

Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

**Directie Bestuurlijke en
Politieke Zaken**

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6011 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
BPZ / 107958544

Datum 17 augustus 2026

Betreft Beantwoording vragen inzake de evaluatie Wet digitale overheid

Geachte Voorzitter,

Hierbij bied ik u, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de antwoorden aan op de schriftelijke vragen met kenmerk 181548 die aan mij zijn gesteld door de leden van de fractie van de PVV van de vaste commissie voor Binnenlandse Zaken van de Eerste Kamer naar aanleiding van de brief enkele toezeggingen en de evaluatie van de Wet digitale overheid (Wdo) (Kamerstukken I 2025/26, 34.972/35.868, AG).

W.J.M. Aerdts
Staatssecretaris van Economische Zaken en Klimaat

Eric van der Burg
Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

181548

Ons kenmerk
BPZ / 107958544

De leden van de vaste commissie voor Binnenlandse Zaken hebben met belangstelling kennisgenomen van de brief van 24 april 2026 die door mij samen met de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties is toegestuurd inzake enkele toezeggingen en de evaluatie van de Wet digitale overheid (Wdo). Naar aanleiding van deze brief hebben de leden van de fractie **PVV** nog enkele vragen en opmerkingen.

In de Evaluatie Wet digitale overheid lezen de leden van de PVV-fractie over de stelseltoegang dat deze nog steeds in ontwikkeling is. Zij hebben een aantal vragen over de voortgang van Stelsel Toegang dat, zo geven de leden aan, sinds 2014 in ontwikkeling is. Zij vragen om inzichtelijk te maken of de ontwikkelfase van het Stelsel vertraging oploopt door recente ontwikkelingen zoals de verkoop van Solvinity aan Kyndryl. Ook vragen zij om een overzicht van de totaal gemaakte kosten die gemaakt zijn voor de ontwikkeling van dit stelsel. Verder zien deze leden graag een prognose van de nog te verwachten kosten met een tijdspad voor oplevering van dit stelsel.

Het Stelsel Toegang geeft invulling aan het wettelijk kader zoals dat geldt onder de Wet digitale overheid (Wdo). Voor zover nieuwe ontwikkelingen (bijvoorbeeld ten aanzien van autonomie en soevereiniteit) daar aanleiding toe geven zal daarmee rekening worden gehouden bij de doorontwikkeling van het Stelsel. Het Stelsel Toegang is geen statisch eindproduct maar kent een dynamische doorontwikkeling. Ten opzichte van de huidige ontwikkelagenda zie ik daarom geen vertraging ontstaan voor het Stelsel als rechtstreeks gevolg van mogelijke verkopen van ketenpartners aan buitenlandse partijen.

Het Stelsel Toegang is in de basis begin volgend jaar technisch beschikbaar en zal vervolgens modulair in fases worden doorontwikkeld. Functionaliteiten die volgend jaar beschikbaar komen in het Stelsel hebben betrekking op wettelijk vertegenwoordigen en de open toelating voor de erkenning van private inlogmiddelen voor publieke dienstverlening. Publieke dienstverleners kunnen volgend jaar starten met het aansluiten op het Stelsel. Voorbereidingen daarvoor zijn al begonnen.

De realisatie van het huidige Stelsel Toegang is gestart na de vaststelling van de Wdo medio 2023. In totaal is daarvoor sindsdien € 37,6 miljoen beschikbaar gesteld; realisatiecijfers eind 2025. (Zie voor nadere toelichting het Rijks ICT-Dashboard). De prognose voor 2026 bedraagt circa € 11 miljoen en de prognose voor 2027 is € 7 miljoen. Daarmee is het Stelsel Toegang in de basis gereed.

Ook vragen de leden van de PVV fractie of naar aanleiding van de kwestie Solvinity beleid nodig is zodat IT-diensten, die de (toegang tot) publieke dienstverlening raken, nooit in buitenlandse handen (welke dan ook)

terechtkomen.

Zoals aangegeven in de 'Visie digitale autonomie en soevereiniteit van de overheid'¹ staan het verminderen van ongewenste strategische afhankelijkheden, het vergroten van technologische zelfredzaamheid en het stimuleren van samenwerking binnen Europa centraal in de manier waarop de Nederlandse overheid haar digitale (open strategische) autonomie en haar digitale soevereiniteit kan versterken.

