



Handleiding aansluiten op TVS

voor Leveranciers Clusteraansluitingen (LC)

Versie: 1.1

Datum: 11-10-2023

Status: Definitief

Inhoud

Handleiding aansluiten op TVS.....	1
1. Inleiding	4
Vragen of suggesties?.....	4
1.1 Wie mogen aansluiten op TVS?.....	5
1.2 Wat is een Leverancier Clusteraansluiting?	5
1.3 Beschikbare authenticatiediensten (IdP's) voor een Clusteraansluiting.....	6
1.3.1 Betrouwbaarheidsniveaus.....	7
2. Voorbereiding.....	7
2.1 Rol- en taakverdeling voor het aansluitproces.....	7
2.2 Start samenwerking.....	8
2.3 Samenwerking met dienstverleners.....	8
2.4 Check randvoorwaarden	8
2.4.1 BSN-gerechtigdheid	9
2.4.2 Controle inschrijving KvK.....	9
2.5 Voorbereiden Assessment.....	9
2.5.1 Meervoudig assessment.....	9
2.5.2 Enkelvoudig assessment.....	9
2.6 SAML Kennis	10
2.7 PKI-overheid-certificaten aanvragen	10
2.8 Akkoordverklaringen dienstverleners	11
3. Aansluiten op de TVS preproductie-omgeving.....	12
3.1 Aanvragen aansluiting	12
3.2 Aanleveren ontbrekende gegevens.....	12
3.3 Aansluitbestand.....	12
3.4 SAML Metadata	13
3.5 Activeren preproductie-aansluiting binnen de keten	13
3.6 Afronden Preproductie-aanvraag.....	14
4. Testen aansluiting op de preproductie-omgeving	15
4.1 Zelf testen van de aansluiting op de preproductie-omgeving	15
4.2 Aansluiting aanbieden aan TVS	15
4.3 Acceptatie door TVS	15
5. Aansluiten op de productieomgeving	16
5.1 Aanvragen aansluiting	16
5.2 Aanleveren ontbrekende gegevens.....	16
5.3 Aansluitbestand.....	16

5.4 SAML Metadata.....	17
5.5 Activeren productieaansluiting binnen de keten	17
5.6 Inbeheername van de aansluiting	17
5.7 Blijf geïnformeerd.....	18

1. Inleiding

In deze handleiding vindt u alle stappen die u als Leverancier Clusteraansluiting (LC) moet uitvoeren om met succes op TVS aan te sluiten. Deze handleiding is bedoeld voor leveranciers clusteraansluitingen die willen aansluiten op TVS en leveranciers die in opdracht van deze leveranciers clusteraansluitingen ontwikkelen.

Organisaties en dienstverleners die een directe aansluiting op TVS willen realiseren kunnen de handleiding voor Directe aansluitingen volgen.

Vragen of suggesties?

Wij helpen u bij het aansluiten op TVS. Heeft u vragen over het aansluitproces? Neem dan contact op via tv�@dictu.nl. Wij helpen u graag verder.

Kleinere wijzigingen aan dit document communiceren wij niet breed, dus kijk zelf met enige regelmaat of er een nieuwere versie van dit document online staat.

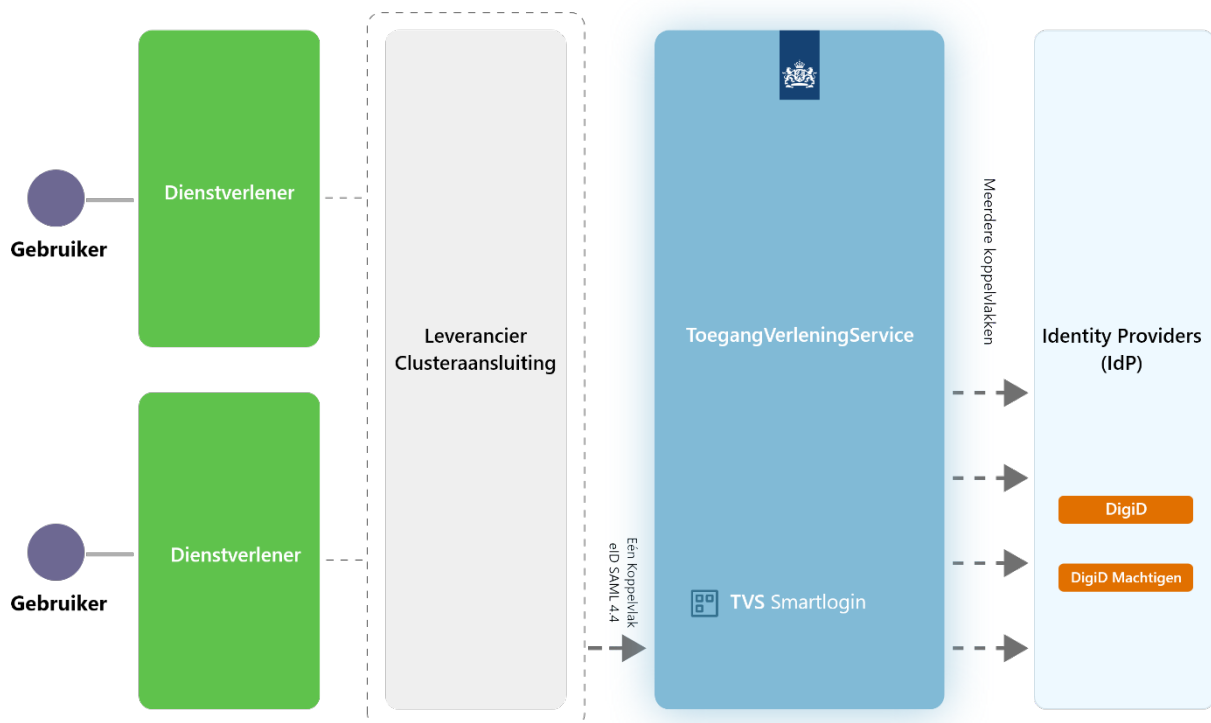
1.1 Wie mogen aansluiten op TVS?

