



Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Herkenbare en veilige digitale overheid
2. Datum behandeling	10-02-2022
3. Aard van de behandeling: (dubbelklikken op vakje en 'ingeschakeld' aanvinken)	☐ Scrum ☐ Hamerstuk ☐ Ter besluitvorming ☒ Ter bespreking ☐ Ter kennisname ☐ Anders:
4. Eerder behandeld in:	☐ PL ☐ ICM ☐ MFG ☐ MT- DO i.o. ☒ Anders: MT-I 28-4 ☐ Niet Uitkomst behandeling in bovenstaand gremium: ☐ Overeenstemming (geen toelichting vereist) ☒ Afspraak om laatste stand ontwikkelingen te delen met het OBDO
5. Voorgeschiedenis / context:	Voor burgers en ondernemers is het lastig om op een eenvoudige wijze te verifiëren of de overheid werkelijk de afzender is van informatie die gepubliceerd is op onder meer een website of verstuurd is via e-mail of een ander medium dat gebruikt wordt voor digitale overheidscommunicatie.¹ Dit is een maatschappelijk probleem want burgers moeten de overheid online eenvoudig kunnen herkennen en vertrouwen. Onvoldoende herkenbaarheid leidt tot allerlei ongewenste effecten: • onzekerheid bij gebruikers of een website van de overheid is of niet; • onnodig tijdsverlies wegens gebrek aan verificatie en controle mogelijkheden; • negatieve gebruikerservaring van overheidsdienstverlening (inefficiency, ontoegankelijkheid); • verminderd gebruik van digitale overheidsdienstverlening; • ondermijning van vertrouwen in de overheid door toenemend risico op onjuiste informatie of blootstelling aan desinformatie; • risico voor burgers, ondernemers én overheidsorganisaties op verlies van gegevens en /of geld (denk aan phishing-aanvallen via neppe overheidssites). BZK/DS pakt dit probleem aan maar kan het niet alleen oplossen. Aanpak van het herkenbaarheid- en veiligheidsprobleem vereist grip en regie van de

¹ Dit blijkt uit onderzoeken van BZK/DS, 'Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid' (Kantar 2019, te vinden op rijksoverheid.sitearchief.nl) en [Eindrapport 'Een herkenbare en betrouwbare digitale overheid' - Digitale Overheid](#) (Ecorys 2020).

Daarnaast heeft bijvoorbeeld de consumentenbond een handreiking opgesteld om burgers te helpen onderscheid te maken tussen websites van commerciële aanbieders en van overheidspartijen, zie: [Bemiddelingssites overheidsloketten | Consumentenbond.nl](#)

