

Checklist Testen Routeringsvoorziening TVS

Versie: 2.0

Datum: 16-04-2024

Status: Definitief

Voor vragen kunt u mailen naar tvsv@dictu.nl

Inhoud

1 Inleiding	3
1.1 Doel van dit document	3
1.2 Doelgroep en gebruik van dit document	3
1.3 Gerelateerde documenten	3
1.4 De laatste versie van dit document	3
1.5 Verbetersuggesties.....	3
2 Testcriteria voor aansluiten op TVS	4
2.1 Gegevens van uw aansluiting.....	4
2.2 Communicatie	5
2.3 Browser.....	6
2.4 DigiD en DigiD Machtigen	9
2.5 eTD diensten.....	12

1 Inleiding

1.1 Doel van dit document

Dit document bevat de testcriteria die DICTU aan de aansluiting van een ICT Software leverancier of een individuele dienstverlener op de routeringsvoorziening TVS stelt. Deze testcriteria dragen bij aan een veilig, eenduidig en correct gebruik van TVS en de achterliggende authenticatiediensten.

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 de Routeringsdienst TVS waarmee alle door Wdo erkende inlogmiddelen worden ontsloten als authenticatiediensten;
- Leveranciers die aansluitingen ontwikkelen voor dienstaanbieders.

Ontwikkelaars van een webdienst gebruiken de checklist voor zelfcontrole. DICTU 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 de Routeringsvoorziening TVS aansluiten.

1.3 Gerelateerde documenten

Document	Inhoud
Functionele beschrijving TVS	Dit document bevat informatie over de functie van TVS voor dienstverleners.
Toegang TVS t.b.v. beoordeling Checklist testen	Bevat aanvullende informatie voor het verlenen van toegang om de ingevulde checklist testen te kunnen controleren (o.a. te whitelisten IP-adressen en BSN's die toegang moeten krijgen)
TVS Keten Communicatiekanalen	In dit document kunt u lezen wie deze partners zijn en hoe u zich kunt aanmelden op hun communicatiekanalen.
Handleiding certificaatwissels op TVS	Dit document bevat meer informatie over het certificaatwisselproces op TVS.

Deze documenten zijn te vinden op: <https://dictu.nl/toegangverleningservice/documentatie-en-links>

1.4 De laatste versie van dit document

DICTU verbetert en verduidelijkt dit document met regelmaat. DICTU 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 DICTU staat.

1.5 Verbetersuggesties

DICTU ontvangt graag uw suggesties om dit document te verbeteren. U kunt hiervoor contact opnemen met DICTU via tvsv@dictu.nl.

2 Testcriteria voor aansluiten op TVS

2.1 Gegevens van uw aansluiting

Vul het formulier in en mail het aan tvsv@dictu.nl

TVSnummer :
.....

Uw gegevens

Naam :
.....

Telefoonnummer :
.....

Emailadres :
.....

Functie :
.....

Handtekening :
.....

De gevraagde gegevens vallen onder Privacy wet- en regelgeving welke is terug te vinden op dictu.nl/privacy.

2.2 Communicatie

Nr.	Testcriterium	✓	Toelichting
C1	<p>Geen testdata of "under construction"-teksten De pagina's of schermen voor en na de authenticatie bevatten geen teksten of plaatjes die aangeven dat de site "under construction" is. Deze bevatten ook geen testgegevens of links naar testpagina's of -schermen.</p> <p><i>Opmerking: geldt niet voor een preproductie-aansluiting.</i></p>	<input type="checkbox"/>	
C2	<p>Geen vermelding TVS Nergens op de website of in de webapplicatie wordt er vermelding gemaakt van de ToegangVerleningService of TVS.</p>	<input type="checkbox"/>	
C3	<p>Geen deeplinks Links naar authenticatiediensten voor 'meer informatie' verwijzen</p> <ul style="list-style-type: none"> • voor DigiD naar https://digid.nl • voor Machtigen naar https://machtigen.digid.nl (dus niet direct naar de betreffende pagina's) • voor eHerkenning naar https://www.eherkenning.nl 	<input type="checkbox"/>	
C4	<p>Geen uitleg en geen bereikbaarheidsgegevens Afnemer geeft nergens uitleg (zoals veelgestelde vragen) over DigiD en/of Machtigen en/of eHerkenning en/of de ToegangVerleningService (TVS). En nergens worden bereikbaarheidsgegevens (zoals het telefoonnummer of e-mailadres) van de authenticatiediensten- en/of DICTU-Servicedesk vermeld.</p> <ul style="list-style-type: none"> • Indien er iets over DigiD of Machtigen moet worden vermeld, wordt voor DigiD verwezen naar https://digid.nl • en voor Machtigen naar https://machtigen.digid.nl • voor eHerkenning wordt er verwezen naar https://www.eherkenning.nl/nl 	<input type="checkbox"/>	
C5	<p>Gebruik app stores De app met TVS-toegang mag alleen via de officiële appstores van Apple voor iOS en Google voor Android worden gedistribueerd.</p>	<input type="checkbox"/>	

