los van het e-mailadres dat gebruikt wordt door de medewerkers van de organisatie voor de interne communicatie binnen de overheidsorganisatie. Zoals eerder gesteld er vaak een grote verwevenheid met autorisaties en interne processen zodat wijziging van deze mailadressen grote impact heeft waarom het ook bij voorbaat al buiten scope geplaatst is. Contact via persoonlijke e-mail tussen individuele ambtenaren en burgers (en ondernemers) is vrij beperkt, online contact tussen overheid en burger vindt in toenemende mate plaats via onlineformulieren en chats.

4.2.5 Technische aansluitvoorwaarden

Voor de inrichting van een uniforme domeinnaamextensie dienen duidelijk technische randvoorwaarden van toepassing te zijn. Uit de inbreng van het NCSC volgt dat de extensie alleen toekomstbestendig en robuust kan functioneren wanneer de onderliggende DNS-infrastructuur voldoet aan moderne internet- en beveiligingsstandaarden. Daarbij gaat het in ieder geval om ondersteuning van IPv6 op nameservers (en wellicht ook webservers), het gebruik van RPKI voor de beveiliging van routering, en DNSSEC voor de cryptografische ondertekening van DNS-verkeer.

Daarnaast wordt aangegeven bij uitgifte van een nieuw subdomein van gov.nl direct passende basisinstellingen in te stellen voor SPF en DMARC, zodat op domeinniveau goede uitgangspunten bestaan voor e-mailbeveiliging. Verder zijn er aanvullende standaarden, zoals BGPsec en ASPA, die nog minder breed worden toegepast, maar wel relevant kunnen zijn in de verdere doorontwikkeling van een veilige en toekomst vaste inrichting.

Het NCSC benadrukt daarnaast dat het risico op technisch falen klein is wanneer de infrastructuur schaalbaar en gespreid wordt opgezet. Dat betekent onder meer: meerdere nameservers op verschillende locaties, bij verschillende hostingpartijen en in verschillende autonome systemen, met waar mogelijk ook variatie in gebruikte software. Ook moet worden voorkomen dat de nameservers op de verschillende locaties afhankelijk zijn van dezelfde upstream netwerkleverancier. Toepassing van BGP Anycast draagt bij aan extra weerbaarheid, onder meer tegen DDoS-aanvallen.

Tot slot is van belang dat het beheer wordt belegd bij een partij met aantoonbare kennis en ervaring met grootschalig DNS-beheer. Daarmee wordt het risico op een single point of failure in de praktijk sterk beperkt.

4.2.6 Techniek *.gov.nl versus *.overheid.nl

Technisch gezien is het verschil tussen .gov.nl en .overheid.nl beperkt, omdat bij beide keuzes dezelfde hoofdopgave blijft bestaan: de impact wordt vooral bepaald door ketenafhankelijkheden, DNS- en infrastructuurkeuzes, certificaatbeheer, redirects en SEO, permalinks en linked data, en de relatie met functionele e-mail. Uit de technische analyses en verdiepingssessies blijkt dat een uniforme extensie in beide gevallen haalbaar is, maar alleen met een robuuste DNS-inrichting, delegatie waar nodig en goed ingeregelde centrale voorzieningen, zoals een centraal uitgiftepunt en een aanvraag- en uitgifteproces onder duidelijke aansluitvoorwaarden.

Het belangrijkste technisch voordeel van .gov.nl is dat .gov.nl op de Public Suffix List (PSL) staat, terwijl .overheid.nl daar nog niet op staat. Dat betekent dat .gov.nl direct beter aansluit op de manier waarop browsers en software domeinen afbakenen (o.a. voor cookies en subdomeinen) terwijl .overheid.nl eerst nog aan de PSL moet worden toegevoegd via een aanvraagprocedure bij SIDN (en daarna tijd nodig heeft om in browsers en andere omgevingen door te werken). Vanuit strikt technisch perspectief is .gov.nl daarmee iets eenvoudiger en directer toe te passen, maar voor de bredere migratiecomplexiteit maakt de keuze tussen beide varianten uiteindelijk maar beperkt verschil. Een ander voordeel van .gov.nl is dat het technisch vergeleken met .overheid een ‘greenfield’ is en daardoor makkelijker op een robuuste manier kan worden ingericht.

Het NCSC adviseert vanuit het cybersecurityperspectief om het second-leveldomein .gov.nl te verkiezen boven het second-leveldomein .overheid.nl’, vooral omdat de kortere domeinnaam de mogelijkheden om typosquatting toe te passen aanzienlijk reduceert.

4.2.7 Samenvattend

Samenvattend is een uniforme extensie technisch haalbaar, maar alleen als de onderliggende inrichting zorgvuldig wordt vormgegeven. Dat vraagt om een robuuste opzet van DNS en het uitgiftepunt als kritieke infrastructuur, een gedelegeerd model voor DNS en certificaten met centrale kaders, en een centrale aanpak voor redirects en behoud van vindbaarheid. Daarnaast moet ruimte blijven voor uitzonderingen, zoals linked data, permalinks en wettelijk verankerde URL’s.

Ook zijn een realistische fasering, een goede inventarisatie van afhankelijkheden en ketentesten per keten nodig. Voor de inrichting van de extensie zouden bovendien duidelijke technische aansluitvoorwaarden moeten gelden, zoals ondersteuning van IPv6, RPKI, DNSSEC en passende e-mailstandaarden.

Vanuit securityperspectief heeft .gov.nl de voorkeur boven .overheid.nl.

4.3 Financiën

De invoering van een uniforme domeinnaamextensie brengt financiële gevolgen met zich mee. Daarbij gaat het niet alleen om de kosten van invoering, maar ook om de kosten van het huidige domeinportfolio, de structurele kosten van beheer en governance in een nieuwe situatie en de kosten van communicatie en publieksvoorlichting. Om de financiële impact goed te kunnen duiden, wordt hieronder onderscheid gemaakt tussen de nulsituatie, de incidentele kosten van invoering en de structurele kosten. Daarbij wordt ook rekening gehouden met de inzet die nodig is voor communicatiecampagnes, omdat juist die communicatie van belang is voor de herkenbaarheid en het effect van de nieuwe extensie.

4.3.1 Huidige situatie (nulsituatie)

Voor de financiële impact van een uniforme domeinnaamextensie is het belangrijk om eerst naar de huidige situatie te kijken. Het is lastig gebleken om een nauwkeurig beeld te krijgen van de exacte kosten aangezien deze kosten zeer gefragmenteerd en/of moeilijk herleidbaar zijn in relatie tot de betreffende organisaties en daarbinnen tot afdeling, dossier of project. Op dit moment omvat alleen al het webregister van de Rijksoverheid (versie december 2025), zoals gehanteerd in de scope-afbakening van deze impactanalyse, ongeveer 1.200 domeinen. Gerekend met een gemiddelde beheerlast van € 15.000 tot € 50.000 per domein[24] komt de huidige structurele beheerlast van het domeinportfolio van de Rijksoverheid[25] uit op een voorzichtige € 42 miljoen per jaar[26], exclusief personele kosten.

4.3.2 Incidentele kosten

Invoering van een uniforme domeinnaamextensie brengt incidentele kosten met zich mee. Het gaat dan om kosten voor voorbereiding, overgang en invoering. Denk aan het inrichten van een tijdelijke projectorganisatie om de migratie te sturen en te faciliteren en kosten voor het inregelen van een centrale governance, inclusief de registry- en registrarrol. De belangrijkste incidentele kosten hebben betrekking op de daadwerkelijke omzetting van het bestaande webportfolio, alsook op het noodzakelijke dubbeldraaien, de inzet van tijdelijke hardware en het beschikbaar moeten houden of archiveren van oude domeinen. Voor de uitgifte van nieuwe domeinnamen met de uniforme extensie is de impact ten opzichte van de bestaande situatie beperkt, omdat dit in beginsel al centraal kan worden gefaciliteerd. Daarnaast zal de transitie op een begrijpelijke manier aan het publiek moeten worden gecommuniceerd om verwarring te voorkomen.

Op basis van een externe doorrekening (Berenschot 2026) [15] bedraagt de verwachte eenmalige investering voor de migratie van het volledige webportfolio binnen scope circa € 49,6 miljoen, met een bandbreedte van € 40,1 miljoen tot € 59,2 miljoen. Deze raming is gebaseerd op een classificatie van 1.204 domeinen met een publieke functie, verdeeld in 329 laag complexe websites, 849 gemiddelde websites en 26 complexe websites. Daarbij is gerekend met gemiddelde migratiekosten van respectievelijk € 11.400 voor een laag complexe website, € 49.400 voor een gemiddelde website en € 152.000 voor een complexe website. De raming laat zien dat het grootste deel van de incidentele kosten ontstaat bij de gemiddelde websites, niet omdat deze individueel het duurst zijn, maar omdat dit verreweg de grootste categorie binnen het portfolio is. De complexe websites vormen daarentegen een relatief kleine maar financieel zware categorie, met hoge kosten per website als gevolg van intensieve werkzaamheden in met name hosting, code-aanpassingen, testen en organisatorische afstemming.

[24] 15K per jaar is een voorzichtige inschatting van regelmatig terugkerende (jaarlijkse) kosten van beheer en exploitatie van domeinen (bijvoorbeeld het toepassen van WCAG standaarden voor digitoegankelijkheid), ssl certificaten, bio scan, webarchivering, jaarlijkse leverancierskosten, etc.). Beheer van websites en webapplicaties varieert van enkele duizenden tot tienduizenden euro's per jaar, afhankelijk van de technische complexiteit. Sommige partijen rekenen zelfs met gemiddeld 50K per domein per jaar (26K enkel techniek, 50K inclusief redactie). Er wordt een gemiddelde gebruikt van 35K.
[25] Dit onderzoek is gebaseerd op het domeinnaamregister van AZ/DPC (stand: december 2025).
[26] Uitgaande van een gemiddelde van 35K per domein per jaar. Berekening 1200 domeinen x 35K.

Resultaat: Een inschatting van een volledige migratie van het webportfolio naar een uniforme domeinnaam uitgesplitst naar eenvoudig, gemiddeld en complex te migreren.

- **Eenvoudig:** €3,75 miljoen.
- **Gemiddeld:** €41,9 miljoen, met een bandbreedte tussen €33,5 miljoen – €50,3 miljoen.
- **Complex:** €3,9 miljoen, met een bandbreedte tussen €2,8 miljoen – €5,1 miljoen.

Hiermee is de totale kosteninschatting €49,6 miljoen met een bandbreedte tussen €40,1 miljoen en €59,2 miljoen.

De bandbreedte in de raming hangt vooral samen met verschillen in techniek, security-inrichting, koppelingen en organisatorische afstemming. Daarmee bevestigt de raming dat de financiële impact van invoering substantieel is en sterk wordt bepaald door de omvang en samenstelling van het bestaande webportfolio. Tegelijkertijd geeft Berenschot aan dat deze raming hoger uitkomt dan eerdere indicatieve schattingen, omdat nadrukkelijk rekening is gehouden met validatie door experts, ervaringen uit recente migratieprojecten en de bestuurlijke en organisatorische afstemming die bij overheidsmigraties in de praktijk een substantieel deel van de inspanning bepaalt. Daarmee geeft de raming een realistischer beeld van de werkelijke migratieopgave binnen de gekozen scope.

Uitgaande van een programma-aanpak kan daarnaast worden gedacht aan een programma- en implementatieteam, waarbij naast migratieondersteuning ook wordt gefaciliteerd in compliancy, sanering en centrale coördinatie. Hiervoor kan indicatief worden uitgegaan van ongeveer € 720k per jaar[27] aan programma-activiteiten. Deze kosten staan los van de feitelijke migratiekosten van het webportfolio, maar zijn wel randvoorwaardelijk om de invoering beheerst te laten verlopen. Tegelijkertijd geldt dat deze investeringen zich op langere termijn kunnen terugverdienen wanneer invoering van de uniforme domeinnaamextensie samenvalt met structurele opschoning en uitfasering van overbodige domeinen[28].

De exacte incidentele kosten per organisatie of type website zullen in de praktijk verschillen. Daarbij geldt dat een deel van de werkzaamheden kan worden ingepast in regulier beheer, lifecyclemomenten en natuurlijke overgangsmomenten. Hoe langer de doorlooptijd van de invoering, hoe meer ruimte bestaat om een deel van de benodigde capaciteit binnen de lijn op te vangen en hoe lager de extra piekbelasting buiten de reguliere werkzaamheden.

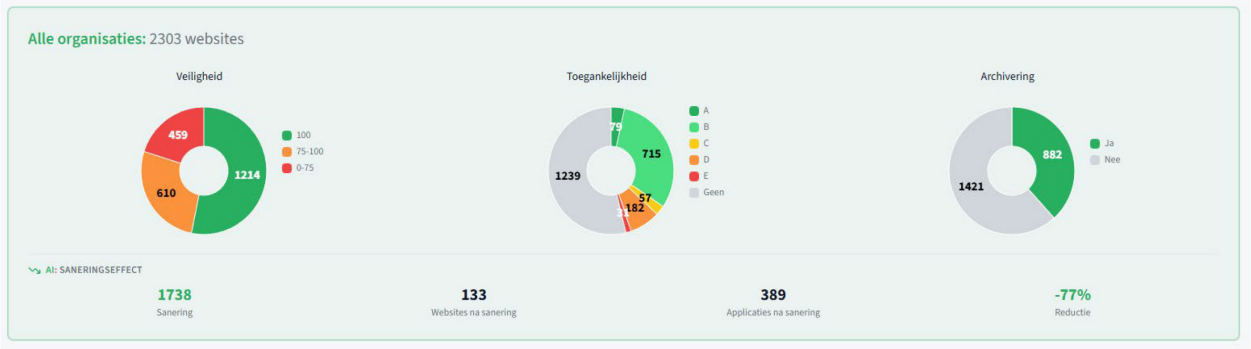
Overige incidentele kosten zijn het opzetten van een centraal aanvraag -en uitgiftepunt (gedeeltelijk geautomatiseerd) en communicatieactiviteiten (*zie tabel 3*)

4.3.3 Saneringspotentieel webportfolio Rijksdienst

Adviseurs werkzaam binnen Rijkswaterstaat hebben in 2025 een AI-tool (Portfoli) ontwikkeld (bèta-versie) waarmee inzicht gegeven kan worden in het saneringspotentieel van de websites binnen de Rijksdienst. Middels deze tool wordt er per organisatie inzage

[27] Schatting coördinatie en ondersteuning implementatie uniforme domeinnaamextensie en opschoning en sanering.
[28] Deze raming is onderdeel van een claim die in het kader van de Nationaal Actieplan Webbeleid (NAWB) financiering is ingediend in 2025.

gegeven uit hoeveel en welk type websites het webportfolio bestaat, en wat hiervan gesaneerd kan worden. Voor alle organisaties tezamen (2303 websites) wordt een reductie van 77% voorgesteld. Zie onderstaande weergave (figuur 1):



Figuur 1 Weergave saneringspotentieel Portfoli d.d. 09-04-2026. Portfoli haalt informatie op uit officiële publieke bronregisters en webarchieven. Op basis van deze input telt de tool in totaal 2303 domeinen (websites en applicaties) van departementen en uitvoerders, waarvan op basis van een AI-advies na sanering 133 websites en 389 applicaties over zouden kunnen blijven. De tool geeft onder meer inzage in de veiligheid, digitoegankelijkheid én archivering van de gevonden domeinen.

Het AI-advies uit de tool is nog vrij rigide, wat ertoe heeft geleid dat aanvullend een handmatige inschatting is gemaakt op het webportfolio binnen scope of domeinen voor migratie of juist opschoning danwel uitfasering in aanmerking kunnen komen.