	gehele publieke sector op haar portfolio van internetdomeinen - inclusief beheer, onderhoud en toepassing van de afgesproken informatieveiligheidsstandaarden voor een veilige digitale overheid, alsook de toegankelijkheidsvereisten die inmiddels een wettelijk karakter hebben.² Het OBDO heeft eerder het belang van de open standaarden in de strijd tegen phishing onderkend en streefbeeldafspraken geformuleerd. Het belang daarvan werd ook nog eens onderstreept in de uitzending van Zembla uitzending van 7 oktober jl. over vitale infrastructuur.³ Eind oktober ontving het OBDO in een separate e-mail al de laatste meting, met als oproep de implementatie van deze open informatie veiligheidstandaarden verder aan te jagen bij de achterblijvers in hun achterban (conform taak OBDO uit instellingsbesluit art.4 lid 2)⁴. Verbetering van de herkenbaarheid en veiligheid van de digitale overheid is een belangrijk thema, dat raakt aan andere belangrijke onderwerpen als informatieveiligheid, dienstverlening, inclusie, identiteit en communicatie. Het onderwerp verdient een integrale aanpak waarin alle relevante dossiers worden betrokken en het probleem niet beredeneerd wordt vanuit één enkele (dominante) benadering, maar juist vanuit perspectief van de burger. Uit onderzoek van december 2020⁵ naar de tevredenheid van burgers en ondernemers over digitale overheidsdienstverlening blijkt dat zij het op orde brengen van de basis infrastructuur van (digitale) dienstverlening een belangrijke beleidsprioriteit vinden. Daarnaast blijkt uit een eerder onderzoek, dat burgers moeite hebben met het onderscheiden van publieke websites en e-mail, van private (commerciële aanbieders).⁶
6. Samenvatting/toelichting	In 2019 heeft BZK/DS een interbestuurlijke verkenning uitgevoerd naar verbetering van de herkenbaarheid en betrouwbaarheid van de digitale overheid (websites/e-mails), inclusief een publieksonderzoek en een quick scan MKBA verkenning.⁷ Uit dit interbestuurlijk traject bleek dat er voor de gemiddelde burger weinig houvast is om te bepalen of een overheidswebsite of e-mail echt is en veilig kan worden gebruikt en dat onvoldoende herkenbaarheid van een overheidswebsite of e-mail kan leiden tot allerlei ongewenste effecten. Bij afronding van deze verkenning in januari 2021 bleek op dat moment op ambtelijk niveau geen draagvlak te bestaan voor verplichte invoering van een voor iedereen geldende uniforme extensie voor domeinnamen en e-mails (big bang scenario). Hiervoor zijn een politiek besluit en beschikbaar stellen van financiële middelen randvoorwaardelijk. Wel was er ambtelijk draagvlak voor verkenning op welke manier integraal kan worden toegewerkt naar een voor burgers en ondernemers herkenbare digitale overheid op het webverkeer. Het beschikbaar stellen van een invoering van een uniforme extensie voor partijen die daar wel behoefte aan hebben zou daarvan onderdeel kunnen uitmaken.

2 Uit recente metingen van Bureau Forum Standaardisatie blijkt dat overheidsorganisaties de streefbeeldafspraken uit 2017, 2018 en 2019 nog niet gehaald hebben. Doordat de afgesproken anti-phishing standaarden nog niet zijn geadopteerd, komt valse e-mail, verstuurd uit naam van (bijv. bestuurders van) overheidsorganisaties, nog steeds bij burgers, bedrijven en ambtenaren aan.

3 Zie [Groot deel vitale sector kwetsbaar voor cybercriminelen - Zembla - BNNVARA](#)

4 Bijvoorbeeld door via hun CIO's een actie uit te laten zetten: uit recente voorbeelden blijkt dat door CIO's (VWS, BZK) ingezette projecten om informatieveiligheid en internetdomeinen op orde te krijgen, effectief zijn. En het probleem van de achterblijvers periodiek te laten agenderen in de CIO- en CISO gremia (zoals CIO-beraad, SIO etc.)

5 Zie 'Oordeel Burgers en Ondernemers over Overheidsdienstverlening 2020' (Pieterse / Kantar december 2020)

[Eindrapport onderzoek overheidsdienstverlening 2020 | Rapport | Rijksoverheid.nl](#)