TVS is beschikbaar voor de volgende organisaties:

- ICT Leveranciers voor een TVS Clusteraansluiting
- Overheidsinstellingen
- Zorgverleners

1.2 Wat is een Leverancier Clusteraansluiting?

Een aansluiting waarbij de ICT-leverancier optreedt als een tussenpartij met een SaaS-dienst is een zogenaamde Clusteraansluiting. De ICT-leverancier treedt op als tussenpartij tussen TVS en dienstverleners. Dienstverleners zijn bijvoorbeeld zorgverleners zoals huisartsen en ziekenhuizen en publieke uitvoeringsinstanties t.g.v. diensten aan burgers en bedrijven. Dienstverleners melden zich aan bij hun ICT-leverancier om aangesloten te worden op TVS. Een clusteraansluiting op TVS ziet er als volgt uit:



Onderdeel	Uitleg
Gebruiker	Dit is de eindgebruiker (een burger) die gebruik maakt van de diensten van de dienstverleners.
Dienstverleners	Dienstverleners zijn overheidsinstellingen en zorgverleners die zijn aangesloten op TVS.
Leverancier Clusteraansluiting	ICT-leverancier van een zogenaamde Clusteraansluiting. Wordt gebruikt om meerdere dienstverleners over één aansluiting te ontsluiten.
Koppelvlak SAML	Dit is het koppelvlak waarmee een portaal wordt aangesloten op TVS. U sluit aan via één Koppelvlak voor alle authenticatiediensten.
Identity Providers	Een identity provider (IdP) of een authenticatiedienst is een service die digitale identiteiten opslaat en beheert. TVS biedt bij een clusteraansluiting enkel ondersteuning voor DigiD en DigiD Machtigen.
Smartlogin	De TVS smartloginpagina is een routeringspagina voor dienstverleners die gebruik maken van meerdere authenticatiediensten. Vanaf deze pagina kan de gebruiker een keuze maken voor een authenticatiedienst.

Een clusteraansluiting heeft onder andere de volgende eigenschappen:

- 1 technische aansluiting met TVS
- Het is een SAAS-dienst van een ICT-leverancier
- Kan gebruikt worden door meerdere dienstverleners
- ICT-leverancier vraagt de aansluiting aan
- Dienstverlener geeft akkoord voor de aansluiting
- ICT-leverancier ontwikkelt de aansluiting en is verantwoordelijk voor het aansluitproces
- ICT-leverancier is verantwoordelijk voor het assessment proces

1.3 Beschikbare authenticatiediensten (IdP's) voor een Clusteraansluiting

Wanneer u aansluit middels een clusteraansluiting op TVS dan zijn de volgende authenticatiediensten beschikbaar:

- DigiD
- DigiD Machtigen

eHerkenning en eIDAS zijn niet beschikbaar op een clusteraansluiting vanwege beperkingen vanuit het eTD-stelsel. Indien een dienstverlener hier gebruik van wil maken, dan is een **directe** aansluiting met TVS vereist. Naar verwachting is ultimo 2023 eIDAS wél beschikbaar binnen een clusteraansluiting.