2.3 Browser

Nr.	Testcriterium	✓	Toelichting
T1	Betrouwbare verbinding De inlogpagina van Afnemer met (de link naar) de authenticatiedienst is beveiligd met een geldig TLS-certificaat op een domein met DNSSEC. Het gebruikte certificaat veroorzaakt geen (fout)meldingen in de browser over de status of geldigheid van het certificaat. De URL van het hoofd- en eventuele subdomein mogen geen verwijzingen naar authenticatiediensten en TVS bevatten.	<input type="checkbox"/>	
T2	Toegankelijkheid inlogpagina De inlogpagina van Afnemer met (de link naar) de authenticatiedienst heeft geen onderbrekingen zoals een pop-up, nieuw window of tabblad.	<input type="checkbox"/>	
T3	Schermgedrag bij annuleren Als de gebruiker het authenticatieproces annuleert (SAML-statuscode "AuthnFailed"), komt de gebruiker terug op de inlogpagina 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.	<input type="checkbox"/>	
T4	Juiste aanroep-URL De webapplicatie roept de TVS-authenticatiepagina aan via de URL die wordt genoemd in de metadata van TVS (voor SAML). De aanroep moet rechtstreeks plaatsvinden, dus zonder tussenkomst van andere URL's of domeinen (dus zonder forwarding of redirects).	<input type="checkbox"/>	



T5	<p>Redirect binnen domein</p> <p>De gebruiker wordt bij het inloggen geredirect naar de inlogpagina van de authenticatiedienst en na succesvolle authenticatie naar een pagina binnen hetzelfde domein. Dit geldt ook bij niet-succesvolle authenticatie of bij annuleren. De redirects moet plaatsvinden zonder tussenkomst van andere URL's of domeinen (dus zonder forwarding of redirects).</p> <p>Voorbeeld van stapsgewijze flow zoals toegestaan:</p> <ul style="list-style-type: none"> • https://webpagina.nl/inloggenvoordigid • https://www.digid.nl/inloggen • https://webpagina.nl/ingelogd <p>Voorbeeld van stapsgewijze flow zoals ook toegestaan:</p> <ul style="list-style-type: none"> • https://webpagina.nl/inloggenvoordigid of https://inloggen.webpagina.nl/ • https://www.digid.nl/inloggen • https://ingelogd.webpagina.nl/ <p>Niet toegestaan is:</p> <ul style="list-style-type: none"> • https://webpagina.nl/inloggenvoordigid • https://anderepagina.nl • https://www.digid.nl/inloggen • https://webpagina.nl/ingelogd 	<input type="checkbox"/>	
T6	<p>De authenticatie slaagt</p> <p>Het authenticatieproces verloopt conform de koppelvlakspecificaties. De gebruiker kan inloggen en de dienst aanbieder ontvangt na een succesvolle authenticatie een reactie van de authenticatiedienst.</p>	<input type="checkbox"/>	
T7	<p>Betrouwbaarheidsniveaus correct afgehandeld</p> <p>De Afnemer bepaalt het minimale betrouwbaarheidsniveau. De burger mag altijd op een hoger niveau inloggen.</p> <p>Bijvoorbeeld:</p> <ul style="list-style-type: none"> • De Afnemer vereist niveau Laag met een tweede factor: de gebruiker kan inloggen met Laag met tweede factor, met Substantieel en met Hoog. • De Afnemer vereist niveau Substantieel: de gebruiker kan inloggen met Substantieel en met Hoog, maar niet met Laag. 	<input type="checkbox"/>	