6 Zie noot 1

7 Idem

	Inmiddels zijn we een jaar verder en heeft het kabinet in haar reactie op het rapport van de Parlementaire Onderzoekingscommissie Kinderopvangtoeslag (POK) middelen vrijgemaakt voor de verbetering van de toegankelijkheid, betrouwbaarheid, kwaliteit, vindbaarheid en duurzaamheid van de informatievoorziening- en huishouding van de overheid zodat in de toekomst geen twijfel meer bestaat over de juistheid en echtheid van overheidsinformatie.⁸ Zodoende is BZK/DS gestart met de verkenning van een aantal oplossingsrichtingen om het probleem van de herkenbaarheid en veiligheid van de digitale overheid aan te pakken: 1. Een overheidsbreed internetdomein- en validatieregister; 2. Onderzoek naar invoering van een uniforme domeinnaamextensie zoals .overheid.nl of .gov.nl achter de bestaande domeinnaam, voor de overheid; 3. Uitwerking van een eenduidig beheerbeleid ten aanzien van internetdomeinen (inclusief actualisatie huidige domeinnaambeleid voor het rijk (2011)).⁹ Aanvullend zal Forum Standaardisatie in het kader van het veiliger maken van de digitale overheid het aantal te monitoren (overheids)domeinen in de (half)jaarlijkse IV standaardenmeting vergroten, zodat daarin onder meer de veiligheidsregio's worden meegenomen¹⁰
7. Discussiepunten	Ter verbetering van de herkenbaarheid en veiligheid van de digitale overheid wordt het OBDO verzocht om: a) hun inzicht te delen in hoeverre het probleem herkend wordt; b) te reflecteren over de drie oplossingsrichtingen die nu verkend worden (waaronder advies over het vervolgproces): 1. Uitbreiding van de scope van het register internetdomeinen dat momenteel door het Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP) in samenwerking met de Dienst Publieks Communicatie van het ministerie van Algemene Zaken (AZ/DPC) wordt ingericht voor de rijksoverheid op basis van het bestaande Register van Overheidsorganisaties. Voorstel is dit register echt overheidsbreed te maken, zodat daarover richting de burger gecommuniceerd kan gaan worden. Een register biedt de burger handelingsperspectief om te controleren of internetdomeinen van de overheid zijn of niet. Een overheidsbreed register helpt daarnaast het portfolio-beheer van de gehele overheid beter in kaart te brengen en sturing/regie te optimaliseren. Denk aan monitoring / gerichte attendering op de verplichte toegankelijkheids- en informatieveiligheidsvereisten waaraan overheden zich moeten houden. 2. Onder voorbehoud van de uitkomsten van de technische impactanalyse van CIO Rijk¹¹ starten met een overheidsbrede verkenning van een scenario waarin een uniforme overheidsextensie kan worden ingevoerd voor overheden die dit wensen (denk aan sites die eindigen met .overheid.nl).¹²

8 Zie [Kabinetsreactie op het rapport 'Ongekend onrecht' | Nieuwsbericht | Rijksoverheid.nl](#)

9 Zie [Domeinnaambeleid | Rijkswebsites | CommunicatieRijk](#)

10 Het aantal te monitoren (overheids)domeinen wordt uitgebreid van 550 (huidige aantal) naar 2.800.

11 Dit onderzoek wordt momenteel door ICTU uitgevoerd in opdracht van CIO-Rijk, met betrokkenheid van AZ/DPC, BZK/Digitale Samenleving en Forum Standaardisatie.

12 Uit een impactanalyse van VNG is gebleken dat gemeenten het probleem rondom de herkenbaarheid van hun websites niet ervaren. Zij zijn mede uit financiële overwegingen geen voorstander van verplichte invoering van een uniforme extensie, zeker niet in een big bang scenario. Zij zoeken de oplossing voor het herkenbaarheidsprobleem eerder in het stellen van eisen rondom toegankelijkheid en eenduidige vormgeving van websites. De Waterschappen hebben daartegen aangegeven de geschetste problematiek rondom de herkenbaarheid van de digitale overheid te herkennen. Zij zijn – onder voorwaarden – bereid mee te gaan met een uniforme extensie zoals overheid.nl of gov.nl, ook

	3. Uitwerking van een overheidsbreed (internet)domein beheerbeleid op basis van de onderzoeksuitkomsten van de lopende verkenning van Forum Standaardisatie, zodat overheidsbreed door overheidsorganisaties op eenduidige wijze regie kan worden gevoerd op hun website- en e-mail portfolio.

met oog op de reputatie van Waterschappen en Belastingssamenwerkingen. Provincies hebben nog geen standpunt ingenomen, zij zouden graag eerst inzicht hebben in de technische en financiële impact.



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Herkenbare en veilige digitale overheid

Presentatie DS Digitaal
9-12-2021



Daniël Verlaan
@danielverlaan

Replying to @danielverlaan

Begin december probeerde ik **via een oud, overgenomen GGD-domein** per e-mail een account voor CoronIT aan te vragen.