1.3.1 Betrouwbaarheidsniveaus

De volgende betrouwbaarheidsniveaus zijn beschikbaar op TVS:

- Midden
- Substantieel
- Hoog

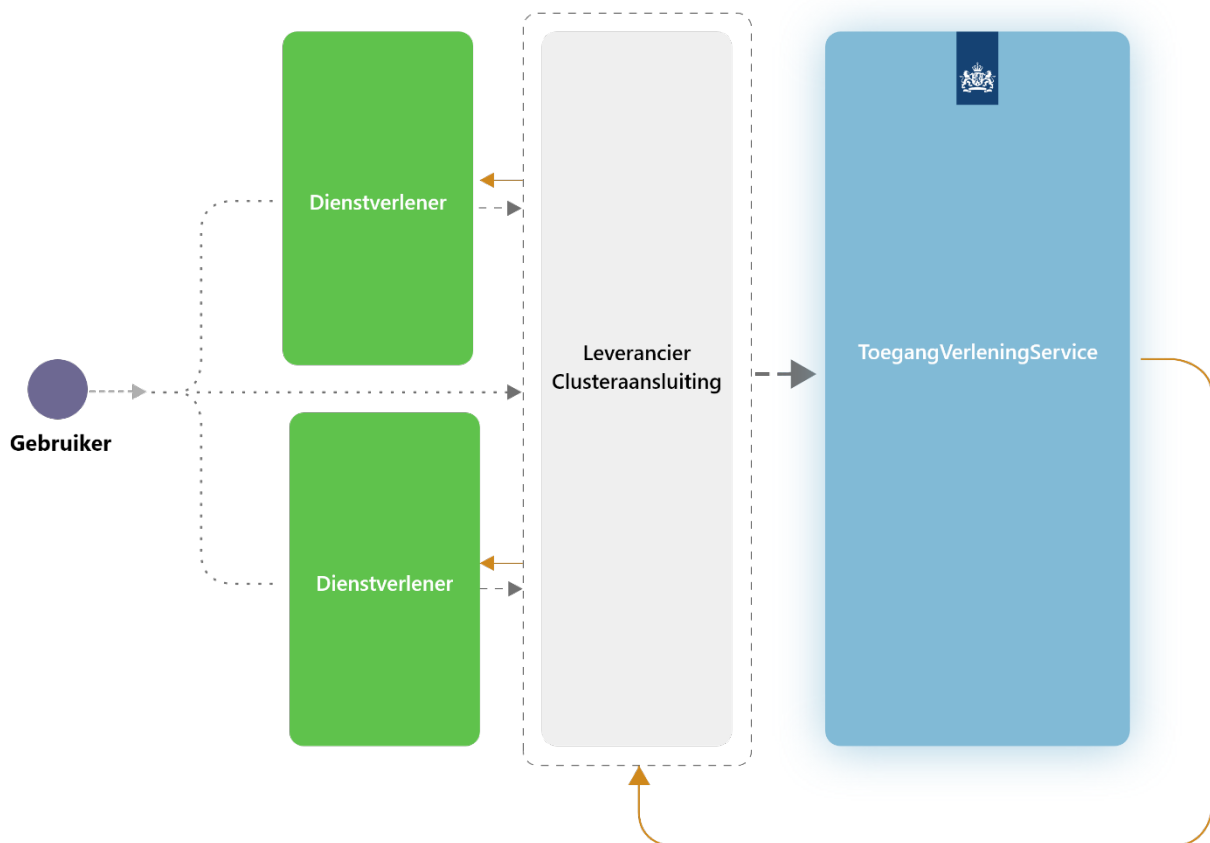
Voor het bepalen van het juiste betrouwbaarheidsniveau kunt u gebruik maken van de Regelhulp betrouwbaarheidsniveaus <https://regelhulpenvoorbedrijven.nl/betrouwbaarheidsniveaus/>

2. Voorbereiding

2.1 Rol- en taakverdeling voor het aansluitproces

Om als Leverancier Clusteraansluiting aangesloten te worden op TVS moeten er een aantal stappen succesvol worden doorlopen.

Het moet duidelijk zijn wie waar verantwoordelijk voor is. De ICT-leverancier wordt aangesloten op TVS, dus zal communicatie met TVS altijd via de ICT-leverancier verlopen. De ICT-leverancier is het ingang- en aanspreekpunt voor de dienstverleners. De communicatieflow bij een clusteraansluiting ziet er als volgt uit:



In onderstaand schema vindt u een rolverdeling met bijbehorende taken en verantwoordelijkheden, die nodig zijn om het aansluitproces zo effectief en efficiënt mogelijk te laten verlopen.