Voor IT-diensten die de (toegang tot) publieke dienstverlening raken is het essentieel dat de continuïteit en veiligheid van deze diensten gewaarborgd blijft. Bestaande beleidskaders rondom digitale soevereiniteit kunnen publieke dienstverleners hierbij helpen. Zo gelden er vanaf 1 januari 2026 nieuwe beveiligingseisen voor bedrijven die overheidsopdrachten uitvoeren met risico's voor nationale veiligheid (ABRO-eisen). Daarnaast is er een Rijksbrede IT-sourcingstrategie² die het mogelijk maakt om binnen het Rijk risico-gebaseerd, verantwoord en uniform te besluiten over IT-inkoop en leverancierskeuze. Het herziene Rijkscloudbeleid biedt nieuwe kaders aan Rijksoverheidorganisaties voor het gebruik van (publieke) clouddiensten³.

Wat betreft het in buitenlandse handen raken van bedrijven hebben we in Nederland een stelsel van investeringstoetsing waarbij risico's voor de nationale veiligheid en/of het publieke belang als gevolg van verwervingsactiviteiten worden beheerst. Te beheersen risico's hierin zijn: i) het ontstaan van ongewenste strategische afhankelijkheden, ii) aantasting van de continuïteit van vitale processen, en iii) aantasting van de integriteit en exclusiviteit van informatie. Verder wordt onderzocht of er naast de eisen die nu al onder de Wdo aan inlogmiddelen worden gesteld, aanvullende eisen nodig zijn in verband met soevereiniteit.

Ten aanzien van het functioneren van de Wdo wordt gevraagd om te reageren en te reflecteren op de constatering in de evaluatie dat, mede door het ontbreken van toezicht, in de praktijk in beperkte mate uitvoering wordt gegeven aan de Wdo. In het verlengde hiervan wordt gevraagd of alle dienstverleners, en met name de private dienstverleners als onderwijs- en zorgorganisaties, die onder de Wdo vallen hebben voldaan aan de verplichtingen die de Wdo stelt, zoals het vaststellen van de betrouwbaarheidsniveaus en de kanaalaanwijzing.

De constatering die in de evaluatie gedaan is over de beperkte mate van uitvoering van de Wdo is breder dan het toezichtsvraagstuk. Deels heeft het feit dat er nog geen uitvoering is gegeven aan de Wdo ermee te maken dat het Stelsel Toegang nog niet gerealiseerd is, de daarmee gepaard gaande open toelating van inlogmiddelen nog niet is gestart en de hiervoor geldende acceptatieplicht (en het toezicht hierop) nog niet aan de orde is.

¹ Visie Digitale autonomie en soevereiniteit van de overheid | [Rijksoverheid.nl](https://rijksoverheid.nl)

² Rijksbrede Strategie IT-sourcing Strategie (Oktober 2025) | Digitale Overheid

³ Herziening Rijksbreed Cloudbeleid (3 juli 2026) | Tweede Kamer der Staten-Generaal

Voor wat betreft het classificeren van betrouwbaarheidsniveaus en het gebruik van publieke middelen in het publieke domein geldt dat deze verplichtingen nu al gelden. De verantwoordelijkheid om hier uitvoering aan te geven ligt primair bij de dienstverleners. Voor wat betreft het classificeren van betrouwbaarheidsniveaus geldt dat ik op het moment dat zij een verzoek indienen om aan te sluiten op het Stelsel Toegang zal controleren of de classificatie heeft plaatsgevonden.

Naar aanleiding van de constatering in de evaluatie dat de voorzieningen voor ouderlijk gezag en bewindvoering, die onder de reikwijdte van artikel 5 zijn mogelijk gemaakt, zich nog in een pilotfase bevinden en dat het benodigde betrouwbaarheidsniveau met DigiD Machtigen (nog) niet kan worden verkregen, vragen de leden van de PVV-fractie een onderbouwing waarom de gestelde deadline wederom niet behaald wordt.

Na de afronding van de Evaluatie van de Wdo is het parlement geïnformeerd door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de tijdlijn van digitaal wettelijk vertegenwoordigen. Dit naar aanleiding van een toezegging aan het lid Ceder (ChristenUnie). Ten opzichte van deze tijdlijn is nog geen vertraging ontstaan. Ik verwijs kortheidshalve naar deze brief (TK 2025-2026, 26643/29362, nr. 1497).

Voor de machtigingsvoorziening geldt dat de registratie van een machtiging overeen moet komen met het betrouwbaarheidsniveau van de af te nemen dienst. Op dit moment is het niet mogelijk om vrijwillig te machtigen op betrouwbaarheidsniveau substantieel en hoger.

In 2025 is gestart met het vernieuwen van DigiD Machtigen. Hierbij staat centraal dat DigiD Machtigen kan fungeren als vrijwillige machtigingsvoorziening binnen het Stelsel Toegang, die voldoet aan de Wdo met de vereiste betrouwbaarheidsniveaus. Momenteel wordt onderzocht op welke wijze het juiste betrouwbaarheidsniveau kan worden gegarandeerd, zonder dat dit ten koste gaat van de gebruiksvriendelijkheid en digitale toegankelijkheid van vrijwillig machtigen. Ik streef ernaar dat begin 2027 een passende oplossing is gevonden, waarna kan worden gestart met de aanpassingen van DigiD Machtigen.

De leden vernemen graag waarom gekozen is voor het rijbewijs voor de toepassing van de applet en aan welke andere middelen wordt gedacht om de applet op te plaatsen.

De applet die geschikt is voor DigiD Hoog is beschikbaar voor rijbewijzen uitgegeven na 26 april 2018 en identiteitskaarten uitgegeven na 1 juli 2021. In 2016 is gekozen om de applet die benodigd is voor DigiD Hoog in de eerste fase op het rijbewijs en de ID-kaart te plaatsen. Met deze combinatie kan het grootste aandeel mensen dat beschikt over een Nederlands identiteitsbewijs DigiD Hoog activeren. Destijds is besloten om de eID nog niet op het paspoort te introduceren en de eID-functionaliteit op het rijbewijs en ID-kaart door te ontwikkelen voordat de keuze werd

gemaakt om deze functionaliteit ook te introduceren op het paspoort. Op dit moment wordt er onderzocht welke mogelijkheden er zijn om DigiD Hoog op een andere, meer toegankelijke manier te introduceren zonder afhankelijk te zijn van de applet en te voldoen aan gestelde eIDAS-richtlijnen vanuit de Europese Unie.

In verband met het vraagstuk omtrent digitale soevereiniteit vragen de leden van de PVV-fractie, waarom een land als de Verenigde Staten als risicovolle statelijk actor wordt beschouwd en Frankrijk, dat zich volgens de leden bij de Nederlandse aanbesteding van de nieuwe onderzeeboten schuldig maakte aan lastercampagnes tegen niet-Franse partijen, dat niet-Franse partijen hackte (spionage) en alle dubieuze praktijken uit het boekje erbij haalde om de opdracht binnen te slepen, als 'betrouwbaar' wordt bestempeld.

Het kabinet voert voor digitale soevereiniteit een landenneutraal en risicogebaseerd beleid, zoals ook het bredere economische veiligheidsbeleid. Zoals aangegeven in de brief 'Voortgang kabinetsaanpak economische veiligheid'⁴ is het Nederlandse economische veiligheidsbeleid landenneutraal, conform internationale principes, rechtsbeginselen en verplichtingen zoals het non-discriminatiebeginsel. Ook bij aanbestedingen wordt binnen de geldende wettelijke kaders beoordeeld op onderliggende risico's, op basis van eerdergenoemde landenneutrale en risicogebaseerde benadering.

Tot slot willen de leden van de PVV-fractie graag de garantie dat gebruik van een Europese wallet (als digitaal paspoort) nooit verplicht wordt en burgers ook zonder wallet kunnen blijven communiceren met de overheid.

Het gebruik van Europese Digitale Identiteitswallets (EDI-wallets) is vrijwillig, zoals uit de Europese eIDAS-verordening volgt. De toegang tot publieke diensten mag niet op enige wijze beperkt of belemmerd worden voor natuurlijke personen die geen EDI-wallet willen of kunnen gebruiken. Publieke organisaties die een EDI-wallet accepteren, dienen altijd een alternatief aan te bieden voor personen die geen gebruik willen maken van een EDI-wallet. Daarnaast schrijft de verordening voor dat bestaande elektronische identificatie- en authenticatiemiddelen naast de EDI-wallet kunnen blijven bestaan. Het gebruik van andere inlogmiddelen zoals DigiD, blijft daarmee mogelijk. Burgers die geen EDI-wallet willen of kunnen gebruiken, zullen dus met de overheid kunnen blijven communiceren, en behouden toegang tot overheidsdiensten. Een EDI-wallet is dan ook geen verplicht digitaal paspoort en kan op grond van de huidige Europese regelgeving niet verplicht worden gesteld voor burgers.