Dat lukte, maar ik moest na twee stappen **nóg** een stap ondernemen en dat vond ik - samen met de hoofdredactie en Juza - te ver gaan.

Toen heb ik de GGD ingelicht:

[Translate Tweet](#)

Daarop kreeg ik een reactie van de servicedesk dat ze nog enkele gegevens moesten krijgen om het CoronIT-account aan te maken. Daarop heb ik samen met de hoofdredactie van RTL Nieuws besloten om het onderzoek stop te zetten, niet verder te gaan dan noodzakelijk, en jullie via de telefoon en per e-mail te informeren.

Omdat het duidelijk is dat de CoronIT Servicedesk niet doorhad dat ik mailde vanaf een oud domein, denk ik dacht het uiteindelijk wel mogelijk was om toegang te krijgen tot CoronIT. Een kwaadwillende zou hier in de toekomst misbruik van kunnen maken. Ik hoop dat de Servicedesk hiervan op de hoogte wordt gesteld, om de beveiligingsmaatregelen verder aan te scherpen. Ondanks dat ben ik blij om te zien dat er wel degelijk vormen van authenticatie in acht werden genomen.



Lek maakte het mogelijk om te e-mailen uit naam van Rijksoverheid en RIVM

03 april 2020 14:55

Laatste update: 03 april 2020 17:49

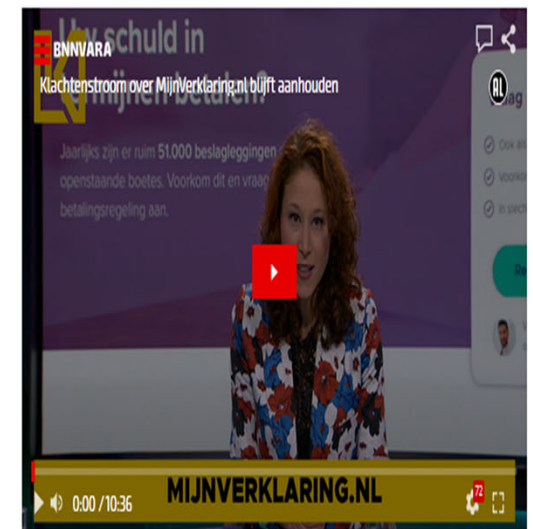
44 NUJij-reacties



Criminelen en anderen kwaadwillenden konden door niet goed ingestelde instellingen e-mailen uit naam van de Rijksoverheid en het Rijksinstituut voor Volksgezondheid en Milieu (RIVM), bevestigen woordvoerders van beide organisaties vrijdag na berichtgeving door [RTL Nieuws](#).

