Adviescollege
ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de staatssecretaris, de heer E. van der Burg
Postbus 20011
2500 EA Den Haag

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon
info@adviescollegeicttoetsing.nl

Betreft
Aanbieding advies Programma Stelsel Toegang

Datum
29 oktober 2026

Kenmerk
2026-0000576418

Uw kenmerk
2025-0000331514

Bijlage(n)
Advies Programma Stelsel Toegang

Geachte heer Van der Burg,

U heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het Programma Stelsel Toegang. Het Adviescollege ICT-toetsing heeft dit onderzoek inmiddels afgerond. Bijgaand treft u het definitieve advies aan.

Uw medewerkers zijn geïnformeerd over de strekking van het advies. Voor de volledigheid maak ik u erop attent dat nu de periode van vier weken ingaat waarbinnen het advies met de bestuurlijke reactie naar beide kamers van de Staten-Generaal dient te worden gestuurd. Op grond van onze instellingswet zijn wij gehouden het advies binnen twee weken openbaar te maken.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

Adri de Bruijn
Voorzitter

Adviescollege ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de staatssecretaris, de heer E. van der Burg
Postbus 20011
2500 EA Den Haag

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon
info@adviescollegeicttoetsing.r

Betreft
Advies Stelsel Toegang

Datum
26 oktober 2026

Kenmerk
2026-0000576419

Uw kenmerk
2025-0000331514

Bijlage(n)
1

Geachte heer Van der Burg,

Uw ministerie heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het Programma Stelsel Toegang van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De opdrachtgever van het programma is de directeur Digitale Overheid. Het advies kan als volgt worden samengevat:

Het Programma Stelsel Toegang zorgt ervoor dat burgers en bedrijven kunnen kiezen tussen private en publieke inlogmiddelen voor veilige en betrouwbare digitale toegang tot de overheid. BZK geeft hiermee invulling aan de Wet Digitale Overheid (Wdo), waarmee de eerste versie van de Europese eIDAS-verordening wordt geïmplementeerd. Burgers en bedrijven kunnen straks inloggen namens een ander, met een hoog betrouwbaarheidsniveau en met een middel van hun keuze. Inmiddels is er ruim € 43 miljoen uitgegeven, is het programmaplan drie keer bijgesteld en is het realiseren van de doelstelling nog niet in zicht. Ondertussen is genoemde Europese verordening herzien, eIDAS 2.0, om een digitale wallet voor inloggen te introduceren.

Conclusie

Als gevolg van een laag realisatietempo van het Programma Stelsel Toegang hebben burgers en bedrijven nog steeds geen zicht op veiligere inlogmogelijkheden met keuzevrijheid en namens een ander.

A. Het Programma Stelsel Toegang levert nog weinig concrete resultaten.
B. De voorzieningen voor veilig inloggen sluiten niet aan op eIDAS 2.0.
C. Inzet op meer keuzevrijheid dan nodig maakt ontwikkeling inlogmiddelen duur.
D. Voor burgers dreigt een verwarrend geheel aan inlogmiddelen te ontstaan.

Advies

Versnel de uitvoering van het programma door focus aan te brengen op het burgerperspectief:

1. Lever zo snel mogelijk functionaliteit waar burgers en bedrijven om vragen.
2. Houd rekening met de wallet bij de doorontwikkeling van de voorzieningen.
3. Creëer duidelijkheid over het geheel aan inlogmiddelen dat beschikbaar komt.

Deze adviezen vragen een intensievere samenwerking met het programma EDI-stelsel NL dat vanaf 2027 onder Economische Zaken en Klimaat (EZK) valt. Stuur daarom samen met uw collega van EZK op het realiseren van beide programma's.

Hieronder vindt u eerst een korte beschrijving van het programma en zijn omgeving. Daarna werken we bovenstaande analyse en adviezen nader uit. Wij concentreren ons hierbij op de belangrijkste risico's van het programma. Daarbij nemen we ook die onderdelen mee die buiten de geformuleerde scope van het programma vallen maar die belangrijk zijn voor het succes van het programma of waarmee een afhankelijkheid bestaat. In de bijlage vindt u de details van het programma.

