



DigiD Checklist Testen

[DigiD Checklist Testen](#)

Deze pagina bevat de testcriteria die Logius aan de aansluiting van een webdienst op DigiD stelt. Deze testcriteria dragen bij aan een veilig, eenduidig en correct gebruik van DigiD.

Deze pagina is bedoeld voor zowel aansluitingen op het SAML v2.0 koppelvlak van DigiD als op het CGI koppelvlak van DigiD. Nieuwe aansluitingen vinden plaats op het SAML v2.0 koppelvlak.

Deze criteria gelden voor aansluitingen aangevraagd tot 1 december 2022. Daarna geldt de [Checklist aansluiten op DigiD en DigiD Machtigen](#).

Versiegegevens

Publicatiedatum: 28-12-2021

Versie: 7.0

Inleiding

Doelgroep en gebruik van deze pagina

Deze checklist is bedoeld voor:

- overheidsinstellingen en organisaties met een publiekrechtelijke taak (hierna: dienstaanbieders) die gebruik willen maken van DigiD als authenticatiemiddel;
- leveranciers die aansluitingen ontwikkelen voor dienstaanbieders.

Ontwikkelaars van een webdienst gebruiken de checklist voor zelfcontrole. Logius controleert periodiek en bij elke nieuwe aansluiting of een aansluiting aan de criteria in deze checklist voldoet.

Let op: de dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de systemen die op DigiD aansluiten.

Gerelateerde pagina's

- [Handleiding aansluiten DigiD](#)
- [Koppelvlakspecificatie SAML](#)

De laatste versie van deze pagina

Logius verbetert en verduidelijkt deze pagina met regelmaat. Logius informeert dienstaanbieders per e-mail alleen bij wijzigingen met een grote impact. Controleer daarom zelf regelmatig of er een nieuwe versie van deze pagina op de website van Logius staat.

Verbetersuggesties

Logius ontvangt graag uw suggesties om deze pagina te verbeteren. U kunt hiervoor contact opnemen met [Logius](#).

Testcriteria voor DigiD-aansluitingen

Testcriteria voor communicatie

Testcriterium	Toelichting
C1 Geen testdata of "under Construction"-teksten	De pagina's van de webapplicatie direct voor en na het inloggen op DigiD bevatten geen teksten of plaatjes die aangeven dat de site "under construction" is. Deze pagina's bevatten ook geen testgegevens of links naar testpagina's. <i>Opmerking: dit criterium is niet vereist in de preproductieomgeving van DigiD.</i>
C2 Deeplinks	Indien de website of applicatie gebruikmaakt van deeplinks naar DigiD, dan verwijzen deze naar https://www.digid.nl , en niet direct naar de betreffende pagina's.

- C3 Schrijfwijze
- Schrijf DigiD aan elkaar met twee hoofdletters 'D'.
 - Schrijf over 'DigiD' in plaats van bijvoorbeeld 'de DigiD'.

Op elke plaats waar u doorverwijst naar DigiD voor authenticatie gebruikt u onderstaand logo:

- C4 Logo
- Dit logo is te downloaden op: <https://logius.nl/diensten/digid/documentatie> Afmetingen zijn minimaal 20x20 pixels, gangbaar is 100x100 pixels. Naast het logo geeft u een link die doorverwijst naar het inlogscherm van DigiD. Link en logo staan zodanig bij elkaar dat de gebruiker er vanuit kan gaan dat deze voor het inloggen via DigiD is. Afmetingen minimaal 20x20 pixels en gangbaar 100x100 pixels.
- Veelgestelde C5 vragen en helpdesk
- Er staan geen veelgestelde vragen over DigiD op uw website. Indien hier iets over vermeld moet worden is alleen een verwijzing naar <https://www.digid.nl/> toegestaan.
 - U vermeldt nergens het telefoonnummer of e-mailadres van de DigiD-servicedesk op uw website.