Klachtenstroom over MijnVerklaring.nl blijft aanhouden

1 feb 2020 • leestijd 4 minuten • 321 keer bekeken

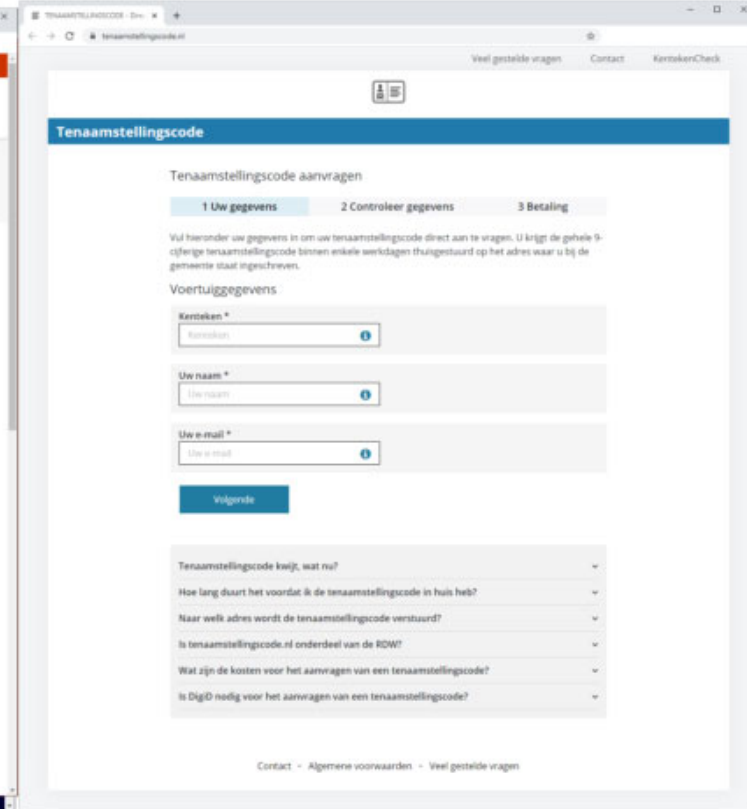
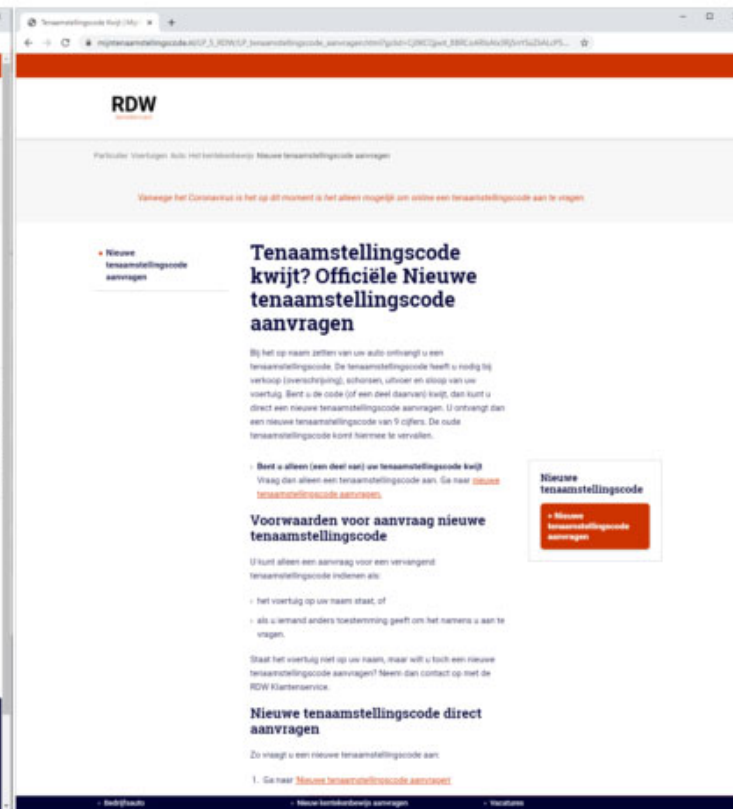
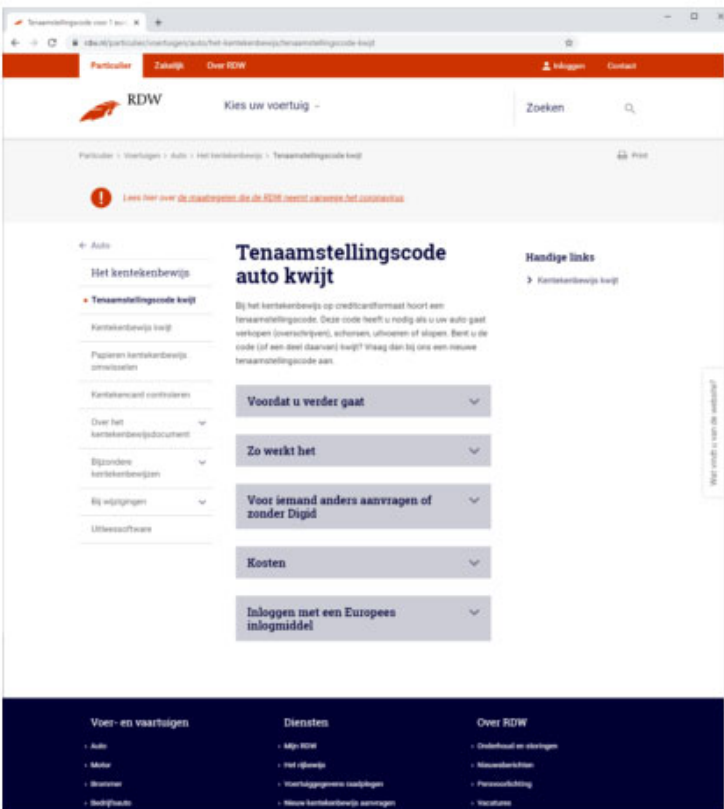