Rolverdeling ICT-leverancier	Taken en verantwoordelijkheden
Tekenbevoegde	Heeft tekenbevoegdheid voor het aanvragen van een cluster aansluiting op TVS
Projectleider	Begeleidt het gehele aansluitproces op TVS.
Technisch specialist	Heeft technische kennis van de omgeving waarop TVS wordt ingevoerd en heeft voldoende kennis van de specifieke systemen en de Koppelvlak specificatie eID SAML 4.4 om de aansluiting te realiseren.

2.2 Start samenwerking

Voordat u het aansluitproces start is het verstandig kennis te nemen van de informatie die hierover beschikbaar is. Het doornemen van het document Functionele beschrijving TVS (<https://dictu.nl/toegangverleningservice/documentatie-en-links/functionele-beschrijving-tvs>) samen met deze handleiding is een goed startpunt. Zo heeft u een beter beeld van wat TVS is en kunt u tijdig de juiste voorbereidingen treffen. Dat bevordert een vlot verloop van het aansluitproces.

2.3 Samenwerking met dienstverleners

Om een cluster aansluiting te kunnen realiseren op de productie-omgeving heeft u twee dienstverleners nodig die de aansluiting willen activeren. Een dienstverlener kan bijvoorbeeld een zorgaanbieder zijn. Als ICT-leverancier dient u dus binnen uw cliëntèle na te gaan welke dienstverleners hierin gezamenlijk met u willen optrekken.

2.4 Check randvoorwaarden

Aan het gebruik van TVS zijn een aantal eisen verbonden. Dat betekent dat u een aantal voorbereidingen moet treffen om aan te tonen dat u aan de gestelde eisen voldoet.

Onderdeel	Preproductie	Productie
BSN-gerechtigdheid	Niet verplicht	Verplicht voor de dienstverlener
Controle inschrijving KvK	Verplicht	Verplicht

2.4.1 BSN-gerechtigdheid

Het gebruik van DigiD als inlogmiddel is alleen toegestaan als de betreffende organisatie (dienstverlener) het BSN van burgers mag verwerken. BSN-gerechtigd noemen we dat.

De controle hierop vindt plaats aan de hand van een centraal register, de ALB-lijst. Controleer of uw aan te sluiten dienstverleners daarin zijn geregistreerd, zie https://stb.bsn-koppelregister.nl/alb/autorisatielijst_bsn.xml.html. Staan de aan te sluiten dienstverleners nog niet op de ALB-lijst? Dan kunnen ze zich kosteloos registreren in het UZI-register. Organisaties worden dan automatisch ook opgenomen op de ALB-lijst.

Deze vereiste geldt niet voor de ICT-leverancier aangezien een ICT-leverancier niet met BSN's zal werken.

2.4.2 Controle inschrijving KvK

De tenaamstelling van de aanvraag moet overeenkomen met de wijze waarop uw organisatie is geregistreerd bij de KvK. Controleer daarom of uw KVK-registratie nog actueel is (organisatienaam, adres, gemandateerden om te ondertekenen).

2.5 Voorbereiden Assessment

Alle organisaties die DigiD gebruiken moeten voldoen aan de beveiligingsnormen van het NCSC. Deze normen hebben betrekking op de organisatie en de techniek en wordt via een DigiD-beveiligingsassessment getoetst door een erkend EDP-auditor (RE). Dit assessment moet plaatsvinden binnen twee maanden nadat de aansluiting is geactiveerd op de productieomgeving van TVS. Vervolgens moet het assessment jaarlijks worden herhaald in de periode januari-mei.

Bij het treffen van de voorbereidingen van het assessment kunt u onder andere denken aan het indienen van de zelfverklaring, het benaderen van een RE-auditor, afstemmen van de scope van het assessment, het plannen en uitvoeren van een pre-audit*, het plannen en uitvoeren van een penetratietest en contractformalisatie.

* Niet verplicht, maar wordt wel geadviseerd.

2.5.1 Meervoudig assessment

Bij een cluster aansluiting kan – onder voorwaarden – worden volstaan met een meervoudig assessment (één assessment voor alle op de betreffende aansluiting aangesloten dienstverleners). In een overeenkomst tussen u en Logius komt u overeen aan deze voorwaarden te voldoen. Dat noemen we zelfverklaring of accreditatie. We raden aan goed kennis te nemen van deze voorwaarden en -waar nodig in overleg met de aan te sluiten dienstverleners - tot een besluit komen over de toepasbaarheid van een meervoudig assessment.

Meer informatie over het meervoudig assessment: <https://www.logius.nl/diensten/digid/ict-beveiligingsassessments-digid/het-meervoudig-assessment>

2.5.2 Enkelvoudig assessment

Indien u geen overeenkomst aangaat met Logius voor een meervoudig assessment, dan wordt de aansluiting gezien als een enkelvoudig assessment cluster aansluiting. Wanneer u voor deze optie gaat moeten alle dienstverleners die aangesloten worden op de cluster aansluiting afzonderlijk ge-audit worden.