T8	<p>Uitlogmogelijkheid</p> <p>Er dient vanaf het moment van inloggen met TVS en voor de duur van de sessie op het scherm van Afnemer een mogelijkheid getoond te worden om uit te loggen. Deze uitlogmogelijkheid beëindigt de lopende sessie.</p>	<input type="checkbox"/>	
T9	<p>Sessieduur</p> <p>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.</p>	<input type="checkbox"/>	
T10	<p>Automatisch uitloggen</p> <p>Als na inloggen blijkt dat Afnemer de Gebruiker niet in behandeling neemt of als de behandeling beëindigt, moet dit direct aan de gebruiker worden gemeld en moet de gebruiker worden uitgelogd.</p>	<input type="checkbox"/>	
T11	<p>Navigatiekliks</p> <p>Het inlogportaal van de authenticatiedienst of de TVS Smartloginpagina moet met maximaal 2 navigatie kliks benaderbaar zijn.</p> <p>Voorbeeld: Homepage -> Patiëntenportaal -> Inlogpagina authenticatiedienst (of TVS Smartlogin)</p>	<input type="checkbox"/>	
T12	<p>Geen meerdere inlogknoppen</p> <p>Bij gebruik van de TVS Smartloginfunctionaliteit mag er maar één inlogknop aanwezig zijn die direct doorverwijst naar de TVS Smartloginpagina. Deze knop mag alleen het geschreven woord "inloggen" bevatten. Naast deze knop mogen er wel inlogknoppen aanwezig zijn voor eigen inlogmiddelen.</p>	<input type="checkbox"/>	

2.4 DigiD en DigiD Machtigen

De volgende controles zijn alleen van toepassing op aansluitingen waarbij de authenticatiediensten DigiD en/of DigiD Machtigen zijn geactiveerd.



Nr.	Testcriterium	✓	Toelichting
L1	Beveiligingsrichtlijnen <ul style="list-style-type: none">Op het systeem met DigiD en/of Machtigen toegang, moet de Norm ICT-beveiligingsassessments DigiD worden toegepast.Op de webapplicatie moeten de ICT beveiligingsrichtlijnen van de NCSC worden toegepast.Op de app moeten de ICT-beveiligingsrichtlijnen van de NCSC worden toegepast. <p>U past de basismaatregelen cybersecurity van de NCSC toe.</p>	<input type="checkbox"/>	
L2	Geen propagatie of afgeleide of verlengde toegang <p>De persoonsgegevens, zoals vermeld in het Besluit verwerking persoonsgegevens GDI, hoofdstuk 3, artikel 6 en 7, die na een succesvolle authenticatie met DigiD of Machtigen beschikbaar komen voor Afnemer en/of Gebruiker, mogen alleen worden gebruikt tijdens die sessie. Indien Gebruiker daarna (op een later tijdstip) deze gegevens of een afgeleide vorm daarvan hergebruikt in hetzelfde of een ander systeem, mag dit alleen:</p> <ul style="list-style-type: none">als Gebruiker zich opnieuw authentiseert op tenminste hetzelfde gewenste Betrouwbaarheidsniveau van de dienst volgens de aansluitvoorwaarden; en als het systeem voldoet aan de beveiligingsrichtlijnen van DigiD.	<input type="checkbox"/>	
L3	Schrijfwijze <ul style="list-style-type: none">DigiD wordt aan elkaar geschreven met twee hoofdletters 'D'. Schrijf 'DigiD' in plaats van bijvoorbeeld 'de DigiD'.Schrijf DigiD en Machtigen na elkaar met een spatie ertussen: 'DigiD Machtigen'	<input type="checkbox"/>	