Eind november 2019 besteedden we in Kassa aandacht aan de website [MijnVerklaring.nl](#). Dit is een commerciële tussenpartij die - tegen betaling - de aanvraag voor een Verklaring Omtrent het Gedrag (VOG) voor je kan klaarzetten bij [Dienst Justis](#), de screeningsautoriteit van het Ministerie van Justitie en Veiligheid. Consumenten voelden zich misleid door niet-duidelijke communicatie over de totaalprijs. In een



Herkennen burgers de overheid online?

Volgens de consumentenbond zijn overheidsloketten niet herkenbaar voor burgers.



rdw.nl – legitiem – 1 euro
formulieren verstoopt achter
menu's

mijntenaamstellingscode.nl
 – niet overheid – 19,95 euro
Gebruikt RDW huisstijl

tenaamstellingscode.nl –
 niet overheid – 14,95 euro
Gebruikt rijksoverheid
stijlen



Consumentenbond helpt je een overheidsloket te vinden

Zo vind je een overheidsloket

Tips om een overheidsloket te vinden:

- Mijd de advertenties bovenaan de zoekresultaten als je googelt naar overheidsloketten of gebruik een [goede adblocker](#).
- Gebruik de lijst onderaan deze pagina voor enkele belangrijke loketten.
- Weet je niet zeker of je op de officiële website zit? Kijk dan of je de termen 'bemiddelaar' of 'intermediair' tegenkomt.
- Zoek op internet naar ervaringen van anderen met de betreffende site.
- Vind je het moeilijk om toeslagen aan te vragen of aan te passen? Vrijwilligers in tientallen bibliotheken houden [belastingspreekuur](#) en helpen je op weg. Ben je lid van FNV, dan krijg je gratis hulp via de [Belastingservice](#).

[Bemiddelingssites overheidsloketten | Consumentenbond.nl](#)



Zien we door de bomen het bos nog?

Internetdomein	Overheid of Privaat?
databronnencovid19.nl	Overheid
coronalocatie.nl	Privaat
coronaconflict.nl	Overheid
coronamelder.nl	Overheid
mijncoronaprotocol.nl	Privaat
coronabeeld.nl	Privaat
decoronacheck.nl	Privaat
coronatest.nl	Overheid
zelftestbestellen.nl	Privaat
zelftestenbestellen.nl	Overheid



Wat is er aan de hand?

- De overheid moet als afzender van informatie herkenbaar zijn, ongeacht het kanaal/medium. (Principe van overheidscommunicatie)
- Internetdomeinen (inclusief mail) ondersteunen de communicatie / informatie-uitwisseling van de overheid richting burgers en bedrijven en tussen overheden onderling
- Voor burgers en ondernemers (en medeoverheden) is de echtheid van internetdomeinen van de overheid moeilijk te checken (certificaten zijn moeilijk te begrijpen, een slotje zegt niks)
- In onze digitale samenleving zijn internetdomeinen inmiddels kritieke infrastructuur. Maar dit vertaalt zich niet in een goede benadering:
 - Het ontbreekt aan overheidsbreed overzicht van internetdomeinen
 - Het beheer van internetdomeinen is (vaak) niet goed ingeregeld
 - Het ontbreekt aan een beveiligingsstrategie



Hoe zet DS zich in voor een herkenbare en veilige digitale overheid?