Dit migratie- of saneringspotentieel is uitgewerkt in twee tabellen: 1) migratiepotentieel (*zie tabel 1*) en het 2) saneringspotentieel (*zie tabel 2).* Het migratiepotentieel heeft drie opties: 1) volledige migratie: 1204 domeinen migreren nieuwe extensie (€49,6 miljoen euro migratiekosten), 2) gematigde migratie: 555 domeinen migreren naar de nieuwe extensie (ruim €24,miljoen euro migratiekosten) en 3) minimale migratie: 387 domeinen migreren naar de nieuwe extensie (een kleine € 18 miljoen euro migratiekosten) In onderstaande tabel staan deze migratiescenario's uitgewerkt:

Mate van migreren	Aantal sites behouden	Waarvan laag complexe website	Waarvan gemiddelde website	Waarvan complexe website	Gemiddelde kosten
Volledige migratie (100%)	1204	329	849	26	€ 49.640.000
Gematigde migratie (~50%)	555	115	427	13	€ 24.380.800
Minimale migratie (~30%)	387	61	316	10	€ 17.825.800

Tabel 1 - Migratiepotentieel

Het saneringspotentieel is het aantal sites dat juist *niet* wordt gemigreerd naar de nieuwe extensie en dus wordt uitgefaseerd/ gesaneerd. Dit is op te delen in drie opties: 1) geen sanering: 0 sites (geen besparing), 2) gematigde sanering: 635 sites (gemiddelde besparing van €22,2 miljoen euro per jaar) maximale sanering: 815 sites (gemiddelde besparing van €28,5 miljoen euro per jaar). In de onderstaande tabel is het saneringspotentieel uitgewerkt:

Mate van saneren	Aantal sites uitfaseren	Gemiddeld te besparen kosten per jaar (35K p/j)	Bandbreedte kosten laag (15K p/j)	Bandbreedte hoog (50k p/j)
Geen sanering (0 %)	0	-	-	-
Gematigde sanering (~50%)	649	22.715.000	9.735.000	32.450.000
Maximale sanering (70%)	817	28.595.000	12.255.000	40.850.000

Tabel 2 - Saneringspotentieel

4.3.4 Governance kosten (incidenteel -en structureel)

Naast incidentele kosten brengt een uniforme domeinnaamextensie ook structurele kosten met zich mee, met name voor het onderhouden van de centrale governance. Op basis van het inschattingen van de onderstaande tabel (tabel 3) gaat het om ongeveer €2 miljoen per jaar aan structurele centrale governance kosten. Hierbij kan er gedacht worden aan het dagelijks beheer en de aanvraag -en uitgifte van de uniforme domeinnaamextensie (plus de benodigde infrastructuur).

Samen tellen de structurele en incidentele governance kosten op tot een investering van ruim € 3,5 tot € 4,5 miljoen in het eerste jaar, ruim € 13 miljoen tot €17 miljoen in vijf jaar en €23 miljoen in tien jaar afhankelijk van het gekozen invoeringsscenario.

Volgnr.	Activiteit	Beschrijving	Totaal kosten - 1 jaar	Totaal kosten - 5 jaar	Totaal kosten - 10 jaar
1	**Coordinatie (strategisch - tactisch beheer)**	Kaders & sturing op dienst, doorontwikkeling, regie	€ 80.000,00	€ 400.000,00	€ 400.000,00
2	**Registry – beleid & administratie**	Registratiebeleid uitvoeren + administratie	€ 160.000,00	€ 800.000,00	€ 1.600.000,00
3	**Uitgiftepunt – technisch beheer (infra/DNS/netwerk)**	Systeembeheer + netwerk + DNS-beheer	€ 1.120.000,00	€ 5.600.000,00	€ 11.200.000,00
4	**Uitgiftepunt – softwareontwikkeling & onderhoud**	Portalen + onderhoud (mens/machine) en m2m/API's	€ 320.000,00	€ 1.600.000,00	€ 3.200.000,00
5	**Uitgiftepunt – informatiesystemen/hosting**	Exploitatie van uitgiftepunt componenten (virtuele servers etc.)	€ 80.000,00	€ 400.000,00	€ 800.000,00
6	**Internet DNS (authoritative DNS service)**	Authoritative DNS servers als dienst (gespecialiseerde leverancier)	€ 250.000,00	€ 1.250.000,00	€ 2.500.000,00
7	**Assurance & compliance (BIO, right-to-audit, SOC/IR)**	BIO/assurance, audits, IR/SOC afspraken, leveranciersaudits	€ 0,00	€ 0,00	€ 0,00
8	**Integratie domeinregister (RIO) / overige koppelingen**	Koppeling met domeinregister, beperkte integratiekosten	€ 0,00	€ 0,00	€ 0,00
9	**Eenmalige realisatie uitgiftepunt**	Ontwerp + bouw/implementatie uitgiftepunt	€ 1.000.000,00	-	-
10	**Ondersteuning Implementatieteam**	Praktische onderteuning	€ 640.000,00	€ 3.200.000,00	€ 3.200.000,00
11	**Communicatie campagne**	voor ieder implementatietraject/fase moet er een campagne worden opgestart.	PM	PM	PM
	Subtotaal kosten per jaar (1, 5, 10 jaar)		**€ 3.650.000,00**	**€ 13.250.000,00**	**€ 22.900.000,00**
Optie:	**Opschoning en sanering**				
	Coordinatie	Kwartiermaker	€ 80.000,00	€ 400.000,00	-
	Ondersteuning Implementatieteam opschoning en sanering	Praktische onderteuning	€ 640.000,00	€ 3.200.000,00	-
	Subtotaal saneren en opschonen (1 tot 5 jaar)		**€ 720.000,00**	**€ 3.600.000,00**	-
	Totale kosten (incl saneren en opschonen)		**€ 4.370.000,00**	**€ 16.850.000,00**	**€ 22.900.000,00**

Tabel 3 - Governance: structurele -en incidentele kosten

Bij deze bedragen is wel van belang dat eerdere ramingen, zoals die van ICTU en de VNG, inmiddels enkele jaren oud zijn. Door gestegen lonen, hogere tarieven en zwaardere eisen aan beveiliging en continuïteit ligt het voor de hand dat vergelijkbare kosten nu hoger kunnen uitvallen dan in die eerdere analyses.

4.3.5 Kansen voor structurele kostenbesparingen

Invoering van een uniforme domeinnaamextensie en een goede governance helpt de Rijksoverheid om in control te komen op de huidige ongecontroleerde aanwas van steeds nieuwe domeinen, waardoor de mogelijkheid ontstaat om structureel kosten te besparen. Daarvoor is actieve sturing nodig op opschoning, bijvoorbeeld op basis van lifecyclemanagement, natuurlijk verloop en het kritische beoordeling of de bestaande domeinen daadwerkelijk bijdragen aan het doel waarvoor ze ooit in het leven zijn geroepen. Dit sluit aan bij de bevindingen uit de verdiepingssessies, waarin onder meer DPC en Rijkswaterstaat aangeven dat de huidige wildgroei alleen echt vermindert als daar ook echt op wordt gestuurd. Met goede governance en sturing verdient het traject

zichzelf op de langere termijn terug. Een goed voorbeeld is het Verenigd Koninkrijk waar de extensie in 2012 is ingevoerd en centrale overheidsinformatie en dienstverlening sinds 2021 rigoureus is gesaneerd tot enkel het gov.uk platform op basis van open standaarden. Deze aanpak heeft inmiddels al meer dan 4 miljard pond aan besparingen opgeleverd.

Daarnaast zijn maatschappelijke baten te verwachten. Hoe meer de extensie wordt toegepast, hoe beter het publiek kan worden uitgelegd hoe domeinnamen (en op termijn logischerwijs ook functionele e-mails) van de overheid, te beginnen met de Rijksdienst, herkend kunnen worden. Dit zal het aantal gedupeerden van imitatie of malafide websites doen afnemen en de daaruit voortkomende schade beperken. Tegelijkertijd kan dankzij een uniforme extensie het risico op misinformatie of desinformatie, zogenaamd uit naam van de overheid, worden beperkt.

4.3.6 Kosten *.gov.nl versus *.overheid.nl

Financieel is het verschil tussen .gov.nl en .overheid.nl te verwaarlozen. De grootste kosten zitten niet in de extensie zelf, maar in de eenmalige migratie van websites en ketens, en in zaken als governance, certificaatbeheer, redirects en communicatie. Wel is de verwachting dat een keuze voor .overheid.nl aan de voorkant meer voorbereiding vraagt en een langere doorlooptijd heeft, omdat deze extensie (anders dan .gov.nl) nog niet als public suffix is ingericht.

4.3.7 Samenvattend

Het financiële beeld laat zien dat invoering van een uniforme domeinnaamextensie weliswaar een forse initiële investering vraagt, maar tegelijk ook een groot structureel besparingspotentieel blootlegt wanneer migratie wordt benut om het webportfolio fundamenteel op te schonen. De analyses laten zien dat de financiële opgave sterk kan afnemen wanneer alleen die websites worden behouden die vanuit taak, bereik of noodzaak in stand moeten blijven (ongeveer € 24,4 miljoen bij gematigde migratie en ongeveer € 17,8 miljoen bij minimale migratie, tegenover ongeveer € 49,6 miljoen bij volledige migratie). Tegelijkertijd kunnen de structurele besparingen aanzienlijk oplopen wanneer verouderde, dubbele of niet-noodzakelijke websites en domeinen actief worden uitgefaseerd (ongeveer € 22,7 miljoen tot € 28,6 miljoen per jaar).

Daarnaast wijzen de analyses erop dat in theorie ook een nog verdergaande saneringsslag denkbaar is (tot ongeveer 77% reductie van het webportfolio). Daarmee wordt onderstreept dat de grootste financiële winst niet primair zit in de keuze tussen .gov.nl en .overheid.nl, maar in het daadwerkelijk terugbrengen van het aantal websites en domeinen, in combinatie met centralere sturing en beheer.

4.4 Communicatie

De maatschappelijke kernwaarde van een uniforme domeinnaamextensie is herkenbaarheid; daarom is communicatie niet ondersteunend maar een noodzaak. Ecorys [6] stelt dat burgers (en ondernemers) nu vaak weinig houvast hebben om echte overheidscommunicatie te herkennen; dit leidt tot verkeerde beoordelingen en ongewenste effecten bij informatie en transacties.

Centerdata [10] toont dat een uniforme extensie de herkenning verbetert en dat een uitgebreide uitleg over de betekenis van de extensie het effect vergroot. Daarmee is

"communicatie over de extensie" niet optioneel, maar een expliciete randvoorwaarde voor het realiseren van de baten.

De verdiepingssessies maken duidelijk hoe kwetsbaar de transitieperiode is vanuit gebruikersperspectief. Rijkswaterstaat en Dictu benoemen dat de grootste uitdaging niet techniek is, maar het publiek: bookmarks, oude links en veranderende vindbaarheid maken dat burgers (en ondernemers) (tijdelijk) hun weg kunnen kwijtraken. Daarmee wordt het risico reëel dat de overgang zélf tot onzekerheid leidt, precies op het thema dat de extensie moet verbeteren.

Dit sluit aan bij de waarschuwing van KvK dat migraties bijna altijd tijdelijke daling in vindbaarheid geven en dat herstel weken tot een halfjaar kan duren, mede afhankelijk van externe links en kwaliteit van de redirects.

Logius/KOOP brengt hier een concreet communicatief ontwerp voor in: een centrale landingspagina (vergelijkbaar met "het Oostenrijks-model[29]") waarop burgers (en ondernemers) kunnen zien welke organisaties al om zijn en waar zij betrouwbare links kunnen vinden, zodat men niet alleen afhankelijk is van zoekmachines. Daarnaast wordt het gebruik van consistente visuele elementen genoemd (banners/balkjes) gedurende de transitie.

Dit is belangrijk omdat Centerdata en Kantar [10] [3] laten zien dat burgers (en ondernemers) niet alleen naar domein kijken maar ook op andere (soms foutieve) heuristieken vertrouwen (logo, taal, reclames, "slotje"), wat in de transitieperiode tot nieuwe misinterpretaties kan leiden.

Een tweede communicatief spanningsveld is de relatie tussen web en e-mail. PBLQ [5] laat zien dat e-mailuniformering vaak niet integraal wordt doorgevoerd in andere landen, maar de Nederlandse sessies benadrukken dat burgers (en ondernemers) web- en e-maildomeinen wél als één geheel ervaren. Logius/KOOP stelt expliciet dat het verwarrend kan zijn als een burger mail krijgt van @logius.nl terwijl de website logius.gov.nl is. Het NCSC onderschrijft dat web en e-mail per merk in samenhang moeten worden beschouwd voor vertrouwen. Dit vraagt om een expliciete communicatiestrategie: óf duidelijk uitleggen dat e-mail anders blijft, óf gefaseerd per merk web en functionele e-mailstromen alignen.

Verder raakt communicatie ook ketenpartners. De Belastingdienst en Logius/KOOP benoemen dat veel externe partijen verwijzen of koppelen naar rijksdomeinen (MKB-sites, medeoverheden via EnableU/RINIS), en dat wijzigingen daarom communicatie en afstemming vereisen richting ketenpartners. Voor gemeenten wordt dit nog pregnanter: de VNG [4] benoemt dat gemeenten veel externe leveranciers en ketenpartners hebben en dat de impact groot wordt als de scope breed is; communicatie en aanpassing van uitingen (online/offline) vormen een substantieel onderdeel van de uitvoeringslast.

De communicatiestrategie kan worden geconcentreerd op banners/ berichtgeving op de websites die voor migratie in aanmerking komen, zo mogelijk ondersteund op een centrale website waar de voortgang van de migratie inzichtelijk wordt gemaakt, onder verwijzing naar het Register Internetdomeinen én de Digihulplijn voor snelle persoonlijke hulp en ondersteuning.

[29] Het centrale platform: Oesterreich.gv.at

Randvoorwaarden voor communicatie kunnen daardoor scherp worden geformuleerd:

- Een rijksbrede communicatiecampagne die uitlegt wat de extensie betekent, hoe burgers (en ondernemers) moeten controleren, en hoe de transitie eruitziet.
- Een "bewegwijzering"-concept (landingspagina, register, centrale uitleg, banners, ondersteuning) dat tijdens de overgang de onzekerheid minimaliseert.
- In de toekomst, wanneer functionele e-mail in beeld komt, een eenduidige boodschap over het *slotje/HTTPS* en wat de overheid wel/niet doet in e-mails (Kantar, Ecorys) [3] [6].
- Communicatie naar ketenpartners (medeoverheden, leveranciers, verwijzers) en beheerste overgangsduur voor redirects.

4.4.1 Publiekscommunicatie / campagne

Gelet op het feit dat een snelle migratie technisch onmogelijk is, kan overwogen worden net als bijvoorbeeld in Tsjechië te kiezen voor een low-impact communicatiestrategie waarbij het publiek via een persbericht wordt geïnformeerd over de uniforme extensie en de scope van invoering (websites van de Rijksdienst zijn in de toekomst niet alleen te herkennen aan het Rijkslogo maar ook aan de extensie). Een eerste communicatiemoment kan het moment van een formeel invoeringsbesluit zijn. Nadat organisaties binnen scope bepaald hebben welke domeinen voor migratie in aanmerking komen, kunnen op websites met meer complexe functionaliteit banners worden geplaatst met de boodschap dat het webadres gaat veranderen. Eenvoudige websites kunnen na omzetting gebruik maken van redirects, waarbij het oude adres nog enige tijd doorverwijst naar het nieuwe adres. In communicatie kan worden verwezen naar het RIO als snelle checkmogelijkheid op de echtheid van een domeinnaam en de Digihulplijn voor extra ondersteuning.