Technische testcriteria

Testcriterium	Toelichting
T1 Browserondersteuning	De pagina waarin u verwijst naar DigiD, wordt correct weergegeven in de top-95% van de meestgebruikte versies van browsers . (NB: Voor SSL-verbindingen zijn alle volgende punten verplicht. Voor CGI-aansluitingen zijn de eerste drie punten niet verplicht. Wij adviseren echter om wel aan deze punten te voldoen.)
T2 U moet een <i>zichtbaar</i> beveiligde verbinding hebben, zich uitend in:	• De URL moet het https-protocol tonen en het beveiligde symbool (het slotje) van het gebruikte certificaat moet zichtbaar zijn in de browser (zowel op de pagina voor als op de pagina na het inloggen) • Een https-verbinding (TLS 1.2 ondersteund) • Geldig SSL-certificaat • Geen certificaat-foutmeldingen voor de gebruiker • Het hoofddomein moet op naam staan van de dienstaanbieder (dus niet de leverancier).
T3 Geen frames	De inlogschermen van DigiD worden niet in een frame gepresenteerd aan de gebruiker. Het adres https://www.digid.nl is zichtbaar in de adresbalk van de gebruiker.
T4 Geen pop-up, nieuw window of tabblad voor inlogscherm DigiD	Na doorverwijzen vanuit de dienstaanbieder wordt het inlogscherm van DigiD in hetzelfde window getoond aan de gebruiker, dus niet in een pop-up, nieuw window of tabblad.
T5 Naam van de organisatie	Op de eerste inlogpagina van DigiD staat de naam van de dienstaanbieder waar de gebruiker gaat inloggen. Indien DigiD een resultcode teruggeeft aan de webapplicatie (met uitzondering van SAML-statuscodes "Authnfailed" en "Succes" en CGI-statuscodes 0000 en 0040) bevat de pagina die wordt getoond de letterlijke foutmelding "Er is een fout opgetreden in de communicatie met DigiD. Probeert u het later nogmaals. Indien deze fout blijft aanhouden, kijk dan op de website https://www.digid.nl voor de laatste informatie."
T6 Foutmelding	De lokale sessie is hierna beëindigd, een gebruiker dient opnieuw in te loggen.
T7 Schermgedrag bij annuleren	Als de gebruiker het authenticatieproces annuleert (SAML-statuscode "AuthnFailed" of CGI-statuscode 0040), komt de gebruiker terug in het scherm vanwaar getracht is de authenticatie te starten. Dit gebeurt in hetzelfde browserscherm. Er dient een melding getoond te worden met de mededeling dat het inloggen is geannuleerd.
T8 Juiste aanroep-URL	De webapplicatie roept de DigiD-authenticatiepagina aan via de URL die wordt genoemd in de metadata van DigiD (voor SAML) of de bevestigingsbrief van Logius (voor CGI).
T9 Geen veldwaarden in de URL (Alleen voor CGI)	De veldwaarden appId of het shared secret worden niet door de webapplicatie in de URL of op het scherm getoond.
T10 Rechtstreekse invoer door gebruiker	De gebruiker moet zijn/haar inloggegevens rechtstreeks op het inlogscherm van DigiD invoeren.

De gebruiker wordt na het inloggen geredirect naar de inlogpagina van DigiD en na succesvolle authenticatie naar een pagina binnen hetzelfde domein. Dit geldt ook bij niet-succesvolle authenticatie of bij annuleren. Voorbeeld van stapsgewijze routing zoals toegestaan:

- <https://webpagina.nl/inloggenvoordigid>
- <https://www.digid.nl/mijn-digid/>
- <https://webpagina.nl/ingelogd>

Niet toegestaan is dus:

- T11 Redirect binnen domein
- <https://webpagina.nl/inloggenvoordigid>
 - <https://anderepagina.nl/...>
 - <https://www.did.nl/mijn-digid>
 - <https://webpagina.nl/ingelogd>

Daarnaast is ook link tracking, het loggen van DigiD-surfgedrag, niet toegestaan. Bijvoorbeeld:

- <https://webpagina.nl/inloggenvoordigid>
- <https://verzamelstatistieken.nl>
- <https://www.digid.nl/mijn-digid/>
- <https://webpagina.nl/ingelogd>

- T12 De authenticatie slaagt
- Het authenticatieproces verloopt conform de koppelvlakspecificaties (zie paragraaf 1.3). De gebruiker kan inloggen bij DigiD en de dienst aanbieder ontvangt na een succesvolle authenticatie een reactie van DigiD met een sectoraal nummer.