3 trajecten voor een herkenbare en veilige digitale overheid

1. Internetdomeinen register
2. Domeinnaamextensie
3. Internetdomeinbeleid



Internet domeinen register

- Samenwerking KOOP en AZ/DPC, op basis bestaande Register Overheids Organisaties (ROO)
- Doel: realisatie register met internetdomeinen met een redactie-omgeving die individuele organisaties in staat stelt hun domeinnaamportfolio in te voeren en te onderhouden. (inclusief geautomatiseerd aanleveren voor organisaties die hun registratie op orde hebben in een extern systeem)
- Realisatie publieke omgeving waar burgers, bedrijven en andere overheden internet domeinen kunnen verifiëren -> Men ziet: of een internetdomein van de overheid is, van welke organisatie het internetdomein is en meer informatie, zoals of het domein aan de verplichte standaarden voldoet, of er een mailserver of website aan gekoppeld is, etc.
- Stel de data als open data beschikbaar voor hergebruik.
- Ondersteuning organisaties met het invoeren en up-to-date houden van de gegevens en beantwoording vragen over het register.
- Onderzoek uniform beeldelement: overheidswebsites laten hiermee zien dat de website een overheidswebsite is, bezoekers kunnen via dit element direct een check uitvoeren in het register.



Institutions and bodies profiles x Institutions and bodies profiles x +

← → ↻ 🏠 🔒 https://european-union.europa.eu/institutions-law-budget/ins

An official website of the European Union How do you know? ^

All official European Union website addresses are in the **europa.eu** domain.

[See all EU institutions and bodies](#)

Home

[Home](#) > [Institutions and bodies profiles](#)

Institutions and bodies profiles

Filter by

Keywords

Organisation type

Select

EU organisation type

Select

Subject

Select

Institutions and bodies profiles (68)

RSS

Showing results 1 to 10

DECENTRALISED AGENCY

[Agency for the Cooperation of Energy Regulators \(ACER\)](#)

The European Union Agency for the Cooperation of Energy Regulators works for a more competitive, efficient and secure energy market.

Website <https://www.acer.europa.eu/>

Email info@acer.europa.eu

Phone number +386 8 205 34 00

Address Trg republike 3, 1000 Ljubljana, Slovenia





Dienst Publiek en Communicatie
Ministerie van Algemene Zaken

CommunicatieRijk > Alle vakkennis > Rijkswebsites > Verplichte richtlijnen >



Websiteregister Rijksoverheid

[Websiteregister Rijksoverheid \(ODS, 170 KB\)](#): november 2021 (actuele versie)

In het Websiteregister Rijksoverheid staan alle websites van de Rijksoverheid. In het Websiteregister zijn bezoekcijfers en verschillende kwaliteitscriteria opgenomen.

genomen.

						F	G	H	I	J	K
						736	Domeinnaam	Websitetest	Internet.nl		
						Bezoeken/mnd	Voldoet	Totaal	IPv6	DNSSEC	HTTP
2											
3	http://www.rijksoverheid.nl	Rijksoverheid	AZ	DPC	Online Advies	23.394.631	ja	ja	ja	ja	ja
4	http://coronadashboard.rijksoverheid.nl	Rijksoverheid	VWS		Kerndepartement/PDC19	8.168.171	ja	nee	nee	ja	nee
5	http://www.rivm.nl	Rijksoverheid	VWS	RIVM		7.208.132	nee	nee	ja	ja	
6	http://www.nederlandwereldwijd.nl	Rijksoverheid	BUZA	Postenweb		6.806.785	ja	ja	ja	ja	ja
7	http://www.government.nl	Rijksoverheid	AZ	DPC	Online Advies	3.102.330	ja	ja	ja	ja	ja
8	http://ici.rivm.nl	Rijksoverheid	VWS	RIVM		1.277.257	nee	ja	ja	ja	ja
9	http://www.rvo.nl	Rijksoverheid	EZK	RVO		1.080.589	ja	ja	ja	ja	ja
10	http://www.netherlandsworldwide.nl	Rijksoverheid	BUZA	Postenweb		677.230	ja	ja	ja	ja	ja
11	http://rijksvaccinatieprogramma.nl	Rijksoverheid	VWS	RIVM		658.317	nee	ja	ja	ja	ja
12	http://www.defensie.nl	Rijksoverheid	DEF		Directie Communicatie	635.204	ja	ja	ja	ja	ja
13	http://www.rwsverkeersinfo.nl	Rijksoverheid	IenW	RWS		572.831	ja	nee	nee	ja	nee
14	http://www.rijkswaterstaat.nl	Rijksoverheid	IenW	RWS		507.743	ja	nee	nee	ja	nee
15	http://www.cbg-meb.nl	Overheid	VWS	CBG		504.674	ja	ja	ja	ja	ja