Ons onderzoek richt zich op de aanpak van het Programma Stelsel Toegang sinds de herziening daarvan in 2025 en minder op de aanpak die daaraan voorafging omdat daar al van is geleerd. Ons advies richt zich vooral op de inlogmogelijkheden voor burgers omdat Europese ontwikkelingen rondom de business-wallet nog niet zijn afgerond. Ons advies richt zich niet op burgers die geen smartphone willen of kunnen gebruiken, want daar moeten niet-digitale voorzieningen voor zijn en blijven.

Omschrijving van het Programma Stelsel Toegang

Achtergrond

Om burgers en bedrijven eenvoudig toegang te geven tot digitale diensten bij de overheid of andere publieke dienstverleners, zoals zorginstellingen, moeten zij op betrouwbare, veilige en toegankelijke wijze kunnen inloggen. Dat kan nu al met DigiD voor burgers en met eHerkenning voor bedrijven. De Wet digitale overheid (Wdo) vormt het kader voor de toegang tot overheidsdiensten en stelt eisen aan de inlogmogelijkheden.

Sinds mei 2024 is de herziene eIDAS-verordening (electronic identification, authentication and trust services, in het vervolg eIDAS 2.0) van kracht. De verplichtingen uit deze verordening treden gefaseerd in werking. Lidstaten moeten eind 2026 burgers minstens één digitale wallet (in het vervolg EDI-wallet van *European Digital Identity*-wallet) gratis ter beschikking stellen waarmee burgers hun identiteit kunnen aantonen, kunnen inloggen bij dienstverleners en gegevens kunnen delen. Door het implementeren van de verordening wordt een veilige manier van inloggen gerealiseerd die in alle Europese landen bruikbaar is. Aan de Tweede Kamer is gemeld dat Nederland de EDI-wallet uit deze verordening pas per 2028 in Nederland toe kan laten. Het programma EDI-stelsel NL ontwikkelt de voorzieningen hiervoor.

Bij het realiseren van betrouwbare, veilige en toegankelijke inlogmiddelen doen zich de volgende uitdagingen voor:

- inloggen met betrouwbaarheidsniveau 'hoog' is voor burgers nog niet op grote schaal mogelijk (in het vervolg een hoog betrouwbaarheidsniveau genoemd);
- wettelijke vertegenwoordiging en machtigen zijn nog niet altijd beschikbaar: voor burgers urgent maar nog niet beschikbaar voor alle doelgroepen en ook niet voor alle toekomstige inlogmiddelen;
- keuzevrijheid bij inloggen is er nog niet: een politieke wens maar de burger kan nog steeds niet met een privaat middel van zijn keuze, bijvoorbeeld een bank-app, inloggen (banken hebben de verplichting om de identiteit van hun klanten vast te stellen en gebruiken deze nu al om een voorziening aan te bieden waarmee een klant zich digitaal kan identificeren; deze voorziening is alleen nog niet erkend voor inloggen bij de overheid);
- afhankelijkheid van Amerikaanse platformen verminderen heeft ook nadelen: inloggen met DigiD zonder Google, Microsoft of Apple account kan alleen voor betrouwbaarheidsniveau 'midden' maar is ook gewenst voor andere inlogmiddelen en op hogere betrouwbaarheidsniveaus;
- misbruikbestrijding is complex met meerdere inlogmiddelen: in een situatie met meerdere inlogmiddelen moeten hiertoe gegevens van verschillende inlogmiddelen worden gecombineerd maar niet elk inlogmiddel ondersteunt dit;

- adoptie door publieke dienstverleners vraagt ondersteuning: voor publieke dienstverleners is het verplicht maar zij hebben ondersteuning nodig om de verschillende toegangsmiddelen op efficiënte wijze te accepteren.