Op moment dat centrale websites zoals rijksoverheid.nl, overheid.nl en digitaleoverheid.nl onder de uniforme domeinnaamextensie komen zou het publiek breder geïnformeerd kunnen worden over de lopende transitie. Naar voorbeeld van bijvoorbeeld Oostenrijk kan verkend worden of het mogelijk is vanuit centrale websites door te verwijzen naar uitvoerders die niet onder de Rijksdienst vallen, zodat de centrale aanlandingspagina's voor overheidsinformatie en dienstverlening in publiekscommunicatie over de extensie centraal komen te staan.

4.4.2 Behoud van vindbaarheid in zoekmachines bij invoering van een nieuwe extensie

Bij het doorvoeren van een nieuwe extensie is een zorgvuldige voorbereiding nodig om de vindbaarheid in zoekmachines zo goed mogelijk te behouden. Allereerst moet een volledig overzicht worden gemaakt van alle bestaande URL's, zodat duidelijk is welke pagina's onder de nieuwe extensie beschikbaar moeten komen en welke redirects nodig zijn. Daarbij is het belangrijk om content, pagina-opbouw en URL-structuur in eerste instantie zoveel mogelijk gelijk te houden. Inhoudelijke wijzigingen of opschoning kunnen beter pas na de overgang plaatsvinden.

Daarnaast is een nulmeting nodig van de huidige prestaties in zoekmachines, zoals de belangrijkste zoekwoorden, best bezochte pagina's en het organisch verkeer. Deze meting is nodig om de effecten van de extensiewijziging later goed te kunnen beoordelen. Daarbij moet rekening worden gehouden met een tijdelijke terugval in

vindbaarheid. Die is bij een extensiewijziging moeilijk volledig te voorkomen, maar met een zorgvuldige aanpak wel te beperken.

De nieuwe website moet vervolgens als exacte kopie van de bestaande website worden ingericht onder de nieuwe extensie. Zolang deze omgeving nog niet live is, moet worden voorkomen dat zoekmachines deze al indexeren. Daarna kunnen redirects worden ingesteld en getest. Ook moeten canonical tags en interne links worden gecontroleerd, zodat zoekmachines en gebruikers direct naar de juiste pagina's worden geleid. Tot slot is het wenselijk om een XML-sitemap op te stellen en het nieuwe domein toe te voegen aan Google Search Console, zodat zoekmachines de overgang sneller kunnen verwerken.[30]

4.4.3 AI training en verificatie

Domain filtering is een manier waarop Large Language Models (LLM's) worden getraind en bepaalde 'categorieën' van betrouwbaarheid/authenticiteit kunnen worden opgesteld. Een uniforme domeinnaamextensie helpt de overheid om gemakkelijk gerichte selecties te maken van domeinen waarop modellen getraind kunnen worden.

Daarnaast helpt een domeinnaamextensie in het verificatieproces als één van de indicaties om betrouwbaarheid van domeinen in te schatten. In systeemprompts kan worden meegenomen dat eerst gekeken moet worden naar informatie op websites met een domeinnaamextensie. Het wordt simpelweg makkelijker om te filteren en prioriteren, ook voor AI.

4.4.4 Communicatie *.gov.nl versus *.overheid.nl

Ook op het gebied van communicatie is het verschil tussen .gov.nl en .overheid.nl beperkt, maar wel relevant. De extensie .overheid.nl sluit intuïtief beter aan bij wat burgers (en ondernemers) direct begrijpen. Deze variant sluit ook nauw aan bij bestaande centrale websites zoals (rijks)overheid.nl, mijn.overheid.nl. en ondernemersplein.overheid.nl. Dat is meteen een belangrijk voordeel. Omgevingen die nu al .overheid.nl gebruiken, kunnen bij invoering van een .overheid.nl-extensie in beginsel ongewijzigd blijven. Dat beperkt de impact op naamgeving, herkenbaarheid en communicatie voor deze groep.

Bij een keuze voor .gov.nl verandert dit wel. Dan moeten ook bestaande centrale omgevingen met .overheid.nl een nieuwe plek krijgen, bijvoorbeeld in de vorm van overheid.gov.nl. Dat levert compactere namen op, maar vraagt ook om een duidelijkere overgang vanuit de huidige situatie. Juist bij centrale websites is die naamgevingsvraag relevant, omdat daar herkenbaarheid en duidelijkheid extra zwaar wegen.

.gov.nl is daarnaast korter en minder gevoelig voor typosquatting en look-alikes. Dat is ook vanuit communicatieperspectief een voordeel, zoals uit publieksonderzoek van Centerdata [10] is gebleken. Verder past .gov.nl beter in de lijn van landen om Nederland heen, waar .gov-varianten al langer worden gebruikt. Welke variant ook wordt gekozen, duidelijke uitleg tijdens de overgang blijft nodig. Dat geldt zeker wanneer meerdere extensies langere tijd naast elkaar blijven bestaan.

[30] Zie bijlage: Stappenplan behoud vindbaarheid zoekmachines (indexering)

Sommige partijen stellen voor om de extensies .overheid.nl én .gov.nl naast elkaar te laten bestaan. Uit eenduidigheid, transparantie- en communicatieoverwegingen lijkt het verstandiger om één extensie te kiezen en deze consequent toe te passen.

4.4.5 Samenvattend

Samenvattend geldt dat communicatie een bepalende randvoorwaarde is voor het succes van een uniforme domeinnaamextensie. De maatschappelijke meerwaarde van de extensie zit vooral in betere herkenbaarheid en transparantie voor burgers en ondernemers. Tegelijkertijd is de overgangsperiode kwetsbaar, omdat oude en nieuwe domeinen tijdelijk naast elkaar kunnen bestaan en dit tot verwarring kan leiden. Ongeacht de keuze voor .gov.nl of .overheid.nl zijn daarom duidelijke uitleg, centrale bewegwijzering en goede afstemming met ketenpartners nodig.

4.5 Governance en beheer

4.5.1 Omvang en versnippering van het domeinportfolio

De Rijksoverheid beschikt op dit moment over een omvangrijk en versnipperd domeinportfolio. Op basis van de huidige inventarisatie van het DNS-landschap gaat het om ongeveer 10.000 domeinnamen die onder verantwoordelijkheid van de Rijksoverheid vallen, verdeeld over verschillende topleveldomeinen (TLD's)[31] (waarvan ongeveer 8.400 onder .nl en kleinere aantallen onder .com, .eu, .org, .info, .net en enkele andere extensies).[32]

Van deze 10.000 domeinen worden ongeveer 8.500 domeinnamen "in eigen beheer" gehouden door rijksorganisaties en hun interne/shared-service-providers, en ongeveer 1.500 domeinnamen via meer dan dertig commerciële partijen beheerd. De grootste interne DNS-dienstverleners zijn op dit moment: AZ/DPC (~ 6.400 domeinen), SSC-Campus (~ 650), Belastingdienst (~ 450), DICTU (~ 450) en SSC-ICT (~225 domeinen). Daarnaast zijn er kleinere blokken bij onder andere DUO, Defensie, KvK, CBS en RDW, en een lange "staart" van commerciële DNS-providers zoals KPN, Cloudflare, Amazon, Argeweb, Solvinity en Akamai.[33]

Dit beeld bevestigt de conclusie uit de technische impactanalyse van ICTU: het huidige DNS-landschap van het Rijk is sterk versnipperd, met meerdere grote interne operators en een substantieel aantal uitbestede domeinen, elk met eigen beheerprocessen, tooling en beveiligingsniveau [8].

4.5.2 Rol van DPC en het huidige domeinnaambeleid

Binnen dit landschap vervult Dienst Publiek en Communicatie (DPC) een centrale rol. DPC is deelnemer bij SIDN (registrar) en fungeert als houder (registrant) van alle domeinnamen van de Rijksoverheid. Het bestaande domeinnaambeleid is primair gericht op het centraal registreren van rijksdomeinen; DPC publiceert maandelijks een overzicht van alle publieke rijkswebsites in het Websiteregister Rijksoverheid.[34]

---

[31] Een topleveldomein (TLD) is het laatste deel van een internetdomeinnaam, direct achter de laatste punt (bijv. .nl, .com, .org). Het is het hoogste niveau in de hiërarchie van het Domain Name System (DNS) en geeft vaak het type organisatie of landcode aan.
[32] Inventarisatie DNS-landschap Rijksoverheid / DNS-inrichting AZ/DPC, 2024.
[33] Inventarisatie DNS-landschap Rijksoverheid / DNS-inrichting AZ/DPC, 2024.
[34] BZK/DPC, Domeinnaambeleid Rijksoverheid en Websiteregister Rijksoverheid.

De huidige DNS-inrichting laat zien dat DPC op dit moment:

- Als registrar optreedt voor ongeveer 5.400 domeinnamen ten behoeve van departementen, agentschappen en ZBO's;
- Eigenaar/beheerder is van ongeveer 550 domeinnamen die vooral direct aan AZ/DPC zijn gelieerd;
- Daarnaast ongeveer 450 domeinnamen beheert die verbonden zijn aan het PRO-platform;
- In totaal ongeveer 6.400 domeinnamen in DNS beheert [14].

Daarmee is DPC de grootste DNS-operator binnen de Rijksoverheid. Tegelijkertijd is het mandaat van DPC in de huidige situatie primair uitvoerend en adviserend: DPC registreert en beheert domeinnamen namens de rijksoverheid, maar heeft beperkt formeel gezag om naamgeving, gebruik en beveiligingsniveau rijksbreed af te dwingen. Dit komt ook naar voren in het buitenlandonderzoek van PBLQ [5], waarin wordt beschreven dat het Nederlandse domeinnaambeleid binnen de Rijksoverheid vooral gericht is op centrale registratie, niet op een strikte, verplicht doorvertaalde naamgevingsconventie of governance voor alle uitvoerders. Het domeinbeheer steunt sterk op domein-liaisons per organisatie, maar daar zitten problemen: te weinig kennis, lage prioriteit en beperkte kwaliteit, wat bijdraagt aan wildgroei en beperkte grip.

Ook is het overzicht van domeinregistraties (webregister) niet sluitend. DPC en Bureau Forum Standaardisatie noemen dat een deel van domeinen niet bij DPC is geregistreerd en dat er hoogstwaarschijnlijk een aanzienlijk aantal "unknown unknowns" bestaat, wat toezicht en sturing ingewikkeld maakt.

Technisch is er wel al een robuuste basis: DPC gebruikt Anycast DNS en komt goed uit tests, maar de sessies benadrukken dat bij een domeinnaamextensie (.gov.nl) de eisen aan robuustheid, redundantie en governance scherper worden omdat je een zeer zichtbare laag creëert.

SIDN is in de huidige situatie *registry* voor het .nl domein. Uit overleg met SIDN komt naar voren dat het invullen van een vergelijkbare registry rol voor de Rijksoverheid (en overheid) voor hen technisch uitvoerbaar is, maar dat de kernvraag governance is: welke rollen en rechten, welk beleid, en wat valt wel/niet onder de extensie.

De voorwaarden waaronder overheidsorganisaties gebruik kunnen maken van de uniforme domeinnaamextensie dienen expliciet te worden vastgelegd in het Internetdomeinbeleid. In twijfelgevallen zou een naamgevingsautoriteit de bevoegdheid kunnen krijgen om een beslissend oordeel over domeinnaamgeving te vellen.

4.5.3 Decentraal DNS-beheer bij departementen, uitvoerders en leveranciers

Naast de centrale rol van DPC is er een breed veld van decentrale DNS-operators. Organisaties als Dictu, Belastingdienst, SSC-Campus, SSC-ICT, DUO, Defensie, RDW, CBS en KvK beheren hun eigen DNS-infrastructuur, met eigen nameservers en configuraties. De huidige DNS-inrichting laat bijvoorbeeld nameservers zien als ns1.ssonet.nl, ns2.dictu.nl, ns3.belastingdienst.nl, ns1/2.ssc-campus.nl etc., gekoppeld aan honderden domeinen per provider [14].

Daarnaast bevinden circa 1.500 domeinnamen zich bij meer dan 30 commerciële partijen, waaronder KPN, Cloudflare, Amazon, Argeweb, Solvinity en Akamai. De governance van deze domeinen is vastgelegd in individuele contracten en SLA's tussen

de betreffende rijksorganisatie en de leverancier; er is hiervoor geen één overkoepelend rijksbreed DNS-kader [8] [14].

In de ICTU-analyse wordt benadrukt dat het inrichten van een betrouwbare DNS-infrastructuur gespecialiseerde expertise vraagt en dat DNS feitelijk een nutsvoorziening en onderdeel van de vitale infrastructuur is. Tegelijkertijd constateert ICTU dat de huidige DNS-inrichting sterk is verspreid over verschillende operators en dat dit het centraal borgen van integriteit, beschikbaarheid, logging en security-maatregelen bemoeilijkt [8].

4.5.4 Governance-niveaus: strategisch, tactisch en operationeel

In het huidige DNS-beheer wordt expliciet onderscheid gemaakt tussen strategisch, tactisch en operationeel niveau.

- Op strategisch niveau wordt het domeinnaambeleid vastgesteld (VoRa/DPC), in samenhang met bredere beleidskaders voor digitale overheid, internetveiligheid en digitale soevereiniteit. Aanbevelingen van onder andere Forum Standaardisatie, NCSC en de BIO vormen hier de technische en security-baseline [8].
- Op tactisch niveau wordt per grote DNS-operator (DPC, DICTU, SSC-Campus, Belastingdienst, etc.) bepaald hoe de DNS-dienst is ingericht: architectuur, security-instellingen (DNSSEC, CAA-records, logging, monitoring), portfoliobeheer van domeinen en aansluiting op interne processen.
- Op operationeel niveau vindt het dagelijkse beheer plaats: het aanmaken en wijzigen van DNS-records, het doorvoeren van migraties en redirects, het oplossen van storingen en het analyseren van incidenten.

In de praktijk betekent dit dat de strategische kaders (relatief) centraal zijn belegd, maar dat het tactische en operationele beheer grotendeels bij individuele dienstverleners en organisaties ligt, met uiteenlopende implementaties en volwassenheidsniveaus.

4.5.5 PRO als gedeeltelijk gecentraliseerde platformvoorziening

Binnen dit brede en versnipperde landschap vormt het Platform Rijksoverheid Online (PRO/PRO2) een belangrijke, maar niet dekkende, centraliserende factor. PRO is een door DPC beheerd webplatform waarop een groot aantal rijkswebsites draait, waaronder rijksoverheid.nl (het gedeelde platform van de twaalf ministeries) en diverse andere sites van departementen, uitvoeringsorganisaties en samenwerkingsverbanden. PBLQ duidt rijksoverheid.nl expliciet als een platformoplossing binnen het domeinnaambeleid, waarbij DPC de techniek, doorontwikkeling, beheer en beveiliging van het platform verzorgt, terwijl aangesloten organisaties verantwoordelijk blijven voor de inhoud [8]. [35]

De organisatorische scope van rijksoverheid.nl is beperkt tot de ministeries, maar uitvoeringsorganisaties kunnen via PRO eigen sites laten draaien met hetzelfde ontwerp en technische fundament. PBLQ constateert dat een deel van de uitvoerders hiervan gebruikmaakt, maar dat de meerderheid van de uitvoeringsorganisaties en ZBO's nog eigen, niet-aan-PRO gekoppelde sites beheert [5].