2.6 SAML Kennis

TVS biedt enkel ondersteuning voor het Koppelvlak eID SAML 4.4

(<https://dictu.nl/toegangverleningservice/documentatie-en-links/koppelvlak-specificatie-eid-saml-44>). Dit koppelvlak is gebaseerd op de internationale SAML2.0 standaard.

2.7 PKI-overheid-certificaten aanvragen

Een digitaal certificaat is een computerbestand dat fungeert als een digitaal paspoort. Het bevat gegevens die nodig zijn voor beveiligd internetverkeer. Digitale certificaten zijn een onmisbare schakel in veilig internetverkeer. Als ICT-leverancier heeft u één of meerdere certificaten nodig. Ook de aangesloten dienstverleners moeten in het bezit zijn van een geldig certificaat:

2.7.1 Dienstverlener

Een dienstverlener heeft een certificaat nodig voor de versleuteling van het BSN.

2.7.2 ICT-leverancier

Een ICT-leverancier heeft een certificaat voor de Mutual TLS authentication, een certificaat voor de Signing van berichten en een certificaat voor de Web-authenticatie van de webdienst nodig.

1. Een PKI-o-certificaat voor de TLS en de signing van SAML berichten moeten specifiek voor de aansluiting op TVS worden aangeschaft. U mag geen gebruik maken van bestaande certificaten. U kunt voor de aanschaf hiervan terecht bij een Trust Service Provider. U kunt ervoor kiezen om één certificaat te gebruiken voor mutual TLS en Signing, maar vanuit veiligheidsoptiek luidt het advies om te kiezen voor twee aparte certificaten.
2. Een certificaat voor de authenticatie van web-diensten. Kies hierbij voor een Domain Validation-certificaat. Hergebruik van een bestaand certificaat is niet toegestaan. Voor de aanschaf van dit certificaat kunt u terecht bij een Trust Service Provider.

Toegestane certificaten

mTLS	PKI-overheid G1 Private Root
Signing	PKI-overheid G1 Private Root
Webdienst	Domain Validation-certificaat, zie ook het factsheet van NCSC https://www.ncsc.nl/documenten/factsheets/2021/september/29/factsheet-pki-overheid-stopt-met-webcertificaten
Encryptie (voor dienstverleners)	PKI-overheid G1 Private Root of UZI-certificaat via het CIBG

G1 Private root certificaten mogen maximaal 3 jaar geldig zijn.

Let op! Voor de ICT-leverancier en dienstverlener geldt dat u één set van deze certificaat(en) nodig heeft voor pre-productie en één set voor de productieomgeving. Aan certificaten is een geldigheidsduur gekoppeld. Stem de aanschaf dus af op de planning.

Let op! PKI-overheid-certificaten kunt u het beste zo vroeg mogelijk aanvragen. Het kan namelijk een aantal weken duren voor uw registratie als nieuwe abonnee rond is. De uitgifte van de certificaten verloopt overigens sneller als uw organisatie al abonnee is van een PKI-overheid-certificaatverstrekker.

2.8 Akkoordverklaringen dienstverleners

Elke dienstverlener die op de productie-omgeving wordt aangesloten dient akkoord te gaan met de algemene voorwaarden van TVS.

Als u een zelfverklaring heeft ingediend bij Logius bent u gerechtigd om de meeste zaken in het kader van de cluster aansluiting te regelen namens de aan te sluiten dienstverleners. Formeel blijven dienstverleners echter altijd verantwoordelijk van de aansluiting op DigiD. U dient hiervoor twee zaken te regelen:

- De dienstverlener dient akkoord te gaan met de voorwaarden voor het juiste gebruik van DigiD en zich te committeren deze te zullen naleven.
- De dienstverlener dient akkoord te gaan met de voorwaarden die DICTU stelt aan het gebruik van TVS. Dat kan via een akkoordverklaring. De leverancier ziet erop toe dat alle aan te sluiten dienstverleners de akkoordverklaring ondertekenen.

De akkoordverklaringen moeten bij het indienen van het aansluitbestand en de metadata mee worden gezonden aan DICTU. Zonder akkoordverklaring kan een dienstverlener niet worden aangesloten op de productieomgeving. U kunt de documenten vinden op onze documentatiepagina <https://dictu.nl/toegangverleningservice/documentatie-en-links>.

3. Aansluiten op de TVS preproductie-omgeving

In deze stap wordt er een preproductie-aansluiting gerealiseerd op TVS.