De dienst aanbieder bepaalt het minimale betrouwbaarheidsniveau. De burger mag er altijd voor kiezen om op een hoger niveau in te loggen. Bijvoorbeeld:

- T13 Betrouwbaarheidsniveaus correct afgehandeld
- De dienst aanbieder vereist niveau Midden □ de gebruiker kan enkel met Midden inloggen.
 - De dienst aanbieder vereist niveau Basis □ de gebruiker kan zowel met Basis als met Midden inloggen.

- T14 Uitloggen
- Er dient vanaf het moment van inloggen met DigiD en voor de duur van de sessie op het scherm van de dienst aanbieder een mogelijkheid getoond te worden om uit te loggen. Deze uitlogmogelijkheid beëindigt de lopende sessie.

- T15 Sessieduur
- Na het inloggen houdt de webapplicatie een sessie met de gebruiker bij. Na maximaal vijftien minuten inactiviteit verloopt de sessie. Bij uitloggen of als alle actieve browserschermen afgesloten worden, vervalt de sessie ook.

Testcriteria voor app2app

Uitgangspunt is dat een app2app-aansluiting wordt toegevoegd aan een al bestaande – en geteste – DigiD aansluiting. De app2app-aansluiting zal niet aan een uitgebreide test onderworpen worden, omdat de reguliere DigiD-aansluiting al voldoet aan de gestelde eisen. De afnemerapp zal slechts getoetst worden op de onderstaande voorwaarden.

Testcriterium	Toelichting
	Schrijf DigiD aan elkaar met twee hoofdletters 'D'.
A1 Schrijfwijze DigiD	Schrijf over 'DigiD' in plaats van bijvoorbeeld 'de DigiD'. Schrijf over 'DigiD app' (app met alleen kleine letters.) DigiD-logo: Op elke plaats waar u doorverwijst naar de DigiD app voor authenticatie gebruikt u onderstaand logo: □ Dit logo is te downloaden op: https://logius.nl/diensten/digid/documentatie
A2 Logo's	Minimale afmeting is 20x20 pixels, gangbaar is 100x100 pixels. Afnemerlogo: De afnemer dient een app-icoon het authenticatieverzoek mee te sturen zodat de DigiD app dat kan tonen tijdens inloggen. De afmetingen van dat afnemerlogo mogen maximaal 512 x 512 pixels zijn en het logo dient als een vierkant aangeleverd te worden. De DigiD app schaalt het logo naar 80 x 80 en plaatst er een raster overheen om het afgeronde hoeken te geven.

Er staan geen veel gestelde vragen over DigiD in de afnemer app. Alleen een verwijzing naar de website van DigiD (homepage) is toegestaan:

A3 Verwijzingen naar DigiD-informatie <https://www.digid.nl>

Nergens staat het telefoonnummer of e-mailadres van de DigiD-servicedesk vermeld in de afnemer app.

A4 Gebruik universal links (iOS) of Android app links Het aanroepen van de DigiD app door de afnemer app en vice versa verloopt via iOS universal links of Android app links. Dit vereist dat de afnemer app geregistreerd staat in de App Store en/of Google Play.

A5 Naam DigiD aansluiting Op het bevestigingsscherm in de DigiD app staan de naam van de afnemer app, zoals dat bij registratie is opgegeven, en het app-icoon dat de afnemer met het authenticatieverzoek meestuurt.

De naam moet onderscheidend en uniek zijn.

Afkortingen en definities

Woord/afkorting	Betekenis
CSP	Certificate Service Provider
CGI	Common Gateway Interface
SAML	Security Assertion Markup Language; Internationale standaard voor het uitwisselen van berichten met beveiligingsgegevens en informatie over eindgebruikers.
DigiD Basis	Betrouwbaarheidsniveau voor authenticeren op basis van inlognaam plus wachtwoord Betrouwbaarheidsniveau voor authenticeren op basis van:
DigiD Midden	• inlognaam plus wachtwoord plus sms-code • DigiD app
DigiD Substantieel	Betrouwbaarheidsniveau voor authenticeren op basis van DigiD app, waarvoor éénmalig een ID-check is uitgevoerd
DigiD Hoog	Betrouwbaarheidsniveau voor authenticeren op basis van een fysiek identiteitsdocument.

Website url: <https://www.logius.nl>

Print datum: 19/04/2024 04:48:43