Daarnaast bestaan er maatschappelijke zorgen over:
- inclusie: kunnen ook minder digitaal vaardige mensen nog wel meedoen en word je als burger niet te veel geforceerd om – bijvoorbeeld – een smartphone aan te schaffen om te kunnen inloggen;
- privacy: ontstaan er mogelijkheden voor centrale surveillance en tracking van burgers en wordt het risico hiervan voldoende gereduceerd.

BZK heeft ervoor gekozen om deze uitdagingen aan te gaan met twee programma's. Naast het Programma Stelsel Toegang is dat het eerder gestarte programma EDI-stelsel NL dat zich richt op voldoen aan de nieuwe eIDAS-verordening. Hierover adviseerden wij in 2025[1].

Het Programma Stelsel Toegang
Het Programma Stelsel Toegang richt zich op het voldoen aan de Wdo voor burgers en voor bedrijven. Het is gestart in 2023. Omdat er te weinig voortgang was, is de aanpak in december 2024 bijgesteld. Het programma levert nu regelmatig een release met nieuwe functionaliteit en probeert daarbij zoveel mogelijk bestaande ICT-voorzieningen te (her)gebruiken. De volgende voorzieningen worden ontwikkeld:
- de bevoegdheidsverklaringsdienst (BVD) waarmee bevoegden kunnen inloggen namens een ander;
- de centrale misbruikbestrijdingsdienst (CMB) waarmee misbruik van inlogmiddelen kan worden gedetecteerd en geregistreerd;
- het stelsel Toegang waarmee een privaat inlogmiddel erkend en gebruikt kan worden voor inloggen bij de overheid;
- doorontwikkeling van de routeringsdienst (TVS) binnen het stelsel Toegang waar dienstverleners op kunnen aansluiten om eenvoudig meerdere inlogmiddelen te accepteren;
- doorontwikkeling van het BSN-koppelregister (BSNk) waardoor dienstverleners versleutelde BSN-nummers kunnen verwerken.

De ontwikkeling van deze voorzieningen wordt uitgevoerd door DICTU en ICTU, en het beheer door Logius.

Het Programma Stelsel Toegang heeft een budget van bijna € 61 miljoen en loopt tot en met 2027. Het budget dient ook voor beheer- en onderhoudskosten voor die periode. Het programma voorziet echter dat niet alle ontwikkelactiviteiten dan zijn afgerond. De nog op te richten Stelsel Toegang organisatie zal de ontwikkelactiviteiten van het programma na 2027 overnemen en het beheer van de voorzieningen op zich nemen. Voor deze activiteiten is nu nog geen financiering geborgd.

[1] Zie Advies EDI-stelsel NL | Adviescollege ICT-toetsing

Conclusie: burgers en bedrijven hebben nog steeds geen zicht op veiligere inlogmogelijkheden met keuzevrijheid en namens een ander.

Datum
26 oktober 2026

Kenmerk
2026-0000576419

Wij kunnen ons vinden in de incrementele aanpak met zoveel mogelijk hergebruik van bestaande voorzieningen die het programma na de herziening in 2025 heeft ingezet. In plaats van het oorspronkelijke plan om een heel nieuw stelsel met voorzieningen op te bouwen zijn de werkzaamheden nu in releases verdeeld die werkzame functionaliteit in delen opleveren. Een voorbeeld is de eerste release van de BVD die alleen zal werken voor bevoegden van kinderen onder de 12 jaar waarna in volgende releases de functionaliteit voor andere doelgroepen zal worden opgeleverd. Vasthouden aan deze ingeslagen weg is een voorwaarde om resultaten te boeken.

We zien echter ook dat burgers en bedrijven nog steeds geen zicht hebben op veiligere en andere inlogmiddelen, om de vier redenen hieronder.