Op te leveren documenten

- SAML metadata
- Aansluitbestand
- Ondertekend aanvraagformulier
- Checklist testen TVS

3.1 Aanvragen aansluiting

Een aanvraag op TVS kan ingediend worden via het online aanmeldformulier op de TVS website.

Online aanmeldformulier <https://dictu.nl/toegangverleningservice/aanvragen>

Na het versturen van het formulier krijgt u een bevestiging van uw aanvraag. Meestal gebeurt dit binnen één werkdag.

3.2 Aanleveren ontbrekende gegevens

Om de aansluiting op TVS te kunnen realiseren heeft het TVS aansluitteam een aantal gegevens nodig. U ontvangt een email waarin om deze gegevens gevraagd wordt. Het gaat om de volgende gegevens:

- U ontvangt een kopie van uw aanvraag in PDF formaat. U wordt verzocht om dit te laten ondertekenen door een tekenbevoegde van uw organisatie
- Een aansluitbestand met de gegevens van de aan te sluiten dienstverleners
- De XML-metadata van uw aansluiting (indien niet aangeleverd bij de aanvraag)

3.3 Aansluitbestand

Een van de voordelen van een cluster aansluiting is dat de leverancier van een cluster aansluiting eenvoudig meerdere dienstverleners kan aansluiten. Om de gegevens van deze dienstverleners te kunnen verwerken werkt TVS met een zogenaamd aansluitbestand.

Zie handleiding aansluitbestand voor leveranciers cluster aansluitingen voor meer informatie:
<https://dictu.nl/toegangverleningservice/documentatie-en-links/handleiding-aansluitbestand>

Let op! Op de preproductie-omgeving moeten er minimaal twee dienstverleners aangemeld worden op de cluster aansluiting. Eén van deze dienstverleners hoort een echte dienstverlener te zijn. Voor de tweede dienstverlener mag de ICT-leverancier zichzelf als een test dienstverlener opgeven, maar dit mag uiteraard ook een echte dienstverlener zijn.

Info: Het wordt geadviseerd om op de preproductie-omgeving beide type certificaten te testen, zowel het G1 Private Root als het UZI-certificaat. Dit is echter niet verplicht.

3.4 SAML Metadata

De metadata voor uw aansluiting dient te voldoen aan de Koppelvlak specificatie eID SAML 4.4, zie <https://dictu.nl/toegangverleningservice/documentatie-en-links/koppelvlak-specificatie-eid-saml-44>.

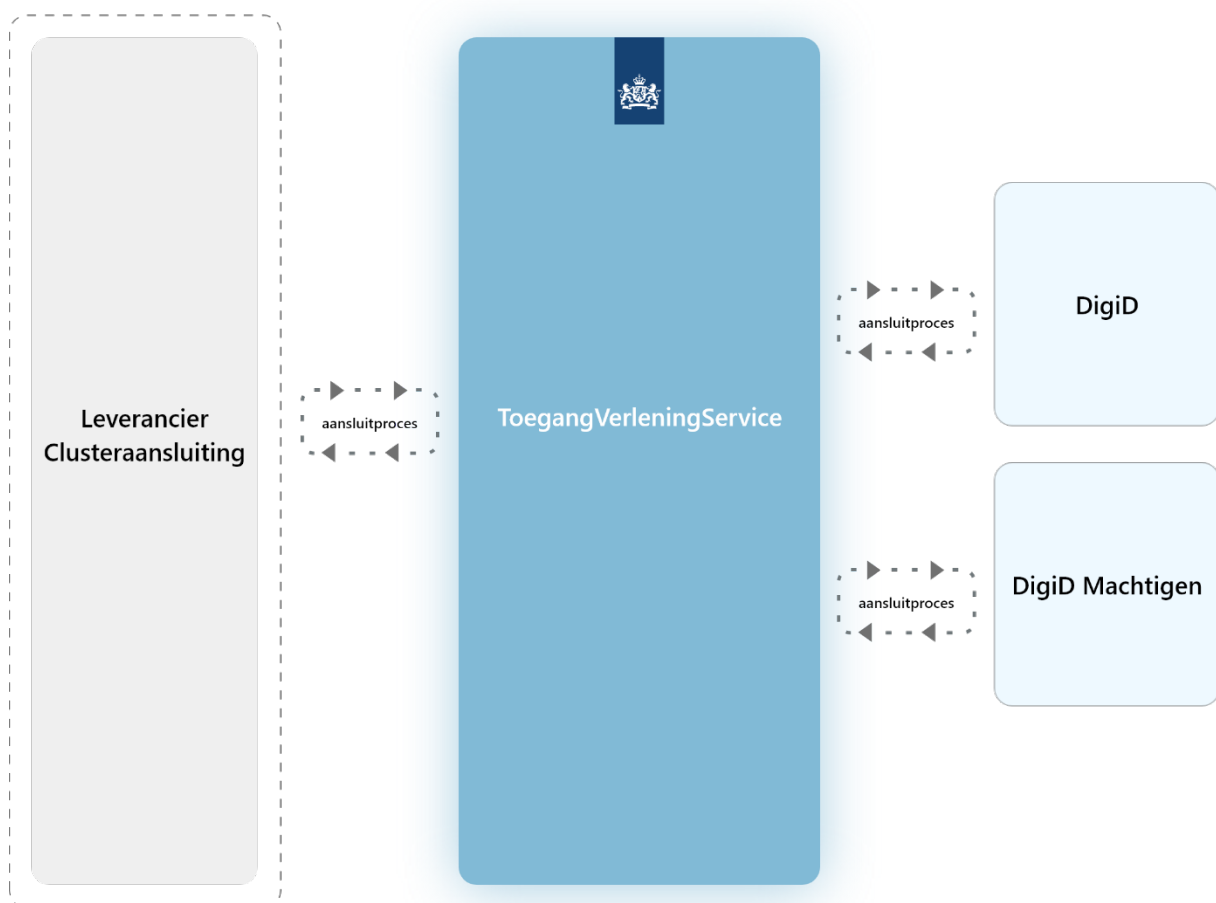
Lees de documentatie goed door. Zonder goedgekeurde metadata kan uw aansluiting niet geactiveerd worden. Het verwerken van de metadata gebeurt via de TVS beheermodule. U kunt de metadata als bijlage mailen naar tvsv@dictu.nl of op een beveiligde URL beschikbaar stellen.