Ook aan de DNS-kant is PRO slechts een deel van het geheel: de huidige DNS-inrichting laat zien dat ongeveer 450 domeinen direct aan PRO zijn verbonden en in DNS door AZ/DPC worden beheerd. Dat betekent dat PRO een substantieel, maar beperkt segment

[35] DPC, documentatie Platform Rijksoverheid Online (PRO/PRO2).

van de rijksdomeinen omvat; het grootste deel van de ongeveer 10.000 domeinnamen draait (DNS-technisch) buiten PRO, bij andere interne of externe operators [14].[36]

4.5.6 Centraal uitgiftepunt, gedelegeerd DNS model

Uit de verdiepingssessies komt een gewenste governance naar voren waarin beleid, uitgifteproces en toezicht centraal worden verankerd, terwijl technische uitvoering robuust en schaalbaar wordt ingericht. Zowel DPC en Bureau Forum Standaardisatie als SIDN benoemen dat de registry-functie voor .gov.nl logisch bij SIDN kan liggen, omdat SIDN die rol nu ook voor .nl (ook: .politie, .amsterdam, etc.) vervult en over schaalbare DNS-infrastructuur en expertise beschikt. Het NCSC ondersteunt het verkennen van SIDN als registry eveneens expliciet vanwege expertise, schaal en potentieel hergebruik van infrastructuur.

Als "meest vanzelfsprekend" worden de volgende uitgangspunten benoemd:

- **BZK als beleidseigenaar**: beleidsafspraken rondom de uniforme domeinnaamextensie beleidsmatig verankeren in het internetdomeinbeleid, inrichting van mandaat en toezicht/handhaving, bepalen toelatingscriteria, naamgevingsconventies, instellen van een centrale naamgevingsautoriteit.
- **DPC als centrale registrar**: spil in het aanvraag en uitgifteproces en borgen dat nieuwe aansluitingen voldoen aan beleid (bijv. PTOLU) vanaf een "schone lei".
- **SIDN als registry** voor .gov.nl: zonebeheer en technische stabiliteit/robuustheid, inclusief governance rond rollen en rechten. SIDN geeft aan dat met hun nieuwe systeem Hello Registry (per 1 september 2026) het opzetten van de extensie technisch goed te doen is, maar dat heldere beleidsafspraken (naamgeving, scope, registratieprincipes) randvoorwaardelijk zijn voor de effectiviteit.
- **Gedelegeerd DNS model**: grote organisaties kunnen, binnen centrale kaders, eigen subdomeinen en (eventueel) eigen DNS-inrichting beheren, zodat autonomie mogelijk blijft waar dat nodig is en single point of failure-risico's worden beperkt. DPC, Bureau Forum Standaardisatie en Logius/KOOP benoemen dit als logisch pad. De Belastingdienst en andere grote partijen hebben eigen infrastructuur en behoefte aan autonomie.

4.5.7 Aanvraag en uitgifteproces

In een eerdere verkenning naar de mogelijkheden voor invoering van een uniforme domeinnaamextensie zijn de volgende processtappen geïdentificeerd:

Aanvraag:

1. Aanvrager maakt duidelijk welke organisatie het betreft (bij voorkeur op basis van het Register Overheidsorganisaties), wie contactpersoon is en wat de contactgegevens zijn.
2. Aanvrager geeft aan welk(e) subdomein(en) worden aangevraagd.
3. Aanvrager geeft aan welke diensten worden ontsloten (website, e-mail, anders)
4. Aanvrager geeft aan welke organisatie het DNS beheer verzorgt. Nameservers dienen aan alle voor overheidsdomeinen verplichte eisen te voldoen, waaronder IPv6 en DNSSEC (zie http://eisenrijkswebsites.nl/ voor een overzicht). Bij gebruik van eigen

[36] DPC, documentatie Platform Rijksoverheid Online (PRO/PRO2).

nameservers dienen DNS-records van een (de) subdomein(en) te worden aangeleverd t.b.v. de activatie van DNSSEC in de DNS-zone van de uniforme domeinnaamextensie.
5. De aanvrager geeft aan per welke datum het domein beschikbaar dient te zijn.

Uitgifte:

1. DPC beoordeelt of aanvrager bevoegdheid heeft om de uniforme domeinnaamextensie te beheren/gebruiken.
2. DPC beoordeelt de contactgegevens op volledigheid en bruikbaarheid.
3. DPC beoordeelt of de aanvraag voldoet aan naamgevingsconventies en gebruiksdoel.
4. DPC beoordeelt of de nameservers/DNS-instellingen bekend zijn. En of in geval van eigen nameservers de DNS-records ontvangen en gepubliceerd zijn en de datum waarop de nameservers/DNS-instellingen werden getest.
5. DPC onderzoekt welk certificaat gewenst is.
6. DPC gaat na of e-mail moet worden toegestaan en wie e-mail beheer doet.
7. DPC keurt de aanvraag goed of af. (NB bij onduidelijkheid dient domeinnaamgeving te worden beoordeeld door bijvoorbeeld een onafhankelijke naamgevingsautoriteit).
    a. Indien goedgekeurd wordt het nieuwe/gewijzigde domein opgenomen in het Register Internetdomeinen Overheid (RIO).

Bij invoering van een uniforme domeinnaamextensie binnen de Rijksoverheid kan DPC voorlopig dezelfde rol blijven innemen die het nu heeft. In geval van verdere verbreding richting de medeoverheden dient onderzocht te worden of een andere uitvoeringsorganisatie binnen de Rijksoverheid een meer geëigende plek is om overheidsbrede aanvragen af te handelen. Dan zou ook (gedeeltelijke) automatisering van het aanvraag en uitgifteproces voor de hand liggen.

4.5.8 Naamgeving, defensieve registraties en overgangsafspraken

SIDN benadrukt dat uniformiteit staat of valt met duidelijke naamgevingsconventies en keuzes rond afkortingen versus volledige namen. Een pragmatische oplossing die SIDN noemt is volledige naam registreren en redirecten naar een voor de hand liggende afkorting, maar dit vraagt beleidskeuzes. Aanvullend adviseren zij ook om defensieve registraties zoveel mogelijk te beperken en vooral gecontroleerd de oude .nl-domeinen te laten verwijzen naar de nieuwe domeinen (met de uniforme domeinnaamextensie).

DPC waarschuwt dat te harde centrale sturing op naamgeving draagvlak kan schaden; governance moet dus enerzijds mandaat hebben, anderzijds bestuurlijk werkbaar zijn.

4.5.9 Veiligheid

SIDN stelt expliciet: een nieuwe extensie is niet “waterdicht” voor veiligheid. Het draagt niet automatisch bij aan centraal certificaatbeheer; de winst zit vooral in herkenbaarheid en in het feit dat je bij nieuwe aansluitingen met een schone lei beleids- en beveiligingseisen kunt afdwingen. SIDN benoemt tevens dat je op second level domeinnaam-niveau meer kunt sturen (bijv. op mailserverbeleid) dan op .nl als geheel, maar dat phishingdomeinen buiten de extensie altijd mogelijk blijven (bijv. goF.nl of .overhe1d.nl).

Zoals eerder aangegeven adviseert het NCSC een keuze voor .gov.nl.[37] Omdat de DNS infrastructuur van gov.nl (of overheid.nl) kritieke infrastructuur wordt zodra de uniforme

[37] Paragraaf 4.2, zie: functionele e-mail, technische aansluitvoorwaarden.

domeinnaamextensie meer gebruikt zal worden, is het belangrijk dat het aan de nodige standaarden zoals DNSSEC, RPKI, etc. voldoet. Domeinnaam monitoring diensten van SIDN zouden gebruikt kunnen worden om nieuw geregistreerde, mogelijk malafide domeinen op te sporen. Domein expiratie is mogelijk, echter in de nieuwe situatie is het niet mogelijk voor een kwaadwillende om na het verlopen van een subdomein (van gov.nl of overheid.nl) dit subdomein op te kopen. Zelfs al zou het subdomein op een gegeven moment niet meer gebruikt worden. Hierdoor kan een Man-in-the-Middle aanval (MitM), op basis van het registreren van een (sub)domein door een kwaadwillende, niet meer plaatsvinden.

4.5.10 Governance *.gov.nl versus *.overheid.nl

Ook voor governance en beheer is het verschil tussen .gov.nl en .overheid.nl beperkt, maar wel relevant. In beide gevallen blijven duidelijke centrale kaders nodig voor naamgeving, toewijzing, uitzonderingen, mandaat en toezicht. Een keuze voor .gov.nl sluit beter aan op het model waarin DPC de centrale beleids- en registrar rol vervult en SIDN de logische registry-partij is. Een keuze voor .overheid.nl verandert die hoofdstructuur niet wezenlijk, maar sluit wel beter aan op een deel van de bestaande centrale naamgeving. In beide gevallen blijft een model met centrale regie en gedelegeerde uitvoering het meest logisch. Zonder die combinatie blijft het risico bestaan dat de huidige versnippering in stand blijft.

4.5.11 Samenvattend

- De Rijksoverheid beschikt over ongeveer 10.000 domeinnamen, waarvan het grootste deel onder .nl valt en circa 1.500 bij commerciële DNS-providers is ondergebracht [14].
- DPC is centrale registrar en grootste DNS-operator (~6.400 domeinen), verantwoordelijk voor het domeinnaamregister en het PRO-platform, maar met een mandaat dat in de praktijk vooral uitvoerend en adviserend is [5] [14]. [38]
- Grote uitvoerders en shared-service-organisaties beschikken over eigen DNS-infrastructuren, waarmee het tactische en operationele beheer van DNS sterk decentraal is georganiseerd [8][14]. Bij invoering van een uniforme domeinnaamextensie heeft een gedelegeerd DNS model de voorkeur. Onderzocht kan worden of SIDN in dit model een rol als registry kan spelen. DPC zou in een dergelijk model de registrar rol kunnen blijven invullen.
- PRO/PRO2 biedt een gecentraliseerde platformvoorziening voor een deel van de Rijkswebsites (met centrale techniek, beveiliging en domeinnaambeheer via DPC), maar dekt slechts een deel van het totale Rijkswebportfolio; veel uitvoerders, portalen en campagnes draaien buiten PRO [5]. [39]
- Vanuit technische en security-optiek wordt DNS door ICTU en andere partijen gezien als een vitale nutsvoorziening, terwijl de huidige governance en inrichting nog sterk gefragmenteerd is. Invoering van een uniforme domeinnaamextensie maakt Rijksbrede sturing mogelijk op beschikbaarheid, integriteit, beveiliging en opschoning van het domeinportfolio en helpt de Rijksoverheid daarmee in control te komen [8].
- Ten aanzien van de herkenbaarheid geeft SIDN aan dat het mogelijk blijft om websites met imitatie extensies in de lucht te brengen, denk aan .gof.nl of

[38] BZK/DPC, Domeinnaambeleid Rijksoverheid en Websiteregister Rijksoverheid.
[39] DPC, documentatie Platform Rijksoverheid Online (PRO/PRO2).

.overhe1d.nl. Echter invoering maakt monitoring op dit soort imitaties vele malen makkelijker dan de huidige situatie.

Dit hoofdstuk laat zien dat de invoering van een uniforme domeinnaamextensie alleen kansrijk is als governance en beheer centraal en duidelijk worden ingericht. De huidige situatie kent versnippering in domeinbeheer, beperkte centrale sturing en onvoldoende uniformiteit in naamgeving en registratie. Voor een nieuwe situatie zijn daarom heldere kaders nodig voor naamgeving, toewijzing, uitzonderingen, mandaat en toezicht. Daarbij ligt een model met DPC in de centrale beleids- en registrarrol en SIDN als logische registry-partij het meest voor de hand, gecombineerd met gedelegeerde uitvoering waar dat nodig is.

5 Implementatiescenario's

Op basis van opgehaalde informatie worden twee implementatiescenario's voorgesteld.

1. Gefaseerde invoering met een doorloop van maximaal 5 jaar.
2. Gefaseerde invoering met een doorloop van 5 tot maximaal 10 jaar.

Het eerste scenario lijkt vanuit communicatieoverwegingen makkelijker uitlegbaar richting het publiek en noemen we daarom "burger centraal".

Het tweede scenario lijkt vanuit implementatieperspectief beter uitvoerbaar en in te plannen voor organisaties met complexe webportfolio's en noemen we daarom "bedrijfsvoering centraal".

In beide gevallen wordt bekeken hoe in de migratie zoveel mogelijk rekening kan worden gehouden met het lifecyclemanagement of gebruik van specifieke "windows" ofwel geschikte momenten om de transitie naar een extensie in te zetten [13].

In beide scenario's vormt invoering van de uniforme extensie op centrale websites (e.g. Rijksoverheid.nl, Overheid.nl, mijn.overheid.nl en ondernemersplein.nl) het vertrekpunt voor bredere publiekscommunicatie.

5.1 Scenario 1: Burger en ondernemer centraal (centrale aanlandplek krijgt voorrang + beperkte doorlooptijd)

Na het invoeringsbesluit krijgen nieuwe websites vanaf dag één een nieuwe extensie toegewezen conform de spelregels van een aangepast internetdomeinbeleid (via een addendum). Centrale websites krijgen voorrang (redirecten en omzetten) in de migratie. Tegelijkertijd wordt de migratie van weinig complexe websites opgepakt en wordt de gefaseerde omzetting van complexe omgevingen binnen 5 jaar voorbereid en in gang gezet.

In dit scenario ligt de nadruk op herkenbaarheid en publieksvertrouwen door centrale informatieve websites van de Rijksoverheid als eerste zichtbaar onder de uniforme extensie te positioneren. Vanaf het moment van het invoeringsbesluit en aanpassing van het internetdomeinbeleid worden alle nieuwe websites binnen de Rijksoverheid standaard uitgegeven met de uniforme extensie via een centrale aanvraag- en uitgifteproces via Dienst Publiekscommunicatie (DPC). Daarna worden de eenvoudige websites binnen scope (rijkshuisstijl/rijkslogo) versneld omgezet. Tegelijkertijd start de voorbereiding en gefaseerde omzetting van complexe tot zeer complexe websites en portfolio's bij grote uitvoeringsorganisaties (zoals Belastingdienst, RVO en Rijkswaterstaat) op een door

organisaties zelf te bepalen startmoment, met als randvoorwaarde dat de volledige transitie binnen 5 jaar wordt gerealiseerd. De voortgang wordt inzichtelijk gemaakt op een centrale website en via banners op de websites die voor migratie in aanmerking komen en is controleerbaar via het Register Internetdomeinen van de Overheid (RIO). Daarnaast is ondersteuning beschikbaar via de Digihulplijn.

5.1.1 Fasering / uitgangspunten

1. **Invoeringsbesluit**
   Inrichten projectteam, voorbereiden besluitvorming, definitieve keuze extensie en aanpassing internetdomeinbeleid. Mogelijkheid pilots om ervaring op te doen.

2. **Vanaf invoeringsbesluit: alle nieuwe websites Rijksdienst standaard met uniforme extensie**
   Nieuwe domeinnamen met publiek webverkeer worden in principe alleen nog uitgegeven onder de uniforme extensie via het centrale aanvraag- en uitgifteproces (incl. toets op noodzaak/ontsluiting via centrale websites). Het internetdomeinbeleid wordt hierop aangepast. In uitzonderingsgevallen blijven afwijkingen mogelijk. Bij nieuwe aanvragen wordt beoordeeld of de beoogde nieuwe informatie/dienstverlening niet via bestaande centrale websites kan worden ontsloten.

3. **Centrale websites: eerst redirecten, vervolgens omzetten**
   De centrale websites (voor informatie, wegwijzing en dienstverlening) krijgen voorrang: eerst wordt een redirect-domein met de uniforme extensie ingericht (waar dit veilig kan), waarna omzetting naar de nieuwe domeinnaam volgt.

