Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DigiD Checklist Testen

Datum	11-05-2020
Versie	7.0
Status	Definitief

Colofon

Projectnaam	DigiD
Versienummer	7.0
Organisatie	Logius Postbus 96810 2509JE DEN HAAG servicecentrum@logius.nl 0900 555 4555 (10 ct p/m)

Inhoud

1 Inleiding

1.1 Doel van dit document

Dit document 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.

Dit document 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.

1.2 Doelgroep en gebruik van dit document

Deze Checklist Testen 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.

1.3 Gerelateerde documenten

Document	Inhoud
Handleiding aansluiten DigiD	Een stap-voor-stap handleiding voor het aansluiten op DigiD
Koppelvlakspecificatie SAML	De specificaties van het SAML-koppelvlak
Koppelvlakspecificatie CGI	De specificaties van het CGI-koppelvlak

Deze documenten zijn te vinden op https://www.logius.nl/diensten/digid/documentatie.

1.4 De laatste versie van dit document

Logius verbetert en verduidelijkt dit document 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 dit document op de website van Logius staat (https://www.logius.nl/diensten/digid/documentatie).

1.5 Verbetersuggesties

Logius ontvangt graag uw suggesties om dit document te verbeteren. U kunt hiervoor contact opnemen met Servicecentrum Logius via servicecentrum@logius.nl.

2 Testcriteria voor DigiD-aansluitingen

2.1 Testcriteria voor communicatie

	Testcriterium	✓	Toelichting op testresultaat
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. *Opmerking: dit criterium is niet vereist in de preproductieomgeving van DigiD.*	❑	
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'.	❑	
C4	**Logo** Op elke plaats waar u doorverwijst naar DigiD voor authenticatie gebruikt u onderstaand logo:  Dit logo is te downloaden op https://www.logius.nl/diensten/digid/wie-doet-wat. Minimale afmeting is 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 link voor het inloggen via DigiD is.		
C5	**Veelgestelde 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.	❑	

2.2 Technische testcriteria

	Testcriterium	✓	Toelichting op testresultaat
T1	**Browserondersteuning** De pagina waarin u verwijst naar DigiD wordt correct weergegeven in 95 procent van de meestgebruikte versies van browsers.	❑	
T2	**U dient een *zichtbaar* beveiligde verbinding te hebben, zich uitend in:** (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.) • de URL moet het https-protocol tonen en het beveiligde symbool (het slotje) van het gebruikte PKIoverheid-certificaat moet zichtbaar zijn in de browser (zowel op de pagina voor als op de pagina na het inloggen); • een https-verbinding (TLS 1.0 en/of 1.2 ondersteund); • een geldig SSL-certificaat, uitgegeven door een CSP binnen de PKIoverheid en op naam gesteld van de dienstaanbieder; • 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.	❑	
T6	**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.	❑	
T7	**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).	❑	

	Testcriterium	✓	Toelichting op testresultaat
T8	**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.	❑	
T9	**Rechtstreekse invoer door gebruiker** De gebruiker moet zijn/haar inloggegevens rechtstreeks op het inlogscherm van DigiD invoeren.	❑	
T10	**Redirect binnen domein** 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 routering zoals toegestaan: https://webpagina/nl/inloggenvoordigid https://www.digid.nl/mijn-digid/ https://webpagina.nl/ingelogd Niet toegestaan is dus: https://webpagina.nl/inloggenvoordigid https://anderepagina.nl/... https://www.digid.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	❑	
T11	**De authenticatie slaagt** Het authenticatieproces verloopt conform de koppelvlakspecificaties. De gebruiker kan inloggen bij DigiD en de dienstaanbieder ontvangt na een succesvolle authenticatie een reactie van DigiD met een sectoraal nummer.	❑	
T12	**Betrouwbaarheidsniveaus correct afgehandeld** De dienstaanbieder bepaalt het minimale betrouwbaarheidsniveau. De burger mag er altijd voor kiezen om op een hoger niveau in te loggen. Bijvoorbeeld: De dienstaanbieder vereist niveau Midden → de gebruiker kan enkel met Midden inloggen. De dienstaanbieder vereist niveau Basis → de gebruiker kan zowel met Basis als met Midden inloggen.	❑	

	Testcriterium	✓	Toelichting op testresultaat
T13	**Uitloggen** Er dient vanaf het moment van inloggen met DigiD en voor de duur van de sessie op het scherm van de dienstaanbieder een mogelijkheid getoond te worden om uit te loggen. Deze uitlogmogelijkheid beëindigt de lopende sessie.	❑	
T14	**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.	❑	

2.3 Testcriteria alleen voor AML-variant DigiD Eenmalig inloggen

Nr	Testcriterium	✓	Toelichting op testresultaat
EI1	**Gebruiker kan van meerdere diensten van verschillende dienstaanbieders gebruik maken door eenmalig in te loggen.** Gebruiker is ingelogd bij dienstaanbieder X. Open een nieuw tabblad of browserscherm. Log in bij dienstaanbieder Y. De gebruiker is nu ook ingelogd bij dienstaanbieder Y zonder opnieuw zijn login-gegevens te moeten invoeren.	❑	
EI2	**Gebruiker kan na bij meerdere dienstaanbieders ingelogd te zijn bij allemaal uitloggen door bij één van de dienstaanbieders uit te loggen.** Gebruiker is ingelogd bij dienstaanbieder X en bij dienstaanbieder Y in twee verschillende browserschermen en/of tabbladen. Gebruiker klikt op uitloglink- en/of –knop en logt uit bij dienstaanbieder X of Y. Gebruiker wordt teruggeleid naar de DigiD-uitlogpagina waar wordt aangegeven bij welke partij er nog meer is ingelogd en de mogelijkheid wordt getoond om bij alle ingelogde dienstaanbieders uit te loggen. Na uitloggen bij dienstaanbieder X is de gebruiker ook uitgelogd bij dienstaanbieder Y. Na uitloggen bij dienstaanbieder Y is de gebruiker ook uitgelogd bij dienstaanbieder X.	❑	
EI3	**Gebruiker dient zich opnieuw te authentiseren indien na de eerste keer ingelogd te zijn bij een dienstaanbieder getracht wordt in te loggen bij een andere dienstaanbieder waar een hoger betrouwbaarheidsniveau geldt.** De dienstaanbieder bepaalt het minimale betrouwbaarheidsniveau. De burger mag er altijd voor kiezen om op een hoger niveau in te loggen. Bijvoorbeeld: De dienstaanbieder vereist niveau Midden -> de gebruiker kan enkel met niveau Midden inloggen.	❑	

2.4 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 op testresultaat**
A1	**Schrijfwijze DigiD** Schrijf DigiD aan elkaar met twee hoofdletters 'D'. Schrijf over 'DigiD' in plaats van bijvoorbeeld 'de DigiD'. Schrijf over 'DigiD app' (app met alleen kleine letters.)	❑	
A2	**Logo's** 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://www.logius.nl/diensten/digid/wie-doet-wat. 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.		
A3	**Verwijzingen naar DigiD-informatie** Er staan geen veel gestelde vragen over DigiD in de afnemer app. Alleen een verwijzing naar de website van DigiD (homepage) is toegestaan: 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.	❑	

3 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
DigiD Midden	Betrouwbaarheidsniveau voor authenticeren op basis van: • 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.