A. Het Programma Stelsel Toegang levert nog weinig concrete resultaten

De Wdo is in werking getreden maar praktisch gezien zijn de beoogde resultaten, veiliger en betrouwbaarder inloggen, nog niet gerealiseerd: de voorzieningen zijn nog niet gereed en onderliggende regelgeving is nog niet afgerond. Na een lange aanloop met opstartproblemen komen de eerste resultaten van het Programma Stelsel Toegang nu beschikbaar. De voorziening voor Centrale Misbruik Bestrijding is opgeleverd en de eerste release van de BVD wordt binnenkort met een pilot beproefd. Maar burgers en bedrijven missen nog steeds essentiële functies voor digitale toegang:

- De meeste burgers loggen nog steeds niet in met een hoog betrouwbaarheidsniveau. Dit komt doordat zo inloggen ingewikkeld is en alleen beschikbaar voor mensen met een rijbewijs of identiteitskaart. Hierdoor is het verplichte gebruik door aangewezen diensten, zoals zorgverleners, uitgesteld tot 1 juli 2028.
- Inloggen als bevoegde namens een kind van 12 jaar en ouder of namens een volwassene moet nog worden gerealiseerd. De workflow van de gerealiseerde BVD is nu alleen geschikt voor het direct toegang verlenen tot gegevens van kinderen onder de 12 jaar. Voor hen kan direct toegang verleend worden op basis van de bevoegdheidsverklaring omdat ouders en andere bevoegden volledig verantwoordelijk zijn. Voor kinderen van 12 jaar en ouder en voor volwassenen moet de dienstverlener echter de bevoegdheidsverklaring wegen in combinatie met de omstandigheden en handeling voor het verlenen van toegang.
- Burgers kunnen nog niet inloggen met een privaat middel bij de overheid. Het overnemen van het stelsel dat gebruikt wordt voor private inlogmiddelen voor bedrijven (het eTD-stelsel) heeft de technische ontwikkeling versneld, maar het inrichten van de governance en afstemmen van de aansluitvoorwaarden zal nog niet voor 2028 zijn afgerond.
- Voor marktpartijen zijn er nog geen concrete resultaten zichtbaar. Wij verwachten niet dat dit voor 2028 wel mogelijk is doordat marktpartijen nu nog niet weten welke standaard zij moeten implementeren en aan welke voorwaarden zij moeten voldoen. Ook de wijze waarop de Rijksdienst Digitale Infrastructuur (RDI), die nu toezicht houdt op het eTD-stelsel voor eHerkenning, toezicht gaat houden op het stelsel Toegang is nog niet bekend.

Wij zien dat het tempo waarin verbeteringen worden gerealiseerd te laag is om voorgenomen en afgesproken tijdlijnen te halen. Wij zien de volgende oorzaken:

- In het verleden heeft de capaciteit van de uitvoerders (met name Logius) voor vertraging gezorgd. Hun capaciteit moet worden verdeeld over de verschillende lopende initiatieven. Naast de ontwikkeling van het stelsel Toegang zijn dit het EDI-stelsel, de NL-wallet, de routeringsvoorziening (TVS), de BVD, PIN-reset voor DigiD Hoog en modernisering DigiD.

- Het jaarlijks aanvragen van budget bij de Programmeringsraad Generieke Digitale Infrastructuur (PGDI) door het Programma Stelsel Toegang en het programma EDI-stelsel NL zorgt ervoor dat budgetten pas zeker zijn als uitvoerders hun jaarplan al klaar hebben. De activiteiten voor deze programma's moeten dan alsnog in de planning worden ingepast met het risico dat zij achteraan aansluiten bij de uitvoering van activiteiten.
- De releasematige aanpak vraagt van de opdrachtgever een goede sturing op het behalen van de doelstellingen[2]. Door gebrek aan deze sturing ervaren stakeholders in de omgeving onduidelijkheid over de prioritering en de planning. Dit leidt ertoe dat zij het vertrouwen in het programma verliezen, activiteiten om aan te sluiten uitstellen en uiteindelijk niet klaar zijn als dat nodig is.