Domeinnaamextensie

Een uniforme extensie “.overheid.nl / .overheid.nl / anders...” helpt bij verbeteren herkenbaarheid en veiligheid van de digitale overheid.

- Voor burgers/ondernemers/medeoverheden is meteen duidelijk of een website van de overheid is of niet
- Centrale uitgifte / aansturing biedt kansen om eisen te stellen, meer grip overheid op portfolio internetdomeinen
- Mocht het ooit komen tot invoering dan flinke impact, hangt ook van implementatiescenario af (technisch, financieel, organisatorisch)

CIO rijk voert een technische impactanalyse uit:

- aspecten van security, kansen en risico's en beheerbaarheid
- scenario's, oplossingen voor het doorvoeren van wijzigingen
- indicatie van de kosten en baten voor websites
- beschrijving van de dienstverlening door een uitgiftepunt (inclusief de relatie tot de beheerorganisatie van een website en de verdeling van verantwoordelijkheden).



← → ↻ 🏠 🔒 https://european-union.europa.eu/select-language?destination=/node/1

An official website of the European Union **How do you know?** ^

All official European Union website addresses are in the **europa.eu** domain.

[See all EU institutions and bodies](#)



GOV.UK

▼ To

→ **Coronavirus (COVID-19)** | Guidance and support

български

latviešu

español

lietuvių

čeština

magyar

dansk

Malti

[Home](#)

About GOV.UK

GOV.UK is the website for the UK government. It's the best place to find government services and information.

The site is maintained by the [Government Digital Service \(GDS\)](#).



Één domeinnaamextensie

Internetdomein	Overheid of Privaat?
databronnencovid19.overheid.nl	Overheid
coronalocatie.nl	Privaat
coronaconflict.overheid.nl	Overheid
coronamelder.overheid.nl	Overheid
mijncoronaprotocol.nl	Privaat
coronabeeld.nl	Privaat
decoronacheck.nl	Privaat
coronatest.overheid.nl	Overheid



Internetdomeinen beleid

In opdracht van BZK/DS voert Bureau Forum Standaardisatie een verkenning uit naar aspecten die moeten worden meegenomen in een actualisatie van het internetdomeinen beleid (VoRa besluit 2011).

Huidig beleid:

- eenduidigheid van beleid en gebruik
- transparantie van beleid en gebruik
- beschermen van onze juridische positie
- beheersen van kosten

Verbeterpunten (eerste opbrengsten verkenning):

- Doelen als kostenbeheersing en bescherming van juridische positie worden niet (meer) herkend, veiligheid wordt als doel gemist
- Meer sturing nodig op eenduidigheid, weerbaarheid en beheersbaarheid, regie voor het rijk zo mogelijk centraal beleggen
- Medeoverheden meenemen, internetdomeinen beheer gaat iedereen aan, doelgroep moet overheidsbreed zijn
- Rollen, taken en bevoegdheden rond internetdomeinen beheer benoemen en bekrachtigen: wie is aanspreekpunt, wie beslist over uitgifte van nieuwe internetdomeinen
- Beleid moet gericht zijn op alles wat met domeinbeheer en herkenbaarheid van internetdomeinen te maken heeft