Let op! Het metadata-bestand moet naast de verplichte attributen en waarden ook valideren tegen XSD. U kunt dit controleren met een online tool zoals https://www.samltool.com/validate_xml.php maar ook bijvoorbeeld met Notepad ++.

Uw metadata dient ook ondertekend te zijn met een digitale handtekening. Belangrijk hierbij is dat het hiervoor te gebruiken certificaat een PKIOverheid certificaat dient te zijn dat is voorzien van uw OIN.

3.5 Activeren preproductie-aansluiting binnen de keten

Wanneer alle benodigde documenten en gegevens door TVS zijn ontvangen zal de aansluiting geactiveerd worden bij de aangevraagde authenticatiedienst(en). Voor een clusterleveraansluiting kunnen dit DigiD en DigiD Machtigen zijn. TVS houdt hiervoor een doorlooptijd van 5 werkdagen aan. De flow ziet er als volgt uit:



3.6 Afronden Preproductie-aanvraag

Als laatste stap, na de activatie van de aansluiting binnen de keten, ontvangt u een mail met het aansluitbestand waarin de dienstnummers(UUID) voor de aangemelde dienstverleners zijn opgenomen. Tevens staan in deze mail alle TVS endpoints en krijgt u vijf DigiD testaccounts ter beschikking.

4. Testen aansluiting op de preproductie-omgeving

Nadat de aansluiting is geactiveerd kunt u de koppeling tussen de preproductie-omgeving van uw systeem en de preproductie-omgeving van TVS testen.

Info: Het is mogelijk om vanuit meerdere OTA omgevingen van uw systeem te testen met de preproductie-omgeving van TVS. Hiervoor kunt u endpoints in uw metadata opgeven. Zie de koppelvlakspecificaties voor meer informatie.

Op te leveren documenten

- TVS Checklist Testen

4.1 Zelf testen van de aansluiting op de preproductie-omgeving

Het gerealiseerde koppelvlak wordt getest aan de hand van de Checklist testen. De resultaten hiervan moeten worden ingediend bij het TVS aansluitteam. Zorg ervoor dat alle testen positief zijn afgerond alvorens de checklist ter beoordeling aan te bieden aan het TVS aansluitteam.

Het TVS aansluitteam zal de checklist testen ook doorlopen. Hiervoor hebben wij de inloggegevens van de testomgeving nodig. Lever die aan samen met de checklist testen. Eventuele tekortkomingen koppelen wij aan u terug, waarna u in de gelegenheid bent aanpassingen te doen. De Checklist testen moet dan opnieuw worden ingediend en akkoord bevonden.

Let op! Voor elke authenticatiedienst dient u de checklist testen opnieuw in te vullen op de preproductie-omgeving. Heeft u bij de initiële aansluit-aanvraag beide authenticatiediensten geactiveerd? Dan hoeft u de checklist testen later niet opnieuw in te vullen.