B. De voorzieningen voor veilig inloggen sluiten niet aan op eIDAS 2.0

Terwijl het Programma Stelsel Toegang nog bezig is met het implementeren van de Wdo, waarmee Nederland eIDAS 1.0 implementeert, zijn nieuwe verplichtingen uit eIDAS 2.0 van kracht geworden. Het programma anticipeert hier onvoldoende op. Het stelt de aansluiting op de ontwikkelingen uit Europa uit met als reden dat specificaties nog niet concreet genoeg zijn. Andere landen in Europa laten zich hier niet door afremmen en lopen hierdoor voor op de ontwikkelingen in Nederland. Om de voorzieningen uit het Programma Stelsel Toegang aan te laten sluiten op de Europese eIDAS-verordening, zullen voorzieningen die nu in ontwikkeling zijn, later herzien moeten worden:

- De EDI-wallet kan geen gebruik maken van de huidige BVD. Voor mogelijk gebruik in de EDI-wallet moet namelijk een digitaal bewijs gegenereerd worden waarmee een bevoegdheid aangetoond wordt.
- DigiD Hoog is niet op grote schaal te gebruiken omdat het niet mogelijk is om de zelf ingestelde pincode te resetten. DigiD Hoog is nodig om de EDI-wallet te activeren. Vanaf 1 juli 2028 is het gebruik van DigiD Hoog bovendien verplicht in de zorg voor het inzien van vertrouwelijke persoonsgegevens.
- De wijze waarop identiteitsinformatie in de EDI-wallet gebruikt wordt om in te loggen bij een overheidsdienst en aan te sluiten op TVS moet nog worden bepaald. Deze activiteiten zijn uitgesteld met als risico dat dienstverleners niet tijdig aan de verplichting voldoen om de EDI-wallet te accepteren.
- Het ontbreekt de CMB straks aan gedetailleerde gegevens uit logbestanden om misbruiksignalen over de EDI-wallet op te volgen. De CMB signaleert fraudesignalen bij erkende inlogmiddelen binnen het Stelsel Toegang. De EDI-wallet is straks ook een erkend inlogmiddel, maar kan de gegevens uit logbestanden van inlogmiddelen niet aanleveren.

C. Inzet op meer keuzevrijheid dan nodig maakt ontwikkeling inlogmiddelen duur

Wij snappen dat de burger moet kunnen kiezen voor een publiek inlogmiddel en tussen meerdere private inlogmiddelen. Maar de keuzevrijheid die nu gerealiseerd wordt laat de burger niet alleen kiezen tussen publiek en privaat, maar ook tussen een middel dat Europees toegelaten is en een middel dat alleen in Nederland toegelaten is.

Wij vinden de investeringen in het stelsel Toegang om private inlogmiddelen mogelijk te maken een onnodige vorm van keuzevrijheid introduceren. De mogelijkheid om een privaat inlogmiddel aan te bieden wordt immers al gerealiseerd met het stelsel EDI-wallet. De totale kosten van alle stelsels en voorzieningen voor inloggen bij de overheid gaan onnodig hoog oplopen doordat de burger straks kan kiezen uit twee publieke inlogmiddelen en private inlogmiddelen van twee verschillende stelsels:

---

[2] Zie ook onze Handreiking agile werken (https://www.adviescollegeicttoetsing.nl/documenten/2023/12/20/handreiking-agile-werken).

- Het programma EDI-stelsel NL introduceert een EDI-wallet waarmee burgers zich kunnen identificeren en authentiseren. Dit publieke inlogmiddel wordt ontwikkeld onder de noemer NL-wallet. De overheid is verplicht om minimaal één gratis EDI-wallet aan te bieden. Het idee van het EDI-stelsel is dat daarnaast private partijen die aan de eisen voldoen, kunnen worden toegelaten als erkend inlogmiddel.
- Het Programma Stelsel Toegang richt zich op het ontzorgen van publieke dienstverleners en zorgverleners door te zorgen dat DigiD en de EDI-wallets via TVS kunnen worden afgehandeld. Daarnaast ontwikkelt het programma ook een eigen stelsel (stelsel Toegang) om private inlogmiddelen voor de Nederlandse markt te erkennen.