4. **Eenvoudige websites binnen scope: versneld omzetten en waar mogelijk opschonen**
   Eenvoudige, relatief minder complexe websites worden vroeg in het traject omgezet. Waar websites (deels) overbodig zijn of kunnen worden samengevoegd, wordt opschoning meegenomen om beheerlast en kosten te beperken.

5. **Complexe/zeer complexe portfolio's: gefaseerd starten, maar binnen 5 jaar gereed**
   Grote uitvoerders bepalen het meest passende startmoment binnen de 5-jaarstermijn, zodat migratie kan aansluiten op de eigen planning.

6. **Na omzetting: oude domeinen blijven tijdelijk doorverwijzen, daarna uitfaseren**
   Na migratie kan het oude domein nog een afgesproken periode doorverwijzen naar het nieuwe domein, waarna uitfasering/archivering plaatsvindt volgens het domeinnaambeleid.

7. **Transitie-communicatie en controleerbaarheid**
   Tijdens de transitie wordt actief gecommuniceerd via de centrale websites, en kan het publiek (en organisaties) domeinen controleren via het RIO. Waar nodig kan aanvullend een korte toelichting op sites worden geplaatst (bijv. verwijzing naar RIO).

Kernpunten

- Centrale websites worden vroeg als herkenbare aanlandplek onder de uniforme extensie gepositioneerd (eerst redirect, daarna omzetting).
- Alle nieuwe websites binnen scope krijgen direct de uniforme extensie (via centraal uitgifteproces).
- Eenvoudige websites worden versneld omgezet; complexe omgevingen volgen gefaseerd, maar binnen 5 jaar.
- Voortgang is transparant via centrale website en controleerbaar via het RIO.
- Uniform domeinbeleid en robuust DNS-beheer, waar nodig decentraal gekoppeld aan bestaand beheer van organisaties (behoud van eigen verantwoordelijkheid).

Voordelen

- Snelle publiekswaarde: centrale websites kunnen vroeg worden gecommuniceerd als herkenbare en betrouwbare ingang. Het publiek kan in de transitie worden meegenomen door bijvoorbeeld banners te plaatsen op de websites die voor de nieuwe extensie in aanmerking komen, zodat het publiek bij bezoek aan de website geïnformeerd wordt over de komende naamswijziging.
- Beperkte initiële risico's door eerst te starten met centrale en eenvoudige websites.
- LCM-gedreven aanpak blijft mogelijk voor complexe omgevingen, waardoor technische risico's beter beheersbaar zijn.
- Helderder communicatieverhaal dan bij een langer hybride model: er is eerder een "moment" waarop brede publiekscommunicatie kan starten.
- Transparantie: voortgang en geldigheid van domeinen zijn te checken via RIO.

Nadelen

- Meer centrale coördinatie en toezicht nodig (planning, prioritering, support) en daarmee initieel hogere kosten.
- Risico op tijdelijke verwarring door gemixte domeinen tijdens de gefaseerde omzetting; mitigatie vraagt consistente communicatie en RIO-positionering.
- Complexe uitvoerders blijven risicovol: migratie vergt per organisatie maatwerk en kan druk zetten op capaciteit/portfolio-planning.
- Redirects op centrale sites vragen zorgvuldige technische inrichting en beheer (o.a. beveiliging, monitoring, performance).

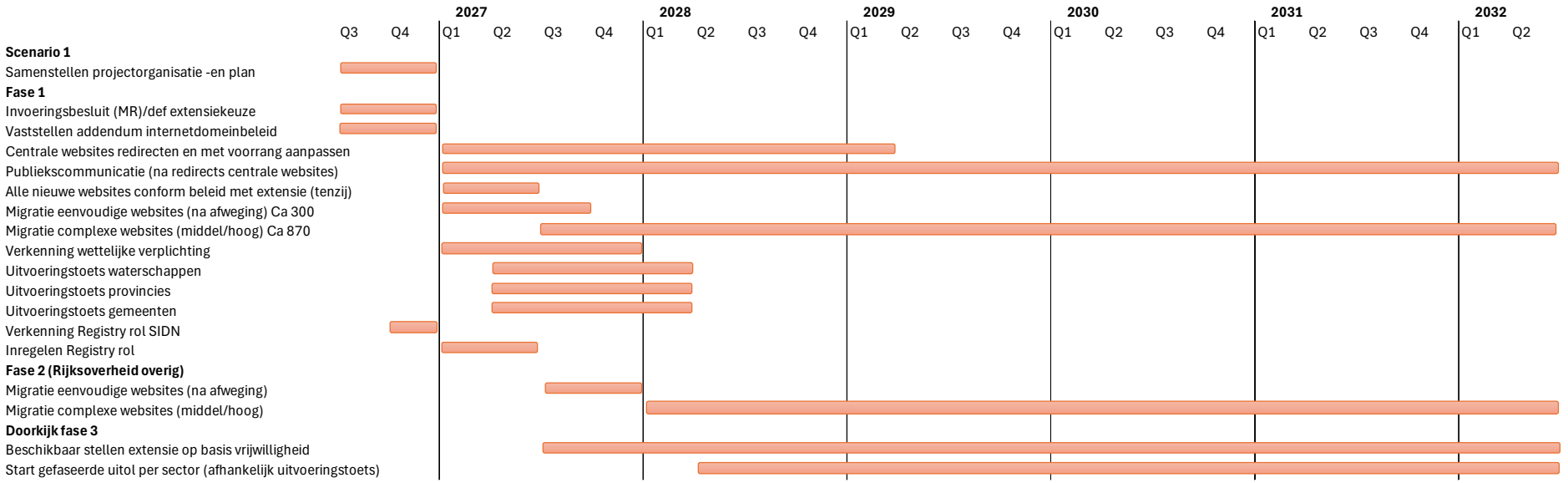
5.1.2 Financiële impact en terugverdientijd

Op basis van de cijfers uit de financiële paragraaf (par. 2.3) is een indicatieve terugverdientijd voor scenario 1 berekend. Daarbij is uitgegaan van een gematigd migratiescenario met ongeveer € 24,4 miljoen aan eenmalige migratiekosten, aangevuld met eenmalige governancekosten van ongeveer € 16,9 miljoen. Daartegenover staat een gematigd saneringspotentieel van ongeveer € 22,8 miljoen per jaar. Op basis van deze uitgangspunten wordt de terugverdientijd van scenario 1 geraamd op **twee tot drie jaar**.

Binnen de totale looptijd van vijf jaar betekent dit dat scenario 1 niet alleen investeringen vraagt, maar ook al tijdens de uitvoering kan omslaan naar financieel

rendement, doordat de structurele besparingen langer doorlopen dan de initiële incidentele kosten.

5.1.3 Planning scenario 1



Opmerking: mogelijk vraagt een invoeringsbesluit ook een aanvullende uitvoeringstoets voor de Rijksoverheid. In dat geval schuift de planning aan de voorkant met een half jaar tot een jaar op.

5.2 Scenario 2: Bedrijfsvoering centraal (klein beginnen, langere doorlooptijd)

Eerst eenvoudige/minder herkenbare websites, daarna centrale websites (publieksmoment later), vervolgens overige complexiteit met doorlooptijd 5–10 jaar

In dit scenario ligt de nadruk op beheersbaarheid en het opbouwen van ervaring door klein te beginnen. Vanaf het invoeringsbesluit worden alle nieuwe websites binnen de Rijksoverheid standaard uitgegeven met de uniforme extensie via het centrale aanvraag- en uitgifteproces. Vervolgens start de omzetting met eenvoudige, relatief minder herkenbare websites. De centrale websites worden pas daarna geredirect en omgezet; dit moment vormt het logische startpunt voor bredere publiekscommunicatie. Tot slot volgt een gefaseerde omzetting van overige eenvoudige, complexe tot zeer complexe websites en portfolio's, waarbij organisaties een passend startmoment kiezen en – afhankelijk van afspraken – een totale doorlooptijd hebben van 5 tot 10 jaar. De voortgang wordt inzichtelijk gemaakt, bijvoorbeeld via banners op de websites die voor migratie in aanmerking komen, en is controleerbaar via het Register Internetdomeinen van de Overheid (RIO). Daarnaast is ondersteuning beschikbaar via de Digihulplijn.

5.2.1 Fasering / uitgangspunten

1. **Invoeringsbesluit**
   Inrichten projectteam, voorbereiden besluitvorming, definitieve keuze extensie en aanpassing internetdomeinbeleid. Mogelijkheid pilots om ervaring op te doen.

2. **Vanaf invoeringsbesluit: alle nieuwe websites Rijksdienst standaard met uniforme extensie**
   Nieuwe domeinnamen met publiek webverkeer worden in principe alleen nog uitgegeven onder de uniforme extensie via het centrale aanvraag- en uitgifteproces (incl. toets op noodzaak/ontsluiting via centrale websites). Het internetdomeinbeleid wordt hierop aangepast. In uitzonderingsgevallen blijven afwijkingen mogelijk. Bij nieuwe aanvragen wordt beoordeeld of de beoogde nieuwe informatie/dienstverlening niet via bestaande centrale websites kan worden ontsloten.

3. **Start met eenvoudige, relatief minder herkenbare websites**
   In de eerste fase wordt ervaring opgebouwd met omzetting van eenvoudige websites, inclusief opschoning waar mogelijk.

4. **Daarna: centrale websites redirecten en omzetten (publiekscommunicatie start later)**
   De centrale websites worden pas omgezet nadat de eerste tranche eenvoudige sites is afgerond of voldoende ervaring is opgedaan. Dit moment wordt benut voor bredere publiekscommunicatie.

5. **Vervolgens: gefaseerde omzetting van overige websites (eenvoudig t/m zeer complex) met 5–10 jaar doorlooptijd**
   Organisaties bepalen een passend startmoment; de totale doorlooptijd kan variëren (bijv. 5 jaar voor departementen/centrale websites en langer voor uitvoerders).

6. **Transitie-communicatie en controleerbaarheid**
   Tijdens de transitie wordt actief gecommuniceerd via de centrale websites, en kan het publiek (en organisaties) domeinen controleren via het RIO. Waar nodig kan aanvullend een korte toelichting op sites worden geplaatst (bijv. verwijzing naar RIO).
7. **Na omzetting: oude domeinen tijdelijk doorverwijzen, daarna uitfaseren**
   Doorverwijzing en uitfasering vinden plaats volgens domeinnaambeleid.
8. **Transitiecommunicatie en controleerbaarheid**
   Tijdens de transitie blijven centrale websites en RIO de basis voor uitleg en controle

Kernpunten

- Beheersbaar opstarten: eerst ervaring met eenvoudige, minder herkenbare websites.
- Centrale websites worden later omgezet; publiekscommunicatie start dus later.
- Nieuwe websites krijgen direct de uniforme extensie via centrale uitgifte.
- Doorlooptijd voor complexe portfolio's kan langer zijn (5–10 jaar), afhankelijk van afspraken.
- Uniform domeinbeleid en robuust DNS-beheer, waar nodig decentraal gekoppeld aan bestaand beheer van organisaties.

Voordelen

- Lagere startcomplexiteit en een geleidelijk leerpad (minder risico in de beginfase).
- Lagere initiële kosten doordat men niet direct met de grootste/complexste omgevingen start.
- Meer ruimte voor organisaties om migratie te koppelen aan eigen lifecycle momenten en ontwikkelingen.
- Het RIO kan vanaf dag 1 als controlemechanisme worden gepositioneerd, ook als centrale websites nog niet omgezet zijn.

Nadelen

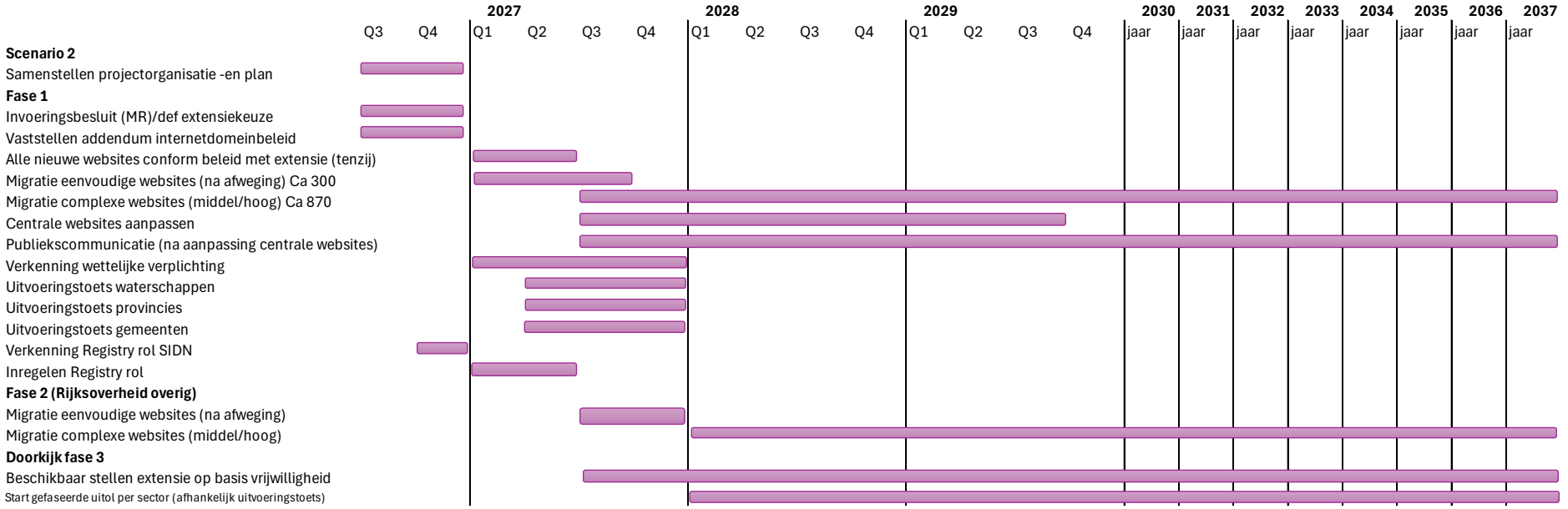
- Later publieksmoment: zolang centrale websites nog niet onder de uniforme extensie vallen, is het lastiger om breed en overtuigend te communiceren over "de nieuwe herkenbare overheid". Het publiek kan in de transitie worden meegenomen door bijvoorbeeld banners te plaatsen op de websites die voor de nieuwe extensie in aanmerking komen, zodat het publiek bij bezoek aan de website geïnformeerd wordt over de komende naamswijziging.
- Langere hybride periode met gemixte domeinen (zeker bij 10 jaar) vergroot risico op verwarring en vermindert uniformiteit in uitstraling.
- Hoger risico op verlies van momentum en eigenaarschap door langere doorlooptijd en meer variatie in startmomenten.
- Redirects en overgangsmaatregelen kunnen technische en communicatieve complexiteit toevoegen (zeker bij complexere sites zodra die aan bod komen).

5.2.2 Financiële impact en terugverdientijd

Op basis van de cijfers uit de financiële paragraaf (par. 2.3) is voor scenario 2 eveneens een indicatieve terugverdientijd berekend. Daarbij is uitgegaan van een gematigd migratiescenario met ongeveer € 24,4 miljoen aan eenmalige migratiekosten, aangevuld met eenmalige governancekosten van ongeveer € 22,9 miljoen. Daartegenover staat een gematigd saneringspotentieel van ongeveer € 22,8 miljoen per jaar. Op basis van deze uitgangspunten wordt de terugverdientijd van scenario 2 geraamd op ongeveer **drie tot vijf jaar.**

Gezien de looptijd van tien jaar betekent dit dat de investering ook in dit scenario ruim binnen de uitvoeringsperiode kan worden terugverdiend en daarna kan omslaan in structurele besparingen. Tegelijkertijd is de financiële curve in scenario 2 minder steil dan in scenario 1, doordat zowel de investeringen als de baten meer geleidelijk over de tijd zijn verdeeld. Scenario 2 vraagt daarmee minder financiële druk aan de voorkant, maar levert het financiële rendement ook later op dan scenario 1.

5.2.3 Planning scenario 2



Opmerking: mogelijk vraagt een invoeringsbesluit ook een aanvullende uitvoeringstoets voor de Rijksoverheid. In dat geval schuift de planning aan de voorkant met een half jaar tot een jaar op.

5.3 Doorkijk en bredere uitrol

In dit onderzoek is gekeken naar de impact van invoering van een uniforme domeinnaamextensie binnen een beperkte scope (departementen en uitvoerders binnen de Rijksdienst), als mogelijke eerste invoeringsfase. De overige organisaties binnen de Rijksdienst zijn hierin nog niet meegenomen. Een logisch vervolg op de beoogde eerste invoeringsfase is de migratie van de (publieke) domeinnamen van de overige organisaties binnen de Rijksdienst. Dit traject kan al binnen één of twee jaar na de start van de eerste fase worden opgestart. Op deze manier kunnen praktijkervaringen uit pilots in de eerste fase worden benut om deze vervolgfase te versnellen.

Op het moment dat de centrale randvoorwaarden voor invoering van een uniforme domeinnaamextensie binnen de Rijksoverheid zijn gerealiseerd ontstaat mogelijkheid om de uniforme domeinnaamextensie breder aan te bieden dan alleen de Rijksoverheid. In dit kader dient te worden nagegaan of een uniforme domeinnaamextensie als overheidsstandaard een wettelijke verplichting kan krijgen onder de WDO of de CBW. In beide gevallen zullen uitvoeringstoetsen per overheidssector (inclusief Caribisch Nederland) gedaan moeten worden om de uitvoerbaarheidsgevolgen en financieringsopgaven die samenhangen met deze verplichting inzichtelijk te maken. Deze onderzoeken met bijbehorende uitvoeringstoetsen kunnen parallel aan de eerste invoeringsfase worden opgestart.

Alternatief scenario kan zijn de uniforme domeinnaamextensie vanaf het moment dat de randvoorwaarden voor invoering centraal zijn ingeregeld, beschikbaar te stellen aan overige overheidssectoren op vrijwillige basis. Voordeel is dat dan geprofiteerd kan worden van de *lessons learned* uit de eerste fase(n) én er inmiddels voldoende massa is ontstaan om invoering van een uniforme extensie uit herkenbaarheidsoverwegingen aantrekkelijker te maken, zeker voor minder bekende overheidsorganisaties.

5.4 Samenvattend

Nu beide scenario's zijn uitgewerkt, wordt duidelijk dat de implementatiekeuze vooral gaat over tempo, uitvoeringsdruk en financieel verloop. Helder is dat invoering van een extensie mogelijk is, mits implementatie gepaard gaat met centrale regie, implementatieondersteuning en actieve sanering van het webportfolio. Scenario 1 kiest voor een meer voortvarende aanpak, waarbij centrale websites en eenvoudigere websites eerder worden omgezet en de publiekswaarde sneller zichtbaar wordt. Scenario 2 kiest voor een meer geleidelijk groeipad, met meer ruimte om aan te sluiten bij natuurlijke vervangingsmomenten en biedt mogelijkheid om de uitvoeringsdruk over een langere periode te spreiden.

Financieel laat scenario 1 sneller rendement zien: de terugverdientijd wordt geraamd op ongeveer twee tot drie jaar binnen een looptijd van vijf jaar. Scenario 2 kent een rustiger financieel verloop, met een terugverdientijd van ongeveer drie tot vijf jaar binnen een looptijd van tien jaar. Beide scenario's kunnen daarmee binnen hun looptijd omslaan naar structurele besparingen, waarbij scenario 1 sneller resultaat laat zien en scenario 2 meer ruimte biedt voor een beheerste en gefaseerde uitvoering.

6 Aandachtspunten en risico's

Bij de uitvoering van de impactanalyse en de mogelijke vervolgfase zijn er verschillende aandachtspunten en risico's die vroegtijdig in beeld moeten zijn. Daarnaast schetst dit hoofdstuk de logische vervolgstappen na afronding van de analyse.

6.1 Aandachtspunten

- **Samenhang met "1overheid-traject"**: Zorg voor afstemming met het bredere traject richting een centraal dienstenportaal van de overheid (1overheid) om versnippering te voorkomen.
- **Gebruik van lessons learned uit Rijkslogo-implementatie (2011):** Deze eerdere invoering biedt waardevolle inzichten over organisatorische adoptie, communicatie en centrale coördinatie.
- **Governance en eigenaarschap van de uniforme domeinnaamextensie:** Er is noodzaak tot een heldere governance-aanpak, inclusief afbakening van eigenaarschap over domeinnamen.
- **Gebruik van meerdere extensies:** Naast .nl ook .gov.nl of .overheid.nl in omloop. Dit kan de communicatie richting burgers en bedrijven bemoeilijken. Vanuit communicatieoverwegingen lijkt het verstandig één uniforme extensie te kiezen. Het is aan te bevelen een definitieve keuze in besluitvorming mee te nemen.
- **Mandaat besluitvorming websites**: Als registrar heeft DPC momenteel enkel een adviserende rol richting de Rijksorganisaties. Ze hebben geen mandaat voor het wel / toelaten van een website en kunnen niet handhaven.
    - In een nieuwe situatie met het 2LD zou het wel aan te raden zijn dat er een mandaat is ingeregeld zodat er beslissingsbevoegdheid is.
- **Impact *.gov.nl op de url www.gov.nl.** De website www.gov.nl zou bij voorkeur uitgesloten moeten worden aangezien gov.nl is opgenomen op de public suffix-lijst. Hierdoor wordt deze uniforme domeinnaamextensie gezien als een domeinnaamextensie zoals .nl, .de en .com. Dit heeft als consequentie dat www.gov.nl en gov.nl technisch meer van elkaar gescheiden zijn dan bijvoorbeeld overheid.nl en www.overheid.nl.
- **Omgang met sterke merken:** bepaalde domeinnamen hebben een belangrijke positie als "sterk merk". Voor deze domeinnamen is goede communicatie bijvoorbeeld via banners op de pagina's extra belangrijk. Ook zal het in praktijk bij dit soort domeinen noodzakelijk zijn om oude en nieuwe omgevingen naast elkaar te draaien, ook met oog op indexering door zoekmachines (behoud vindbaarheid), en onderling door te verwijzen (eerst van de nieuwe url naar de oude omgeving, vervolgens van de oude url naar de nieuwe omgeving).

6.2 Risico's

- **Verwarring bij burgers:** Het tegelijkertijd hanteren van meerdere domeinnamen domeinen (zoals .nl domeinnamen en domeinnamen met.gov.nl en .overheid.nl) kan verwarring veroorzaken en de herkenbaarheid van de digitale overheid tijdelijk verminderen. Om dit risico te mitigeren is duidelijke publiekscommunicatie noodzakelijk. Voor een eerste uitrol binnen de rijksoverheid kan de boodschap zijn dat binnen bepaalde termijn alle websites van de Rijksdienst ook herkenbaar zullen zijn aan de uniforme domeinnaamextensie. Om het publiek hierin mee te nemen kan verwezen worden naar het RIO en kan gewezen worden op

ondersteuningsmogelijkheid door de Digihulplijn. Ook kan worden nagedacht over een centrale website waarop de migratie inzichtelijk wordt gemaakt én wordt doorverwezen naar overige digitale overheidsdiensten.[40]

- **Beperkte medewerking van organisaties:** Risico op onvoldoende deelname van departementen en uitvoeringsorganisaties bij vrijwillige implementatie. Het is dan ook aan te bevelen voor de Rijksoverheid te kiezen voor een verplicht invoeringsscenario, bij voorbeeld op basis van een ministerraadsbesluit.
- **Migratielast voor kleinere organisaties:** Kleinere of technisch minder uitgeruste organisaties kunnen moeite hebben met implementatie en beheer van de nieuwe extensies. Hiervoor is ondersteuning door implementatieteams voorzien.

7 Aanbevelingen

Op basis van de bevindingen in deze impactanalyse zijn de volgende aanbevelingen geformuleerd. Deze aanbevelingen zijn van belang indien wordt besloten tot invoering van een uniforme domeinnaamextensie.

1. Kies definitief voor .gov.nl als uniforme domeinnaamextensie voor de Rijksdienst.
Uit de analyse volgt dat .gov.nl het meest voor de hand ligt vanuit veiligheid en internationale best practices. Tegelijkertijd is .gov.nl technisch eenvoudiger toepasbaar dan .overheid.nl, onder meer doordat .gov.nl al op de Public Suffix List staat.

2. Richt de eerste invoeringsfase op de publieksgerichte websites van de Rijksdienst.
Beperk de eerste fase tot departementen en uitvoeringsorganisaties binnen de Rijksdienst, conform de afbakening van de impactanalyse. Houd e-mail, interne domeinen en overige overheidslagen in deze fase buiten scope, maar verken parallel wel de mogelijkheid om op termijn functionele e-mail aan te laten sluiten op dezelfde extensie.

3. Veranker invoering in centrale governance en pas het internetdomeinbeleid aan.
Invoering is alleen kansrijk wanneer beleid, naamgeving, toelatingscriteria, uitzonderingen, toezicht en handhaving centraal worden ingericht. Aanbevolen wordt om de uniforme extensie beleidsmatig te verankeren in een addendum op het internetdomeinbeleid, met BZK als beleidseigenaar, DPC in de centrale registrarrol en een robuuste registry-functie.

4. Koppel migratie nadrukkelijk aan sanering van het bestaande webportfolio.
De grootste financiële en organisatorische winst ontstaat niet door één-op-één migratie van alle bestaande domeinen, maar door migratie te combineren met opschoning. Dubbele, verouderde of niet-noodzakelijke domeinen hoeven niet te worden gemigreerd, maar kunnen worden uitgefaseerd of samengevoegd. Daarmee wordt niet alleen het portfolio overzichtelijker, maar ontstaat ook reëel perspectief op structurele besparingen.

[40] In Oostenrijk wordt de burger meegenomen via de centrale website www.oesterreich.gv.at. Daar wordt op de pagina Digitale Services ook doorverwezen naar Oostenrijkse centrale uitvoerders die nu nog geen gebruik maken van de extensie). Ook wordt op de centrale website duidelijk uitgelegd met welk e-mailadres ministeries te benaderen zijn. Sommige hebben al wel de extensie, andere nog niet.

5. Kies voor een gefaseerde invoering met centrale regie en ruimte voor implementatieondersteuning.
De scenarioanalyse laat zien dat een gefaseerde aanpak het meest realistisch is. Daarbij ligt het voor de hand om nieuwe websites vanaf het invoeringsbesluit direct onder de uniforme extensie uit te geven en bestaande websites in tranches om te zetten, gekoppeld aan natuurlijke overgangsmomenten. Welke variant bestuurlijk de voorkeur krijgt, hangt af van de weging tussen tempo, uitvoeringsdruk en financieel verloop.

6. Start voorafgaand aan brede invoering met één of meer pilots.
Aanbevolen wordt om, vooruitlopend op formele invoering, één of meer pilotorganisaties te laten starten met sanering en migratie. Dat maakt het mogelijk om praktijkervaring op te doen met techniek, governance, communicatie, redirects, kosten en implementatieondersteuning, en om de kostenraming verder te verfijnen.

7. Reserveer middelen voor centrale ondersteuning, saneringscoördinatie en programmasturing.
Voor invoering zijn op dit moment geen middelen begroot. Als wordt besloten tot vervolg, is het nodig om vanaf volgend jaar middelen vrij te maken voor implementatieondersteuning, saneringscoördinatie, programmasturing en de inrichting van centrale voorzieningen. Juist deze investeringen zijn nodig om de invoering beheerst te laten verlopen en het besparingspotentieel daadwerkelijk te realiseren.

8. Bereid bestuurlijke besluitvorming tijdig voor.
Gelet op de departement overstijgende impact, de benodigde centrale sturing en de gevolgen voor het rijksbrede webportfolio, ligt het in de rede om een besluit over invoering bestuurlijk zwaarder te verankeren. Aanbevolen wordt daarom om, indien voor vervolg wordt gekozen, tijdig een traject richting de ministerraad voor te bereiden.

8 Bijlagen

8.1 Bijlage: Uitgangspunten en randvoorwaarden impactanalyse

Om voor deze impactanalyse de kaders duidelijk te hebben zijn de volgende uitgangspunten geformuleerd:

- Deze impactanalyse heeft de extensie *.gov.nl[41] als uitgangspunt, op basis van brede overeenstemming met direct betrokkenen (AZ, DPC, Bureau Forum Standaardisatie) en een eerdere voorkeur van de staatssecretaris van Huffelen in het principebesluit van 2023. Wel wordt, zoals toegezegd aan het OBDO, de extensie *.overheid.nl in de impactanalyse meegenomen als alternatieve optie. Voor deze alternatieve optie zullen per onderdeel de voor- en nadelen worden benoemd.
- De impactanalyse heeft uitsluitend betrekking op invoering van een uniforme extensie voor domeinen met publiek webverkeer die bedoeld zijn voor (Rijks)overheidsinformatie en dienstverlening.[42]
- De centrale domeinen (rijksoverheid.nl, overheid.nl, mijn.overheid.nl, www.overheid.nl) vormen het startpunt voor overheidscommunicatie en dienstverlening richting de burger. Deze domeinen dienen voorrang te krijgen in de migratie naar de uniforme extensie, mogelijk in eerste instantie via redirects. Daarnaast is de uniforme extensie bedoeld voor domeinen met publiek webverkeer die parallel aan deze centrale domeinen blijven bestaan voor specifieke informatie- en diensten die niet binnen de centrale domeinen kunnen worden ontsloten.
- De scope van het impactonderzoek wordt beperkt tot invoering van de uniforme extensie voor domeinen met publiek webverkeer van alléén de ministeries (departementen) en uitvoeringsorganisaties binnen de Rijksoverheid. E-mail valt buiten de scope van deze impactanalyse en ook intern gerichte domeinnamen vallen buiten scope (denk aan intranetpagina's, interne inlogpagina's, domeinen voor machine-to-machine communicatie, etc.). Dit betekent dat de onderzochte impact slechts op een deel van de organisaties binnen de Rijksoverheid betrekking heeft.
- In geval van een invoeringsbesluit dienen deelnemers binnen de scope verplicht te migreren (verplicht voor de websites binnen een termijn van 5 tot 10 jaar, op basis van lifecyclemanagement: het eerst mogelijke moment waarop een domein met publiek webverkeer wordt vernieuwd lijkt het geschikte moment om te migreren. Hierbij geldt dat de "kroonjuwelen" en meest bezochte websites met voorrang moeten worden omgezet. Voor deze websites kunnen organisaties aanspraak maken op implementatie ondersteuning. De overige websites kunnen door departementen naar eigen inzicht worden omgezet of uitgefaseerd. Websites die de extensie krijgen dienen aan alle richtlijnen en eisen te voldoen. Websites die worden uitgefaseerd hoeven niet eerst te worden gemigreerd.

[41] NB de *.gov.nl extensie is al geregistreerd als public suffix, *.overheid.nl nog niet (het registratieproces voor opname in de public suffix list bij SIDN duurt gemiddeld zes maanden).
[42] Het scheiden van de het publieksgerichte webdomeinen van interne webdomeinen is een voorstel van DPC. Dit vermindert de complexiteit van migratie naar een uniforme extensie en heeft een positief effect vanuit veiligheidsoverwegingen: mocht een publiekgericht webdomein vanwege een hack onbereikbaar zijn dan zou het interne webdomein nog wel kunnen functioneren.

- Na migratie wordt de oude domeinnaam uitgefaseerd, maar blijft conform het domeinnaambeleid van de Rijksoverheid nog wel in bezit van de Rijksoverheid om misbruik te voorkomen[43]
- Buiten scope van deze impactanalyse is verdere uitrol van de uniforme extensie voor andere organisaties binnen de Rijksoverheid. Ook eventuele uitrol van een extensie richting medeoverheden en overige overheidsorganisaties is buiten scope. Ten aanzien van de wenselijkheid om de extensie ook aan organisaties buiten de Rijksoverheid beschikbaar te stellen lijkt het verstandig om na uitrol binnen de Rijksoverheid te zijner tijd opnieuw implementatiescenario's en impactanalyses op te stellen, bijvoorbeeld per overheidslaag.
- Randvoorwaarde voor implementatie is inrichting van een centraal uitgiftepunt voor de uniforme extensie. Hierbij wordt voorzien in een gedelegeerd model waarbij een deelnemer (indien gewenst) zelf zijn/haar domeinnamen (het deel voor de public suffix) onder voorwaarden kan beheren.[44] Met name ten behoeve van het afstemmen en sturen op gebruiksdoelen(e.g. waar worden domeinen wel/niet voor gebruikt). Onderzocht moet worden hoe het uitgifteproces zo vlot en klantvriendelijk mogelijk kan worden ingericht, bijvoorbeeld door automatisering.
- Tweede randvoorwaarde is inrichting van robuuste DNS dienstverlening binnen de Rijksdienst. Wanneer hiervoor aanvullende maatregelen nodig zijn ten opzichte van de huidige situatie dienen deze maatregelen te worden geïmplementeerd. Mocht het ooit komen van een bredere uitrol, dan zou deze randvoorwaarde ook opnieuw tegen het licht moeten worden gehouden.
- Derde randvoorwaarde is gedegen publiekscommunicatie om het publiek in de overgangsfase goed te informeren over overheidswebsites. Hierbij kan bijvoorbeeld gebruik worden gemaakt van het RIO en/of informatiebalkjes.
- Daarnaast dient centraal beleid te worden geformuleerd om gebruik te maken van de uniforme extensie, met aansluitvoorwaarden waaraan deelnemers moeten voldoen. Het vaststellen, beheren en het toezicht houden op het beleid wordt centraal belegd [13]. Het beleid kan worden opgenomen in het internetdomeinbeleid van de Rijksoverheid.

8.2 Bijlage: Raakvlakken

De impactanalyse staat niet op zichzelf maar raakt aan verschillende lopende projecten, programma's en wettelijke kaders. Dit hoofdstuk schetst de belangrijkste samenhang en afhankelijkheden, zodat duidelijk wordt welke initiatieven invloed hebben op de analyse en waar afstemming noodzakelijk is.

Projecten / programma's/ trajecten

Project/programma	Relevantie	Samenhang met SLD extensie
Overheidsbrede notificatie service	Vanuit MijnOverheid wordt er gewerkt aan een overheidsbrede notificatieservice voor e-mail (dienst@organisatie.overheid.nl)	SLD keuzes kunnen niet los van elkaar worden gezien. Burgeronderzoek kan gebruikt worden voor onze impactanalyse. Contactpersoon Elmar Hendrikx.
Open data	N/A	
Register internetdomeinen Overheid	Het publiek kan bij onduidelijkheid een check doen in het register internetdomeinen overheid. Wel is het register nog in doorontwikkeling (koppeling andere domeininformatie bronnen om volledigheid te vergroten).	De voortgang van de migratie is via het register inzichtelijk
Toegankelijkheidsregister	N/A	Invoering van een extensie heeft geen invloed op de geldigheid van toegankelijkheidscertificaten.

Wet -en regelgeving

Traject	Relevantie	Samenhang met SLD extensie
Cyberbeveiligingswet (o.b.v. NIS2-richtlijn) (EU)	Stelt strengere eisen aan digitale weerbaarheid en beveiliging van vitale sectoren, waaronder overheden.	Verhoogt digitale weerbaarheid en traceerbaarheid van overheidsdiensten – sluit aan bij NIS2-doelen. Onderzocht kan worden of sectorale verplichting van een extensie als beveiligingseis (vanuit publiek) mogelijk is.
eIDAS 2.0 (EU)	Reguleert grensoverschrijdende digitale identiteit en betrouwbare online dienstverlening.	.gov.nl-domeinen kunnen functioneren als betrouwbare indicatoren van overheidsdiensten.

Wet digitale overheid (NL)	Regelt digitale toegang tot de overheid en stelt eisen aan herkenbaarheid, betrouwbaarheid en beveiliging.	.gov.nl ondersteunt de uitgangspunten van de Wdo zoals herkenbare en betrouwbare overheidscommunicatie. Onderzocht kan worden of verplichting van een extensie als nieuwe standaard mogelijk is.
BIO – Baseline Informatiebeveiliging Overheid (NL)	Bevat normenkader voor informatiebeveiliging bij overheden (BIO is verplicht).	Vergemakkelijkt naleving van BIO-normen zoals risicoanalyse, logging en monitoring.
Phishing bestrijding & e-mailstandaarden (DMARC/DKIM/SPF)	Standaarden voor veilige e-mailverzending om spoofing/phishing te voorkomen.	Uniform domeinbeheer maakt implementatie en controle van e-mailstandaarden eenvoudiger.
Archiefwet	De archiefwet stelt eisen aan het duurzaam archiveren van o.a. websites.	Uniform domeinbeheer maakt archivering volgens de archiefwet eenvoudiger.
Telecomwet (cookies)	De telecomwet stelt eisen aan websites (o.a. trackers).	Uniform domeinbeheer maakt comliancy met de telecomwet eenvoudiger.

8.3 Bijlage: Input communicatiestrategie uniforme domeinnaamextensie

Doel van de communicatie

De invoering van een uniforme domeinnaamextensie (.gov.nl of .overheid.nl) heeft impact op zowel burgers als overheidsorganisaties. De communicatiestrategie [45]ondersteunt deze transitie door:

- Eigenaarschap en draagvlak te creëren onder websitebeheerders;
- Burgers duidelijk, herhaaldelijk en begrijpelijk te informeren over de wijziging;
- Verwarring over meerdere domeinen te voorkomen tijdens de transitiefase.

Doelgroepen

- Websitebeheerders en communicatieadviseurs[46]
- Burgers

Deze doelgroepen hebben beide een ander doel voor de communicatie, dus we moeten rekening houden met **twee communicatiestrategieën**. Het is in elk geval zeer belangrijk dat de beheerders van de websites eigenaarschap voelen voor deze opgave.

[45] Deze communicatiestrategie dient enkel als denkrichting. Is niet afgestemd met AZ/DPC.
[46] Afnemers van Overheid.nl API's moeten ook geïnformeerd worden als er wordt gewisseld naar een nieuwe extensie.

Websitebeheerders en communicatieadviseurs

Doelgroep en doelen

- Wie is de doelgroep? Wie willen we aanspreken binnen de organisatie?
- Wat zijn hun grootste zorgen? En nog belangrijker: hoe kunnen we deze wegnemen? We willen ze goed voorbereiden en ze de juiste tools en support bieden om de overgang te maken.
- We willen deze groep betrekken en draagvlak creëren, maar het is ook belangrijk dat we consistent blijven.

Ideeën om deze doelen te bereiken

- **Focus groep:** Helder krijgen waar de zorgen zitten in deze doelgroep. Oftewel, waar zien ze het meeste tegenop? Zo kan er een gericht plan worden gemaakt om hen zo goed mogelijk te ondersteunen en weten we waar we de nadruk op moeten leggen om het proces makkelijker te maken voor ze.
- **Kick-off sessie** voor key stakeholders waarin we de strategie uitleggen en de impact en planning bespreken. Het doel is dat deze groep goed begrijpt waarom we dit gaan doen en wanneer. Uiteraard kunnen we ook vragen beantwoorden en ze inspraak laten hebben (waar mogelijk).
- **Toolkits:** Om deze groep te helpen kunnen we toolkits aanbieden op verschillende niveaus:
    - Stappenplan voor technische implementatie en communicatie
    - FAQ's voor intern en extern
    - Template e-mails en communicatie middelen
    - Checklists voor redirects en communicatie.
- **Training:** we kunnen ook trainingen geven per afdeling over de implementatie en de impact van deze wijziging.
- **Support:** We kunnen een support desk opzetten voor vragen en problemen tijdens de overgang, maar we kunnen ook een groep aanmaken waarin de organisaties vanuit de pilot fase elkaar kunnen helpen.
    - Zitten er ook kleine organisaties bij in de bredere uitrol? Indien dat het geval is kan het zijn dat zij niet de mankracht hebben om deze aanpassingen te doen. Daarom de mogelijkheid bekijken of er vanuit het project ondersteuning kan worden geboden of budget vrij worden gemaakt voor tijdelijke ondersteuning. Alternatief is om bijvoorbeeld een aantal organisaties kunnen bundelen en daar een interim werknemer verantwoordelijk voor te maken.
- **Updates/communicatie tijdens het proces:** Tijdens de overgangsfase is het belangrijk om iedereen betrokken te houden, dit kan via een groepschat of nieuwsbrief. Het is ook belangrijk om successen te delen en te vieren en af en toe samen te komen om het proces te blijven monitoren.

Communicatiemiddelen voor de websites

In de toolkit kunnen we templates aanbieden voor de communicatie zodat we controle houden over de uitingen (en voor consistentie zorgen), maar ook zodat we het makkelijker maken.

- Banners op de website
- Nieuwsbrief
- Social media
- Persbericht
- Email handtekeningen

Burgers

Doelgroep en doelen

- De beoogde doelgroep is zeer breed en omvat feitelijk alle inwoners van Nederland en overige gebruikers van Nederlandse overheidswebsites. De communicatieve boodschap dient daarom eenvoudig, helder en eenduidig te zijn, waarbij herhaling als versterkend mechanisme wordt ingezet.

- Het primaire doel van de communicatie is informeren. Daarbij dient nader te worden vastgesteld wat de centrale kernboodschap zal zijn: ligt de nadruk op herkenbaarheid, betrouwbaarheid of uniformiteit?

- Deze keuze is mede afhankelijk van de informatiebehoefte en perceptie van de doelgroep. Voor het ontwikkelen van een effectieve communicatiestrategie is het van belang om inzicht te verkrijgen in de belangrijkste zorgen en behoeften van burgers. Hoewel uniformiteit mogelijk het beleidsdoel is, hoeft dit niet per definitie de boodschap te zijn die het meest relevant of overtuigend is voor het publiek.
- Het is van belang om communicatie te benaderen vanuit het perspectief van de ontvanger: wat is de relevantie en wat zijn de implicaties voor hen?

- Daarnaast verdient het aanbeveling om in de communicatie een indicatie te geven van de tijdshorizon van het traject, zonder hierbij in te gaan op uitvoerige details. Voor nadere informatie kan desgewenst worden doorverwezen naar aanvullende bronnen, zoals het Register Internetdomeinen (RIO), dat tevens kan fungeren als tussenoplossing in de overgangsfase. Ook kan worden doorverwezen naar ondersteuning door de Digihulplijn.

Juist op dit punt heeft de keuze voor een implementatiescenario aanzienlijke gevolgen. In het bijzonder vereist scenario 1 uitgebreide toelichting en disclaimers, hetgeen het risico op verwarring bij het publiek kan vergroten.

Ideeën om deze doelen te bereiken

- Bredere campagne om burgers te informeren over deze aanpassing en verwarring zoveel mogelijk te voorkomen.
- Het doel is om veel zichtbaarheid te creëren en burgers bewust te maken van deze verandering.
- De communicatie maar helder en duidelijk zijn, maar we kunnen wellicht meer informatie geven over de routekaart of verwijzen naar het RIO via een webpagina.
- In het communicatieplan moeten we rekening houden met verschillende fases:
    - Vooraankondiging

    - Mix van domeinextensies
    - Volledige overgang
- Overweging: Het is de overweging waard om bij scenario 1 af te zien van een overkoepelende communicatieve boodschap, en in plaats daarvan primair te communiceren vanuit de afzonderlijke websites, met de betreffende organisatie als afzender. Deze benadering kan op korte termijn bijdragen aan duidelijkere communicatie richting de burger. Tegelijkertijd bestaat het risico dat hiermee het bredere verhaal of de samenhangende overheidsboodschap onvoldoende overkomt. Deze afweging kan worden meegenomen in de briefing aan een extern bureau om advies te verkrijgen over de wenselijkheid en effectiviteit van deze communicatiestrategie

Communicatiemiddelen

- PR aanpak (persbericht, awareness campagne)
- Samenwerkingen met de websites (banners, nieuwsbrieven, e-mails)
- Samenwerkingen met bibliotheken of cursussen die al gegeven worden (gebruik DigiD of over digitale weerbaarheid)
- Traditionele media: afhankelijk van het budget kan je natuurlijk veel mensen bereiken via Out of Home media, radio en televisie.
- Social media
- Online advertenties
- Afhankelijk van het budget en het concept van de campagne kunnen er nog middelen worden toegevoegd, zoals aanwezigheid op bepaalde events of targeted ads.

Aanpak en model

Voor de verdere uitwerking van de campagne-inzet wordt geadviseerd gebruik te maken van het "Get-who-to-by" model voor een briefing of om tot de kern te komen tijdens een brainstorm, bijvoorbeeld:

- **Get**: websitebeheerders
- **Who**: onzeker zijn over technische en organisatorische gevolgen
- **To**: zich eigenaar voelen van de implementatie
- **By**: praktische ondersteuning, training en heldere tijdlijnen

Afhankelijkheden

- Nauwe afstemming met DPC en betrokkenheid van communicatieadviseurs.
- Input uit werkpakket 2 (doelgroep analyse) en 5 (organisatorische impact).
- Budget en scenario-afhankelijke keuzes bepalen de inzet van communicatiemiddelen.

8.4 Bijlage: Overzicht Rijksdienst – uitvoerders per departement

Uitvoerders per departement
AZ (Ministerie van Algemene Zaken)
DPC (Dienst Publiek en Communicatie)
Rijksvoorlichtingsdienst
Ministerie van Asiel en Migratie
Dienst identificatie en screening Asielzoekers
Dienst Terugkeer en Vertrek
Immigratie -en Naturalisatiedienst (IND)
BZ (Ministerie van Buitenlandse Zaken)
BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
ABD (Algemene Bestuursdienst)
AIVD (Algemene Inlichtingen- en Veiligheidsdienst)
FMH (FMHaaglanden)
Logius
O&P Rijk (Organisatie en Personeel Rijk)
RVB (Rijksvastgoedbedrijf)
Rijksorganisatie ODI (Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie)
RvIG (Rijksdienst voor Identiteitsgegevens)
SSC-ICT
EZK (Ministerie van Economische Zaken en Klimaat)
RVO (Rijksdienst voor Ondernemend Nederland)
CPB (Centraal Planbureau)
DICTU
RDI (Rijksinspectie Digitale Infrastructuur)
FIN (Ministerie van Financiën)
Belastingdienst
Belastingdienst/FIOD
Dienst Toeslagen
Douane
IenW (Ministerie van Infrastructuur en Waterstaat)
ILT (Inspectie Leefomgeving en Transport)
KNMI (Koninklijk Nederlands Meteorologisch Instituut)
RWS (Rijkswaterstaat)
JenV (Ministerie van Justitie en Veiligheid)
DJI (Dienst Justitiële Inrichtingen)
IND (Immigratie- en Naturalisatiedienst)
Justid (Justitiële Informatiedienst)
Justis
NCSC (Nationaal Cyber Security Centrum)
NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid)
LVVN (Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur)
RVO (Rijksdienst voor Ondernemend Nederland)
OCW (Ministerie van Onderwijs, Cultuur en Wetenschap)
DUO (Dienst Uitvoering Onderwijs)
Rijksdienst voor het Cultureel Erfgoed
Nationaal Archief

SZW (Ministerie van Sociale Zaken en Werkgelegenheid)
RSO (Rijksschoonmaakorganisatie)
VWS (Ministerie van Volksgezondheid, Welzijn en Sport)
CIBG
RIVM (Rijksinstituut voor Volksgezondheid en Milieu)
Aanvullend
Rijksdienst Caribisch Nederland
Zorginstituut Nederland
Sociaal Cultureel Planbureau

8.5 Bijlage: Samenvatting buitenlandonderzoek

In veel landen die een uniforme domeinnaamextensie invoerden, bleek de grootste uitdaging niet de technische implementatie, maar de overgang van bestaande domeinen naar de nieuwe extensie. Het succes van deze transities hangt sterk samen met de gekozen **migratiestrategie**:

- **Platformmodel:** alle websites worden samengebracht onder één domein (bijv. *gov.uk* of *canada.ca*).
- **DNS-model:** organisaties behouden hun autonomie, maar registreren uitsluitend onder een uniforme extensie (bijv. *.gov.it*, *.gv.at*, *.gov.cz*).

De onderstaand een duiding per land hoe deze zijn omgegaan met bestaande domeinen, centrale portalen en de invoering van een uniforme extensie.

Oostenrijk – oesterreich.gv.at (DNS-model)
Oostenrijk koos voor het domein **.gv.at** als uniforme overheidsaanduiding.
Het centrale burgerportaal **oesterreich.gv.at** werd opgezet als nieuw hoofdportaal onder deze extensie en fungeert sindsdien als toegang tot online overheidsdiensten ("Digitales Amt", "Mein Postkorb").
Bestaande .at-domeinen van ministeries en deelstaten mochten tijdelijk blijven bestaan, maar moesten verwijzen naar de corresponderende .gv.at-versie.
De migratie verliep gefaseerd en werd ondersteund met een nationale publiekscampagne ("Ihr Amt im Netz"), waarmee burgers vertrouwd werden met de nieuwe extensie.

Bronnen: Interoperable Europe – *Digital Government Factsheet Austria 2023*; oesterreich.gv.at portal informatiepagina's.

Tsjechië – gov.cz (DNS-model)
Tsjechië kondigde in 2023 de invoering aan van de uniforme extensie **.gov.cz**, bedoeld voor alle centrale overheden.
De bestaande *.cz*-domeinen worden gefaseerd gemigreerd, waarbij oude domeinen via DNS-redirects verwijzen naar de nieuwe *.gov.cz*-versies.
Het nieuwe centrale portaal **vlada.gov.cz** vervangt geleidelijk het oude *vlada.cz*.
De transitie is opgezet als low-impactstrategie, uitgevoerd door het *Office of the Government* in samenwerking met *NÚKIB* (de nationale cybersecurityautoriteit).

Bronnen: Vlada.gov.cz – persbericht 2023 over overgang naar *gov.cz*; NÚKIB *Report on the State of Cybersecurity in the Czech Republic* (2023).

Polen – gov.pl (DNS-model)
Polen introduceerde de extensie **.gov.pl** in 2018 als exclusief domein voor overheidsorganisaties. Het beheer ligt bij *NASK* (het nationale internetregister).
De migratie verliep gefaseerd: oude *.pl*-domeinen blijven tijdelijk actief met redirects naar de nieuwe *.gov.pl*-versies.
Alle centrale ministeries en agentschappen publiceren inmiddels onder *.gov.pl*, met het portaal **gov.pl** als centrale toegangspoort.
Het beleid is sterk gericht op beveiliging (SPF, DKIM, DMARC verplicht).

Bronnen: NASK / DNS.pl – *Informacje o rejestracji domen gov.pl*; PolitykaBezpieczenstwa.pl (2022); Interoperable Europe – *Digital Government Factsheet Poland 2023*.

Duitsland – bund.de / verwaltung.bund.de (.de-domein)
Duitsland gebruikt al jarenlang het domein **.de** voor overheidswebsites, met centrale portalen **bund.de** en **verwaltung.bund.de** als startpunten voor burgers en bedrijven.
In 2024 is besloten te gaan toewerken naar invoering van .gov.de als uniforme extensie voor overheidsdomeinen. Er bestaat momenteel nog geen verplichting om naar *.gov.de* te migreren; plannen voor een *.gov.de*-alias zijn onderzocht maar (nog) niet vastgesteld.
De federale overheid kiest voor een pragmatische benadering: behoud van bestaande *.de*-domeinen en versterking van de centrale portalen.

Bronnen: Interoperable Europe – *Digital Government Factsheet Germany* (2019); Verwaltung.bund.de – overheidsportaalpagina; Deutschland.de – artikel "E-Government in Germany". Zie ook: https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/digitale_dachmarke/digitale_dachmarke-node.html.

Frankrijk – gouv.fr (DNS-model)
Frankrijk voert sinds 2010 een strak domeinbeleid waarbij overheidswebsites worden uitgegeven onder **.gouv.fr**.
Alle ministeries en diensten gebruiken een subdomeinstructuur (zoals *interieur.gouv.fr*, *service-public.gouv.fr* en *legifrance.gouv.fr*).
Bestaande *.fr*-domeinen redirecten naar hun *.gouv.fr*-equivalent zoals bijvoorbeeld *gouvernement.fr* redirect naar *service-public.gouv.fr. De gouv.fr* extensie functioneert als het officiële overheidsmerk.

Bronnen : Service d'Information du Gouvernement (SIG) – *Charte d'identité visuelle de l'État*; France-visas.gouv.fr; Wikipedia *.fr* / *.gouv.fr*.

Griekenland – gov.gr (platformmodel)
Griekenland implementeerde in 2021 het domein **.gov.gr** als enige toegangspoort tot digitale overheidsdiensten.
Alle eerdere *.gr*-websites van overheden zijn geïntegreerd of gesloten; het nieuwe platform *gov.gr* centraliseert diensten, formulieren en authenticatie (met *gov.gr ID*).
De invoering verliep als "Big Bang", ondersteund door een nationale campagne en directe

politieke aansturing.

Bronnen: Ministry of Digital Governance – *Digital Transformation Bible 2020–2025*; Gov.gr persberichten 2021.

Verenigd Koninkrijk – gov.uk (platformmodel)
Het Verenigd Koninkrijk centraliseerde tussen 2012 en 2015 alle departementale websites onder **.gov.uk**.
Het centrale portaal *www.gov.uk* fungeert als uniforme toegang voor burgers en bedrijven; alle oude departementale domeinen (zoals *hmrc.gov.uk*, *homeoffice.gov.uk*) redirecten sindsdien naar subroutes binnen *gov.uk*.
De transitie werd aangestuurd door de *Government Digital Service (GDS)* en duurde circa vijf jaar.
Sinds 2023 is het platform verder uitgebreid met "One Login for Government", maar het domein *gov.uk* blijft het vaste merk.

Bronnen: Government Digital Service – blogs "*Transition a site to GOV.UK"* en "*The 5 year journey to moving .gov.uk to a new registry"* (2024); Wikipedia *Gov.uk*.

Vlaanderen – vlaanderen.be (platformmodel)
De Vlaamse overheid besloot in 2015 tot een uniforme domeinstrategie: alle websites moesten worden ondergebracht onder **vlaanderen.be**.
Bestaande domeinen redirecten naar subpagina's binnen dit centrale platform (*vlaanderen.be/naam*).
Het platform combineert informatieve en transactiegerichte inhoud en wordt centraal beheerd.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); Digitaal Vlaanderen – *Over Vlaanderen.be*.

Italië – gov.it (DNS-model)
Italië reserveerde in 2009 het domein **.gov.it** exclusief voor publieke entiteiten.
Bestaande *.it*-domeinen werden gefaseerd vervangen door *.gov.it*-varianten, beheerd door de *Agenzia per l'Italia Digitale (AGID)*.
Er was sprake van formele verplichting, maar zonder sancties, waardoor de migratie traag verloopt en .gov.it nog steeds niet consequent is doorgevoerd.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); AGID – *Linee guida domini gov.it*.

Portugal – gov.pt (DNS-model)
Portugal gebruikt **.gov.pt** als verplichte extensie voor centrale overheidsinstanties.
Migratie vond geleidelijk plaats, met centrale goedkeuring per ministerieel domein.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); Gov.pt portal.

Nieuw-Zeeland – govt.nz (DNS-model)
Nieuw-Zeeland hanteert **.govt.nz** voor alle publieke websites.
De adoptie is vrijwillig, maar technisch gefaciliteerd.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); Digital.govt.nz.

Canada – canada.ca (platformmodel)
Canada centraliseerde in 2013 meer dan 1.500 federale websites op **canada.ca**, met volledige content-migratie en redirect van oude *.gc.ca*-domeinen.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); Treasury Board of Canada Secretariat – *Web Renewal Initiative*.

Verenigde Staten – .gov (DNS-model)
De Amerikaanse overheid beheert sinds 1985 het domein **.gov**, centraal uitgegeven door de *General Services Administration (GSA)*.
Federale organisaties zijn verplicht *.gov* te gebruiken; staten en lokale overheden worden aangemoedigd over te stappen. Voorbeeld: ny.gov (domeinnaam staat New York), nyc.gov domeinnaam stad New York).
Bestaande *.org* of *.com*-domeinen mogen blijven bestaan zolang ze veilig zijn.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); GSA – *dotgov.gov* (Domain Services).

Europese Commissie – europa.eu (hybride platformmodel)
De Europese instellingen publiceren uitsluitend onder **.europa.eu**, beheerd door de Europese Commissie.
Oude *.eu.int*-domeinen zijn volledig gemigreerd met redirects.

Bronnen: PBLQ – *Buitenlandonderzoek Domeinbeleid* (2019); Interoperable Europe – *EU Digital Government Factsheet*.

8.6 Bijlage: Verdiepingssessies en gesprekken

Volgnummer	Organisatie	Datum
[v1]	Belastingdienst	20-01-2026 19-2-2026 26-03-2026
[v2]	DICTU	11-12-2025 21-11-2025
[v3]	DPC / Bureau Forum Standaardisatie	11-06-2025 23-02-2026 18-03-2026
[v4]	Logius / KOOP	4-11-2025 19-11-2025 17-03-2026
[v5]	NCSC	13-2-2026
[v6]	Rijkswaterstaat	21-11-2025 8-01-2026

		30-03-2026
[v7]	RIVM	20-11-2025 8-01-2026 23-03-2026
[v8]	RVO en KVK Ondernemersplein	17-2-2026 17-03-2026
[v9]	SIDN	05-12-2026 25-2-2026

8.7 Bijlage: Bronnenlijst

[1] 'Een Top Level Domein voor betrouwbare overheidscommunicatie' (Novay 2013)
Toelichting: Een verkenning van kansen en risico's van invoering van een topleveldomein .overheidNL voor websites en e-mails van de Nederlandse overheid. Op te vragen via https://rijksoverheid.sitearchief.nl/#archive

[2] Adviesrapport flexibilisering e-mail (Microsoft 2018) (intern, niet gepubliceerd)
Toelichting: Een verkenning naar mogelijkheden voor een uniform e-mailadres voor rijksambtenaren.

[3] 'Onderzoek herkenbaarheid van en vertrouwen in websites en e-mails van de overheid' (Kantar 2019)
Toelichting: Publieksonderzoek naar de herkenbaarheid van de digitale overheid op gebied van websites en e-mails. Op te vragen via https://rijksoverheid.sitearchief.nl/#archive

[4] 'Impactanalyse uniforme domeinnaamextensie' (VNG Realisatie 2019)
Toelichting: Onderzoek naar de impact van invoering van een uniforme domeinnaamextensie voor websites en e-mails bij gemeenten.
Url: https://vng.nl/sites/default/files/2022-04/20191213%20rapport%20Uniforme%20domeinnaamextensie_definitief%20%281%29.pdf

[5] 'Buitenlandonderzoek domeinnaambeleid' (PBLQ 2019)
Toelichting: Onderzoek naar beleidsoverwegingen in het buitenland om een uniforme domeinnaamextensie in te voeren. Op te vragen via https://rijksoverheid.sitearchief.nl/#archive

[6] 'Een herkenbare en betrouwbare digitale overheid' MKBA quickscan (Ecorys 2020)
Toelichting: Een maatschappelijke kosten-baten quickscan van oplossingsrichtingen om de herkenbaarheid (en veiligheid) van de digitale overheid te verbeteren. Op te vragen via https://rijksoverheid.sitearchief.nl/#archive

[7] 'Impactanalyse uniforme domeinnaam en e-mailextensie' (intern 2020, concept, niet afgerond en niet gepubliceerd).
Toelichting: intern conceptrapport in kader van een verkenning naar een uniforme domeinnaamextensie voor websites en e-mail van de overheid.

[8] 'Technische impactanalyse eenduidige domeinnaam voor websites' (ICTU 2022) (i.o. CIO rijk, niet gepubliceerd)

Toelichting: Onderzoek naar de technische impact van het invoeren van een uniforme domeinnaamextensie voor standaard overheidswebsites.

[9] 'Adviesrapport Internetdomeinbeleid 2022: Een centrale aanpak met overheidsbreed bereik | Forum Standaardisatie' (Bureau Forum Standaardisatie 2022)
Toelichting: Beleidsadvies ten aanzien van invoeringsscenario's voor verbetering van de herkenbaarheid en veiligheid van de digitale overheid en versterking van de grip van de overheid op het eigen portfolio van internetdomeinen.
Url: https://www.forumstandaardisatie.nl/publicaties/adviesrapport-internetdomeinbeleid-2022-een-centrale-aanpak-met-overheidsbreed-bereik

[10] 'Herkenning van overheidswebsites: helpt een uniforme domeinnaamextensie?' (Centerdata 2023)
Toelichting: publieksonderzoek naar de meerwaarde voor burgers van een uniforme domeinnaamextensie voor de herkenbaarheid van websites (en andere online communicatiekanalen van) de digitale overheid.
Url: https://open.overheid.nl/documenten/0d7f9aee-ce19-4329-b64e-19d7c436584a/file

[11] 'Memo advies domeinnamen' (NCSC 2023, niet gepubliceerd)
Toelichting: advies vanuit securityperspectief over gebruik van .gov.nl versus .overheid.nl.

[12] 'Uniforme domeinextensie voor de Nederlandse overheid. Scope- en reikwijdteonderzoek' (Berenschot 2025)
Toelichting: onderzoek naar de mogelijke invoeringsscope en reikwijdte van invoering van een overheidsbrede uniforme domeinnaamextensie.
Url: https://open.overheid.nl/documenten/2756d304-415b-43c5-83c7-87c90092a212/file

[13] 'Plan van Aanpak impactanalyse uniforme domeinnamen' (PBLQ 2025)
Toelichting: advies voor afkadering van de onderzoeksscope voor een impactbepaling op invoering van een uniforme domeinnaamextensie.
Url: https://open.overheid.nl/documenten/a8128121-e5fd-42b9-b78f-e6b2c6cddacb/file

[14] 'DNS Praatplaat' (CIO-Rijk, 2024, niet gepubliceerd)
Toelichting: Inventarisatie DNS-landschap Rijksoverheid.

[15] 'Uniforme domeinnaam-extensie. Doorrekening incidentele implementatiekosten.' (Berenschot 2026)