⁴ [Kamerbrief over voortgang kabinetsaanpak economische veiligheid | Rijksoverheid.nl](#)

Aan de staatssecretaris van Economische Zaken - Digitale Economie en
Soevereiniteit

DG Digitaliseringsbeleid
Samenleving en Overheid
(i.o.)

nota
TER BESLISSING

Kamervragen EK n.a.v. evaluatie Wdo

Datum aangemaakt
20 juli 2026

Kenmerk
.....

Kopie aan

Bijlage(n)
2

Parafenroute

Aanleiding

Schriftelijke vragen gesteld door de leden van de fractie van de PVV van de vaste commissie voor Binnenlandse Zaken van de Eerste Kamer naar aanleiding van de brief enkele toezeggingen en de evaluatie van de Wet digitale overheid (Wdo) (Kamerstukken I 2025/26, 34.972/35.868, AG). De leden verzoeken u om uiterlijk binnen vier weken na dagtekening van de brief (23 juni 2026) een reactie te versturen.

Advies

U kunt akkoord gaan met de beantwoording van de vragen.

Kernpunten

De gestelde Kamervragen gaan in op de evaluatie Wdo die op 24 april 2026 naar de Eerste en Tweede Kamer is verstuurd. De vragen gaan niet over de inhoud van de Wdo, maar over gerelateerde onderwerpen, als digitale soevereiniteit en EDI-wallets die onder uw verantwoordelijkheid vallen, en over de uitvoering van de Wdo, vertegenwoordigen en DigiD hoog die onder verantwoordelijkheid van SBZK vallen.

SEZ:

- Digitale soevereiniteit / risico's IT-diensten in buitenlandse handen.
- Vrijwillig gebruik van de EDI-wallet.
- De beantwoording van de vragen over soevereiniteit is in overeenstemming met geldend beleid (*Visie digitale autonomie en soevereiniteit van de overheid, Rijksbrede strategie IT-sourcing, Herziening rijksbreed cloudbeleid. Voortgang kabinetsaanpak economische veiligheid*) en afgestemd met CIO Rijk, BuZA en EZK/Digitale autonomie.
- Het gebruik van EDI-wallets is vrijwillig (conform eIDAS/ huidig beleid).

Ontvangen BPZ

SBZK:

- Voortgang en kosten van het Stelsel Toegang.
- Functioneren van de Wdo en toezicht.
- Voortgang van wettelijk vertegenwoordigen en machtigen.
- Keuze van middelen (waaronder het Rijbewijs, ID-kaart) voor het plaatsen van de applet voor DigiD Hoog.
- De beantwoording over de planning/voortgang van het Stelsel Toegang is zoals recent tijdens PO met SBZK besproken.
- De uitvoering van de Wdo inclusief toezicht is (deels) afhankelijk van de ingebruikname van het Stelsel Toegang.
- Na de afronding van de Evaluatie van de Wdo is de TK geïnformeerd door de SBZK over de tijdlijn van digitaal wettelijk vertegenwoordigen (TK 2025-2026, 26643/29362 nr. 1497). Deze tijdlijn is nog actueel: (2027 brede uitrol wettelijk vertegenwoordigen ouderlijk gezag, vervolgens een doorontwikkeling voor particuliere wettelijk vertegenwoordigers – curatoren, bewindvoerders, mentoren).
- De applet t.b.v. DigiD hoog is nu enkel geplaatst op het rijbewijs en de identiteitskaart. Onderzocht wordt of er mogelijkheden zijn om DigiD Hoog op een andere, toegankelijker manier te introduceren, zonder afhankelijkheid van identiteitsbewijzen.

Toelichting

De vragen zijn gericht aan u, vanuit uw verantwoordelijkheid voor de Wet digitale overheid, EDI wallet en digitale soevereiniteit, maar raken ook het dossier van SBZK (GDI voorzieningen, Stelsel Toegang). Daarom is SBZK medeondertekenaar.

Bijlagen

1.	Beantwoording Kamervragen EK PVV– evaluatie Wdo
2.	Kamervragen EK PVV over toezeggingen en de evaluatie Wet digitale overheid