De totale kosten voor het bieden van keuzevrijheid gaan onnodig oplopen doordat er nu, naast DigiD en het eTD-stelsel, meerdere stelsels komen. De vermijdbare kosten worden gemaakt door het uitvoeren van een aantal onnodige activiteiten:

- inrichten van meerdere stelsels met voor elk stelsel eigen sturing, aansluitvoorwaarden en bijbehorend toezicht;
- ontwikkelen van de voorzieningen voor het kunnen erkennen van private inlogmiddelen door het nieuwe stelsel Toegang;

D. Voor burgers dreigt een verwarrend geheel aan inlogmiddelen te ontstaan

In de Tweede Kamer is expliciet aangegeven dat DigiD blijft bestaan en dat het gebruik van de EDI-wallet (conform de verordening) geheel vrijwillig is. Maar daarmee heeft de overheid nog geen duidelijke keuzes gemaakt over de toekomst van inlogmiddelen in Nederland. Welke inlogmiddelen moeten er naast DigiD en de EDI-wallet blijven bestaan? Er worden nu naast deze twee publieke ook twee typen private inlogmiddelen geïntroduceerd. De consequentie van deze keuze is dat het landschap van inlogmiddelen voor de burger onoverzichtelijk wordt. Samengevat kan de burger straks kiezen uit de volgende inlogmiddelen:

1 DigiD. Dit blijft een gratis publiek middel om in te loggen bij de overheid. Logius heeft een project gestart om DigiD te moderniseren zodat burgers er in de toekomst gebruik van kunnen blijven maken.
2 Private middelen die erkend zijn onder het Nederlandse stelsel Toegang en gebruikmaken van voorzieningen uit het eTD-stelsel. Dit wordt ontwikkeld door het Programma Stelsel Toegang.
3 De publieke EDI-wallet waarmee burgers gratis kunnen inloggen bij de overheid en bedrijven. Dit stelsel en de gratis publieke EDI-wallet worden ontwikkeld door het programma EDI-stelsel NL.
4 Private en publieke middelen die toegelaten zijn onder de eIDAS-verordening. Het Nederlandse stelsel voor toelating van een private EDI-wallet wordt ontwikkeld door het programma EDI-stelsel NL.

Dienstverleners worden ontzorgd doordat al deze inlogmiddelen via de TVS ontsloten kunnen worden. Burgers moeten echter zelf hun weg vinden in dit landschap van inlogmiddelen en begrijpen welk inlogmiddel gebruikt kan worden voor welk beschermingsniveau en om in te loggen namens een ander.

Advies: Versnel de uitvoering van het programma door focus aan te brengen op burgerperspectief

Wij adviseren u om de beperkte beschikbaarheid van middelen en expertise optimaal in te zetten zodat burgers zo snel mogelijk betere inlogmogelijkheden krijgen voor digitale toegang tot de overheid. Zorg daarbij voor een goede balans tussen de zorgplicht van de overheid voor het beschermen van de gegevens van burgers en bedrijven, en de politieke wens om de burger en het bedrijf keuzevrijheid te geven bij het selecteren van een inlogmiddel.

1. *Lever zo snel mogelijk functionaliteit waar burgers en bedrijven om vragen.*

De digitale infrastructuur voor inloggen is zó belangrijk voor Nederland dat verbeteringen sneller gerealiseerd moeten worden. Burgers en maatschappelijke instellingen vragen al jaren om betere inlogmogelijkheden voor bevoegden. Daarnaast staat Logius aan de vooravond van nieuwe investeringen in DigiD en moet Nederland, ook met uitstel, aan de deadlines in de eIDAS-verordening gaan voldoen. Het is daarom urgent dat de directie Digitale Overheid keuzes maakt over het gewenste toekomstige gebruik van inlogmiddelen en daarop stuurt.