4.2 Aansluiting aanbieden aan TVS

Heeft u uw checklist testen afgerond? Stuur dan een e-mail naar tvsvs@dictu.nl. Zet hierin de volgende gegevens:

- De te testen preproductie-omgeving URL. Deze omgeving dient door DICTU benaderbaar te zijn.
- Inloggegevens van de testomgeving
- Het TVS-nummer van de aansluiting

4.3 Acceptatie door TVS

Nadat TVS de ingevulde checklist testen heeft ontvangen zal een medewerker deze controleren. TVS stuurt u binnen 5 werkdagen per e-mail de uitslag van de checklist testen. Als hierin nog punten staan die niet voldoen aan de criteria van de TVS Checklist Testen, dan dient u deze punten aan te passen. Daarna kunt u de test opnieuw ter beoordeling aanbieden bij TVS.

5. Aansluiten op de productieomgeving

Aansluiten op de productieomgeving van TVS is grotendeels gelijk aan het aansluitproces op de preproductie-omgeving.

5.1 Aanvragen aansluiting

Om in aanmerking te komen voor een productie aansluiting, dient er eerst succesvol aangesloten te worden op de preproductie omgeving. Een aanvraag op de productie-omgeving moet ook via het online aanvraagformulier worden ingediend. Houd de volgende gegevens bij de hand bij het indienen van de aanvraag:

- Het OIN van uw organisatie
- Logius accreditatienummer (bij een meervoudig assessment)
- Contactgegevens

Na het versturen van het formulier krijgt u een bevestiging van uw aanvraag. Meestal gebeurt dit binnen één werkdag.

5.2 Aanleveren ontbrekende gegevens

Om de aansluiting op TVS te kunnen realiseren heeft het TVS aansluitteam een aantal gegevens nodig. U ontvangt een email waarin om deze gegevens gevraagd zal worden. Het gaat om de volgende gegevens:

- U ontvangt een kopie van uw aanvraag in PDF formaat. U wordt verzocht om dit te laten ondertekenen door een tekenbevoegde van uw organisatie
- Een aansluitbestand met de gegevens van de twee dienstverleners die u wilt aansluiten
- Getekende akkoordverklaringen van de aan te sluiten dienstverleners
- De XML-metadata van uw aansluiting (indien niet aangeleverd bij de aanvraag)

5.3 Aansluitbestand

In het aansluitbestand geeft u de gegevens op van de aan te sluiten dienstverleners. Een niet volledig ingevuld aansluitbestand wordt niet geaccepteerd. De gegevens van de dienstverleners zullen worden doorgestuurd naar Logius.

Zie handleiding aansluitbestand voor leveranciers clusteransluitingen voor meer informatie:
<https://dictu.nl/toegangverleningservice/documentatie-en-links/handleiding-aansluitbestand>

Let op! Op de productie-aanvraag moet u de eerste keer **exact twee** dienstverleners aansluiten. Nadat u de rapportage van het ICT-beveiligingsassessment met DigiD heeft gedeeld, kunt u de aansluiting uitbreiden met extra dienstverleners.

5.4 SAML Metadata

Ook voor de productie-omgeving hoort u SAML metadata aan te leveren dat voldoet aan de Koppelvlak specificatie eID SAML 4.4, zie <https://dictu.nl/toegangverleningservice/documentatie-en-links/koppelvlak-specificatie-eid-saml-44>. Lees de documentatie goed door. Zonder de goedgekeurde metadata kan uw aansluiting niet geactiveerd worden. U mag de metadata als bijlage mailen naar TVS of op een beveiligde URL beschikbaar stellen.

Let op! Het metadata-bestand moet naast de verplichte attributen en waarden ook valideren tegen XSD. U kunt dit controleren met een online tool zoals https://www.samltool.com/validate_xml.php maar ook bijvoorbeeld met Notepad ++. De metadata van de aansluiting moet ook digitaal ondertekend zijn een PKI-overheid certificaat.

Uw metadata dient ook ondertekend te zijn met een digitale handtekening. Belangrijk hierbij is dat het hiervoor te gebruiken certificaat een PKI-overheid certificaat dient te zijn dat is voorzien van uw OIN.

5.5 Activeren productieaansluiting binnen de keten

Wanneer alle benodigde documenten en gegevens door TVS zijn ontvangen zal de aansluiting geactiveerd worden bij de aangevraagde authenticatiedienst(en). Voor een clusterleveraansluiting kunnen dit DigiD en DigiD Machtigen zijn. We houden een doorlooptijd van 5 werkdagen hiervoor aan.

Let op! Zodra Logius de aansluiting activeert, start de termijn van 2 maanden waarbinnen u het meervoudig assessment moet laten uitvoeren en het rapport aan Logius moet opleveren.

Belangrijk! Het jaarlijks assessment moet op tijd zijn uitgevoerd! Maak hierover afspraken met de auditor. