Dienst ICT Uitvoering
Ministerie van Economische Zaken en Klimaat

Checklist Testen Routeringsvoorziening TVS

Versie: 2.1

Datum: 08-09-2025

Status: Definitief

Voor vragen kunt u mailen naar tvs@dictu.nl

Inhoud

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 tvs@dictu.nl.

2 Testcriteria voor aansluiten op TVS

2.1 Gegevens van uw aansluiting

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

TVSnummer:

……

URL acceptatie of preproductie-omgeving:

……

Zorg ervoor dat, wanneer u een gesloten omgeving heeft, de IP-adressen van DICTU zijn opgenomen op de whitelist. Deze kunt u opvragen via tvs@dictu.nl.

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	**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. *Opmerking: geldt niet voor een preproductie-aansluiting.*	❑	
C2	**Geen vermelding TVS** Nergens op de website of in de webapplicatie wordt er vermelding gemaakt van de ToegangVerleningService of TVS.	❑	
C3	**Gebruik app stores** De app met TVS-toegang mag alleen via de officiële appstores van Apple voor iOS en Google voor Android worden gedistribueerd.	❑	

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 op het hoofd- en eventuele subdomein mogen geen verwijzingen naar authenticatiediensten en TVS bevatten.	❑	
T2	**Toegankelijkheid inlogpagina** De inlogpagina van Afnemer met (de link naar) de authenticatiedienst heeft geen onderbrekingen zoals een pop-up, nieuw window of tabblad.	❑	
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. *Opmerking: bij gebruik van de TVS Smartloginpagina wordt de gebruiker bij annulering teruggeleid naar de pagina vanwaar de Smartloginpagina is aangeroepen. De StatusMessage bij gebruik van de Smartloginpagina is "Authentication cancelled"*	❑	
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).	❑	
T5	**De authenticatie slaagt** Het authenticatieproces verloopt conform de koppelvlakspecificaties. De gebruiker kan inloggen en de dienstaanbieder ontvangt na een succesvolle authenticatie een reactie van de authenticatiedienst.	❑	

T6	**Betrouwbaarheidsniveaus correct afgehandeld** De Afnemer bepaalt het minimale betrouwbaarheidsniveau. De burger mag altijd inloggen op een hoger niveau, maar niet lager dan het vereiste niveau. Bijvoorbeeld: • 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.	❑	
T7	**Uitlogmogelijkheid** 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.	❑	
T8	**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.	❑	
T9	**Automatisch uitloggen** 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.	❑	
T10	**Navigatiekliks** Het inlogportaal van de authenticatiedienst of de TVS Smartloginpagina moet met maximaal 2 navigatie kliks benaderbaar zijn. Voorbeeld: Homepage -> Patiëntenportaal -> Inlogpagina authenticatiedienst (of TVS Smartlogin)	❑	

T11	**Geen meerdere inlogknoppen** Bij gebruik van de TVS Smartloginfunctionaliteit mag er slechts één inlogknop aanwezig zijn die direct doorverwijst naar de TVS Smartloginpagina. Deze knop mag alleen het woord Inloggen bevatten. Andere inlogknoppen voor eigen inlogmiddelen zijn wel toegestaan. *Opmerking: Het is toegestaan om het DigiD-logo te tonen bij de inlogknop die verwijst naar de TVS Smartloginpagina, mits uitsluitend DigiD en DigiD Machtigen als identiteitsproviders (IdP's) actief zijn. Wanneer eHerkenning en/of eIDAS ook als IdP's beschikbaar zijn, mag het DigiD-logo niet worden weergegeven.*	❑	

2.4 DigiD

De volgende controles zijn alleen van toepassing op aansluitingen waarbij de authenticatiedienst DigiD is geactiveerd.

Nr.	Testcriterium	✓	Toelichting
L1	**Beveiligingsrichtlijnen** • 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. • U past de basisprincipes van digitale weerbaarheid toe.	❑	
L2	**Geen propagatie of afgeleide of verlengde toegang** 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: • 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.	❑	
L3	**Schrijfwijze** DigiD wordt aan elkaar geschreven met twee hoofdletters 'D'. Schrijf 'DigiD' in plaats van bijvoorbeeld 'de DigiD'.	❑	

L4	**Naam van de BSN- gerechtigde organisatie** 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. 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.	❑	
L5	**Geen deeplinks** Links naar authenticatiediensten voor 'meer informatie' verwijzen voor DigiD naar https://www.digid.nl/.	❑	
L6	**Geen uitleg en geen bereikbaarheidsgegevens** Afnemer geeft nergens uitleg (zoals veelgestelde vragen) over DigiD en/of de ToegangVerleningService (TVS). En nergens worden bereikbaarheidsgegevens (zoals het telefoonnummer of e-mailadres) van de authenticatiediensten- en/of DICTU-Servicedesk vermeld. Indien er iets over DigiD moet worden vermeld, wordt voor DigiD verwezen naar https://www.digid.nl/	❑	
L7	**Betrouwbare verbinding** De inlogpagina van Afnemer met (de link naar) DigiD staat op een .nl domein met DNSSEC en is beveiligd met een geldig TLS-certificaat. De URL van het hoofd- en eventuele subdomein mogen geen verwijzingen naar DigiD bevatten, zoals: digi-d, digi.d, d.igi.d, diegiedee.	❑	

L8	**Logo** Bij iedere doorverwijzing naar DigiD voor authenticatie toont u als dienstverlener het logo van DigiD en de tekst inloggen. Download dit logo in de Toolkit DigiD en DigiD Machtigen. Naast het logo geeft u een link die doorverwijst naar het inlogscherm van DigiD.  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. *Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het DigiD logo al op deze pagina aanwezig is.*	❑	
L9	**Logo App** 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.  Dit logo is te downloaden in de Toolkit DigiD en DigiD Machtigen. Minimale afmeting is 20x20 pixels, gangbaar is 100x100 pixels. *Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het DigiD logo al op deze pagina aanwezig is.*	❑	
L10	**Foutmelding DigiD** Indien DigiD een resultcode teruggeeft aan de webapplicatie (met uitzondering van SAML-statuscodes “Authnfailed”, "Authentication cancelled" (bij gebruik TVS Smartlogin) en “Succes”) bevat de pagina die wordt getoond de letterlijke foutmelding: *“Inloggen bij deze organisatie is niet gelukt. Probeert 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.”* De lokale sessie is hierna beëindigd, een gebruiker dient opnieuw in te loggen.	❑	

L11	**Redirect binnen domein** 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). Voorbeeld van stapsgewijze flow zoals toegestaan: • https://webpagina.nl/inloggenvoordigid • https://www.digid.nl/inloggen • https://webpagina.nl/ingelogd Voorbeeld van stapsgewijze flow zoals ook toegestaan: • https://webpagina.nl/inloggenvoordigid of https://inloggen.webpagina.nl/ • https://www.digid.nl/inloggen • https://ingelogd.webpagina.nl/ Niet toegestaan is: • https://webpagina.nl/inloggenvoordigid • https://anderepagina.nl • https://www.digid.nl/inloggen • https://webpgina.nl/ingelogd	❑	

2.5 DigiD Machtigen

De volgende controles zijn alleen van toepassing op aansluitingen waarbij de authenticatiedienst DigiD Machtigen is geactiveerd.

Nr.	Testcriterium	✓	Toelichting
M1	**Schrijfwijze** Schrijf DigiD en Machtigen na elkaar met een spatie ertussen: 'DigiD Machtigen'	❑	
M2	**Geen deeplinks** Links naar authenticatiediensten voor 'meer informatie' verwijzen voor Machtigen naar https://machtigen.digid.nl/	❑	
M3	**Geen uitleg en geen bereikbaarheidsgegevens** Afnemer geeft nergens uitleg (zoals veelgestelde vragen) over Machtigen. En nergens worden bereikbaarheidsgegevens (zoals het telefoonnummer of e-mailadres) van de authenticatiediensten- en/of DICTU-Servicedesk vermeld. Indien er iets over Machtigen moet worden vermeld, wordt voor DigiD verwezen naar Machtigen naar https://machtigen.digid.nl/	❑	
M4	**Logo DigiD Machtigen** Er bestaat geen logo voor Machtigen. Nergens gebruikt Afnemer een zelfgemaakt logo voor Machtigen.	❑	
M5	**De authenticatie slaagt** Het authenticatieproces verloopt conform de koppelvlakspecificaties. De gebruiker kan inloggen en de dienstaanbieder ontvangt na een succesvolle authenticatie een reactie van de authenticatiedienst.	❑	

2.5 eHerkenning

De volgende controles* zijn uitsluitend van toepassing op aansluitingen waarbij de authenticatiedienst eHerkenning geactiveerd is.

Nr.	Testcriterium	✓	Toelichting
E1	**Beveiligingsrichtlijnen** • Op de webapplicatie moeten de ICT beveiligingsrichtlijnen van de NCSC worden toegepast. • Op de app moeten de ICT-beveiligingsrichtlijnen van de NCSC worden toegepast. U past de basismaatregelen cybersecurity van de NCSC toe.	❑	
E2	**Logo eHerkenning** eHerkenning Dit logo moet in de volgende situaties worden geplaatst: • 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 Dit beeldmerk moet worden toegepast bij iconisch gebruik en geringe ruimte. Bij voorkeur het hele woordmerk plaatsen in verband met de herkenbaarheid. *Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het logo al op deze pagina aanwezig is.*	❑	
E3	**Betrouwbaarheidsniveau** U geeft aan met welk betrouwbaarheidsniveau uw klanten moeten inloggen. Hiervoor gebruikt u de vignetten betrouwbaarheidsniveaus. *Opmerking: bij gebruik van de TVS Smartloginpagina vervalt deze vereiste*	❑	

E4	**Kernboodschap** De volgende kernboodschap staat op uw website: *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.*	❑	

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 inlogscherm van eHerkenning: U wilt inloggen bij <Dienstverlenernaam> Bijvoorbeeld: • U wilt inloggen bij **Kamer van Koophandel**	❑	
E6	**Naam webdienst** Bij het invullen van de dienstnaam moet deze duidelijk en begrijpelijk zijn voor de gebruiker en overeenkomen met de webdienstnaam op uw website. De naam moet een werkwoord bevatten en beschrijven wat de gebruiker kan doen, bijvoorbeeld "parkeervergunning aanvragen". Het gebruik van "inloggen" in de dienstnaam is niet toegestaan. Voor portalen moet de naam aangeven dat het om meerdere diensten gaat. Daarnaast mag de dienstnaam geen betrouwbaarheidsniveau, websiteadres of dienstverlenernaam bevatten, aangezien deze apart worden geregistreerd.	❑	
E7	**Dienstomschrijving** Bij het invullen van de dienstomschrijving moet duidelijk worden wie, waar en wat met de dienst kan worden gedaan. Hierbij is 'wie' meestal een organisatie of onderneming, en niet 'u'. De omschrijving moet aansluiten bij de beschrijving op uw website en helder maken waarvoor gebruikers worden gemachtigd. Voor portalen met meerdere diensten moeten alle diensten duidelijk worden omschreven. De omschrijving mag geen betrouwbaarheidsniveau, websiteadres of de naam van de dienstverlener bevatten, omdat deze apart worden geregistreerd.	❑	
E8	**URL beschrijving webdienst** Het websiteadres moet verwijzen naar de beschrijving van uw dienst of naar de dienst zelf. Voor portalen moet de URL leiden naar een overzicht van de diensten. De link moet actueel blijven en goed vindbaar zijn voor gebruikers.	❑	

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

2.5 eIDAS

De volgende controles zijn uitsluitend van toepassing op aansluitingen waarbij de authenticatiedienst eIDAS geactiveerd is.

Nr.	Testcriterium	✓	Toelichting
EU1	**Beveiligingsrichtlijnen** • Op de webapplicatie moeten de ICT beveiligingsrichtlijnen van de NCSC worden toegepast. • Op de app moeten de ICT-beveiligingsrichtlijnen van de NCSC worden toegepast. U past de basismaatregelen cybersecurity van de NCSC toe.	❑	
EU2	**Logo eIDAS** Bij iedere doorverwijzing naar eIDAS voor authenticatie toont u als dienstverlener het logo van eIDAS en de tekst inloggen.  Meer informatie kun je vinden op Richtlijnen gebruik logo European login. *Bij het gebruik van TVS Smartloginpagina vervalt deze vereiste aangezien het logo al op deze pagina aanwezig is.*	❑	

Richtlijnen voor de dienstencatalogus In de volgende stappen staan de verplichtingen en adviezen omtrent het invullen van de benodigde velden voor de dienstencatalogus			
EU3	**Naam dienstverlener** U dient een correcte en voor uw gebruikers begrijpelijke naam van uw organisatie in te vullen. Indien er sprake is van BSN-verwerking door de dienstaanbieder: bij de inlogmogelijkheid met eIDAS wordt de naam van de (BSN-gerechtigde) afnemer getoond 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.	❑	
EU4	**Naam webdienst** Bij het invullen van de dienstnaam moet deze duidelijk en begrijpelijk zijn voor de gebruiker en overeenkomen met de webdienstnaam op uw website.	❑	
EU5	**Dienstomschrijving** Bij het invullen van de dienstomschrijving moet duidelijk worden wie, waar en wat met de dienst kan worden gedaan.	❑	
EU6	**URL beschrijving webdienst** Het websiteadres moet verwijzen naar de beschrijving van uw dienst of naar de dienst zelf. Voor portalen moet de URL leiden naar een overzicht van de diensten. De link moet actueel blijven en goed vindbaar zijn voor gebruikers.	❑	