Wij adviseren u de volgende prioriteiten aan te houden bij de uitrol van deze functionaliteiten:

- Zorg dat het gebruik van de BVD in de zorg een succes wordt. Beperk de BVD voor 12+ tot het ontsluiten van de bevoegdheidsregisters, zodat een dienstverlener zelf op basis van de juiste informatie autorisatie kan verlenen. De BVD voor 12-, die binnenkort beproefd wordt, kan blijven zoals die is zodat deze relatief grote groep met één keer inloggen direct toegang heeft tot alle gegevens.
- Gebruik het EDI-stelsel als een publiek en privaat alternatief voor DigiD. Een investering in de EDI-wallet geeft de beste waarborgen omdat Nederland zich verplicht heeft tot de invoering hiervan. De vertraging die mogelijk wordt opgelopen doordat de aansluitvoorwaarden voor de EDI-wallet nog niet bekend zijn, kan worden ingelopen met een goed voorbereide implementatie.
- Beperk de doelgroep van de TVS tot de zorg, want daar zit de waarde; maak geen uitbreiding naar een stelsel.

Met deze focus moeten burgers voor de einddatum van het programma kunnen inloggen namens een ander met een inlogmiddel van hun keuze. Wij denken dat het aanbrengen van deze focus leidt tot een betere beheersing van de kosten en daarmee tegemoetkomt aan de taakstelling die ministeries deze kabinetsperiode opgelegd krijgen. Zorg ervoor dat de programma- en beheerkosten zijn vastgelegd met dekking in een departementale begroting.

2. *Houd rekening met de wallet bij de doorontwikkeling van de voorzieningen*

De voorzieningen die het programma Stelsel Toegang ontwikkelt moeten rekening houden met de komst van de EDI-wallet en de zorgplicht van de overheid voor gegevensbescherming. Wij adviseren het volgende:

- Zorg dat praktijkbeproevingen met de EDI-wallet op korte termijn in een gecontroleerde omgeving kunnen starten. Deze praktijkproeven staan in de startblokken. Door nu proactief te zijn kan Nederland meer invloed uitoefenen op de verdere realisatie van EDI-stelsel en -wallet in Europa. Het nog niet compleet beschikbaar zijn van alle technische specificaties is geen reden om deze proeven uit te stellen.
- Zorg dat de EDI-wallet kan omgaan met bevoegdheden uit de registers die de BVD ontsluit door, bijvoorbeeld, een bevoegdheidscertificaat te genereren voor de wallet.
- Richt naast het balieproces voor PIN-reset een balieproces in om de EDI-wallet met een hoog betrouwbaarheidsniveau te kunnen activeren. Hierdoor kunnen veel meer mensen zich op een gebruikersvriendelijke manier identificeren en het hoge niveau gaan gebruiken. Zo ontstaat er een alternatieve route naast het gebruik van DigiD Hoog. Regel de benodigde financiering voor deze aanpassing.
- Ontwikkel een andere aanpak om fraude met wallets te bestrijden want de CMB is hiervoor in de huidige vorm niet inzetbaar.
- Versnel de activiteiten om de TVS aan te kunnen sluiten op de EDI-wallet.

3. *Creëer duidelijkheid over het geheel aan inlogmiddelen dat beschikbaar komt*

Ontwikkel een visie inclusief roadmap waarin duidelijk staat wat de inlogmiddelen voor de komende tien jaar zijn. Stem deze af met de Eerste en Tweede Kamer en communiceer vervolgens richting burgers en bedrijven:

- een duidelijke releaseplanning voor het gehele programma aan alle stakeholders;
- welke inlogmiddelen er blijven en wanneer nieuwe beschikbaar komen, in lijn met advies 1;
- op grond van welke overwegingen een burger kan kiezen voor welk inlogmiddel;
- welke ambities de overheid heeft in het beschikbaar stellen van inlogmiddelen;
- welke voorzieningen er zijn voor mensen die geen gebruik willen of kunnen maken van digitale voorzieningen;
- of dienstverleners de TVS-voorziening verplicht moeten gebruiken;
- vanaf wanneer burgers ook zonder een account van een Amerikaans bedrijf, op diverse apparaten, gebruik kunnen maken van publieke inlogmiddelen die ontwikkeld worden binnen domein Toegang.