L4	<p>Naam van de BSN- gerechtigde organisatie</p> <p>Bij de inlogmogelijkheid met (de link of knop naar) DigiD of Machtigen staat de naam van de BSN-gerechtigde Afnemer zoals deze is geregistreerd in de Autorisatielijst BSN-gerechtigden (ALB) van de RvIG. Dit mag niet de naam zijn van de verwerker of van de softwareleverancier.</p> <p>Indien u aansluit in de rol van een DVA vanuit het MedMij-stelsel moet er op de landingspagina duidelijk vermeld staan bij welke zorgaanbieder de persoon inlogt. Deze naam komt overeen met de naam van de zorgaanbieder op de inlogpagina van de authenticatiedienst.</p>	<input type="checkbox"/>	
L5	<p>Betrouwbare verbinding</p> <p>De inlogpagina van Afnemer met (de link naar) DigiD staat op een .nl domein met DNSSEC en is beveiligd met een geldig TLS-certificaat.</p> <p>De URL van het hoofd- en eventuele subdomein mogen geen verwijzingen naar DigiD bevatten, zoals: digi-d, digi.d, d.igi.d, diegiedee.</p>	<input type="checkbox"/>	
L6	<p>Logo</p> <p>Bij iedere doorverwijzing naar DigiD voor authenticatie toont u als dienstverlener het logo van DigiD en de tekst inloggen of inloggen als gemachtigde. Download dit logo in de Toolkit DigiD en DigiD Machtigen. Naast het logo geeft u een link die doorverwijst naar het inlogscherf van DigiD.</p>  <p>Op de pagina Stijlhandleiding aansluiten Toegang vindt u voorbeelden en vereisten voor het weergeven van inlogknoppen binnen het domein Toegang. Deze checklist helpt u met DigiD, Machtigen maar bijvoorbeeld ook met eIDAS, eHerkenning, ouderlijk gezag en bewindvoering.</p> <p><i>Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het DigiD logo al op deze pagina aanwezig is.</i></p>	<input type="checkbox"/>	
L7	<p>Logo App</p> <p>Bij het implementeren van een aansluiting op een mobiele app wordt op elke plek waar naar DigiD verwezen wordt voor authenticatie dit DigiD-logo gebruikt.</p> 	<input type="checkbox"/>	

	<p>Dit logo is te downloaden in de Toolkit DigiD en DigiD Machtigen. Minimale afmeting is 20x20 pixels, gangbaar is 100x100 pixels.</p> <p><i>Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het DigiD logo al op deze pagina aanwezig is.</i></p>		
L8	<p>Logo DigiD Machtigen</p> <p>Er bestaat geen logo voor Machtigen. Nergens gebruikt Afnemer een zelfgemaakt logo voor Machtigen.</p>	<input type="checkbox"/>	
L9	<p>Foutmelding DigiD</p> <p>Indien DigiD een resultcode teruggeeft aan de webapplicatie (met uitzondering van SAML-statuscodes "Authnfailed" en "Succes") bevat de pagina die wordt getoond de letterlijke foutmelding:</p> <p><i>"Inloggen bij deze organisatie is niet gelukt. Probeer u het later nog een keer. Lukt het nog steeds niet? Log in bij Mijn DigiD. Zo controleert u of uw DigiD goed werkt. Mogelijk is er een storing bij de organisatie waar u inlogt."</i></p> <p>De lokale sessie is hierna beëindigd, een gebruiker dient opnieuw in te loggen.</p>	<input type="checkbox"/>	

2.5 eTD diensten

De volgende controles* zijn uitsluitend van toepassing op aansluitingen waarbij de authenticatiediensten vanuit het eTD-stelsel, zoals eHerkenning en eIDAS, geactiveerd zijn.