Ontwikkel een publiekscampagne over bovenstaande punten. Overweeg daarbij het sterke merk DigiD in te zetten voor de naamgeving van de publieke NL-wallet omdat dit herkenbaar is voor burgers en bedrijven.

Verder adviseren wij het programma om voorzieningen te benoemen naar hun functie en niet naar het programma waarin ze worden gerealiseerd. Dit helpt de buitenwereld om te begrijpen waar het over gaat.

***

Vanwege de grote maatschappelijke relevantie van veilig inloggen voor burgers was het van belang dat het onderzoeksteam een brede kijk op dit onderwerp kon ontwikkelen. Hiertoe hebben wij veel stakeholders gesproken die hun kennis van dit vakgebied en ervaring met het Programma Stelsel Toegang met ons hebben gedeeld. Wij willen alle geïnterviewden bedanken voor hun medewerking en openheid. Zij hebben hiermee een bijdrage geleverd aan dit advies.

Ten slotte: Het opvolgen van deze adviezen vraagt om een intensievere samenwerking met het programma EDI-wallet. Dit programma valt vanaf 1 januari 2027 onder een ander departement, namelijk het ministerie van Economische Zaken. Wij adviseren beide staatssecretarissen de sturing op deze programma's gezamenlijk op te pakken omdat er veel afhankelijkheden bestaan tussen de twee programma's.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

Adri de Bruijn
Voorzitter

w.g.

Sander van Amerongen
Secretaris-directeur

Adviescollege ICT-toetsing

Bijlage

Datum
26 oktober 2026

Kenmerk
2026-0000576419

Informatie over Programma Stelsel Toegang

Nr.	Onderwerp	Toelichting
1.	Projectnaam	Programma Stelsel Toegang
2.	Opdrachtgever	Programma is de directeur Digitale Overheid
3.	Startdatum project	1-1-2023
4.	Einddatum project	1-1-2028
5.	Type project	Vernieuwing
6.	Fase Project	Realisatie
7.	Totaal budget	€ 60,7 miljoen (bestaande uit het toegekende budget tot nu toe van 51,7 en het voor 2027 aangevraagde budget van 9 miljoen)
8.	Reeds uitgegeven per datum	€ 37,6 miljoen per 31-12-2025
9.	Doelstelling	De organisatorische en technische inrichting om aan de Wet digitale overheid te voldoen
10.	Maatschappelijke/ beleidsdoelstelling	Zorgen voor veilige en betrouwbare digitale toegang tot publieke diensten
11.	Meetbare baten	Niet gedefinieerd
12.	Huidige technologie/ architectuur	Verschillend per onderdeel/voorziening
13.	Doeltechnologie/- architectuur	Doelarchitectuur ICT-voorzieningen en werking Stelsel Toegang, versie 1.0, 22 maart 2024
14.	Omvang systeem	Niet onderzocht
15.	Aantal gebruikers	Alle Nederlanders en anderen die gebruikmaken van digitale dienstverlening van de overheid
16.	Belanghebbenden	Burgers en bedrijven
17.	Aanbesteding voorzien	Nee

Informatie over het uitgevoerde onderzoek

Nr.	Onderwerp	Toelichting
1.	Type onderzoek	Project; conform artikel 7, lid 1 sub a2 Wet Adviescollege ICT- toetsing
2.	Aanmelddatum	27-06-2025
3.	Start onderzoek	14-04-2026
4.	Afronden onderzoek	3-8-2026
5.	Datum conceptadvies	1-10-2026
6.	Datum definitief advies	26-10-2026
7.	Eerder onderzoek	Advies over het programma EDI-stelsel NL (2025)
8.	Onderzoeksmethode	Desk research, interviews.