Nr.	Testcriterium	✓	Toelichting
E1	<p>Beveiligingsrichtlijnen</p> <ul style="list-style-type: none"> Op de webapplicatie moeten de ICT beveiligingsrichtlijnen van de NCSC worden toegepast. Op de app moeten de ICT-beveiligingsrichtlijnen van de NCSC worden toegepast. <p>U past de basismaatregelen cybersecurity van de NCSC toe.</p>	<input type="checkbox"/>	
E2	<p>Logo eHerkenning</p> <p>Dit logo moet in de volgende situaties worden geplaatst:</p> <ul style="list-style-type: none"> Op webpagina's waar de gebruiker moet inloggen met een eHerkenning inlogmiddel. Op webpagina's die meerdere formulieren of diensten met eHerkenning aanbieden (let op: het logo hoeft dan niet per formulier te worden getoond). Op webpagina's waar de gebruiker zowel met eHerkenning als DigiD kan inloggen. Op webpagina's waar eHerkenning wordt toegelicht. Bij incidentele uitingen, zoals nieuwsberichten, is dit niet noodzakelijk <p></p> <p><i>Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het logo al op deze pagina aanwezig is.</i></p>	<input type="checkbox"/>	
E3	<p>Betrouwbaarheidsniveau</p> <p>U geeft aan met welk betrouwbaarheidsniveau uw klanten moeten inloggen. Hiervoor gebruikt u de vignetten betrouwbaarheidsniveaus.</p> <p></p> <p><i>Opmerking: bij gebruik van de TVS Smartloginpagina vervalt deze vereiste</i></p>	<input type="checkbox"/>	
E4	<p>Kernboodschap</p> <p>De volgende kernboodschap staat op uw website:</p> <p><i>Meer zekerheid over uw online identiteit, daarom gebruiken wij eHerkenning. Met eHerkenning identificeert u zich veilig en eenvoudig online. Het grote gemak is dat u met eHerkenning bij meerdere organisaties kunt inloggen. U hoeft dus minder wachtwoorden te onthouden. Veilig, makkelijk en betrouwbaar. Ga voor meer informatie naar www.eherkenning.nl.</i></p>	<input type="checkbox"/>	

Richtlijnen voor de dienstencatalogus

In de volgende stappen staan de verplichtingen en adviezen omtrent het invullen van de benodigde velden voor de dienstencatalogus

E5	Naam dienstverlener U dient een correcte, voor uw gebruikers te begrijpen naam in te vullen van uw organisatie. Deze naam wordt op volgende wijze getoond op het inlogscherf van eHerkenning: U wilt inloggen bij <Dienstverlenernaam> Bijvoorbeeld: <ul style="list-style-type: none">• U wilt inloggen bij Kamer van Koophandel	<input type="checkbox"/>	
E6	Naam webdienst U dient een correcte naam van uw dienst in te vullen die duidelijk en te begrijpen is voor uw gebruikers en overeenkomt met de naam van uw dienst op uw website. De dienstnaam moet een werkwoord bevatten en een omschrijving van het 'wat' gebruikers kunnen doen. Dienst: <werkwoord> + <wat kunnen uw gebruikers doen> Bijvoorbeeld: <ul style="list-style-type: none">• Aanvragen parkeervergunning• Melding doen openbare ruimte	<input type="checkbox"/>	
E7	Dienstomschrijving U dient een correcte beschrijving in te vullen van wie, wat, waar kan doen met deze dienst. Daarbij is 'wie' nooit 'u', maar een onderneming of organisatie, vaak in een bepaalde sector. Dienstomschrijving: <Wie kan waar wat doen?> Bijvoorbeeld: <i>Een onderneming kan aanvragen doen voor omgevingsvergunningen en watervergunningen. Daarnaast kunnen diverse meldingsformulieren worden ingediend. Ook kan een vergunningcheck worden gedaan om te zien of een vergunning of melding nodig is.</i> De dienstomschrijving mag niet bevatten: <ul style="list-style-type: none">• het benodigde betrouwbaarheidsniveau;• het websiteadres;• de naam van de dienstverlener	<input type="checkbox"/>	
E8	URL beschrijving webdienst U dient een webadres op te geven van de plaats waar de beschrijving van uw dienst op uw website staat of waar de dienst al publiek beschikbaar is.	<input type="checkbox"/>	

*De volledige richtlijnen kunt u vinden op de handleidingen- en ondersteuningspagina van eHerkenning: <https://www.eherkenning.nl/nl/voor-dienstverleners/aansluiten/handleidingen-en-ondersteuning>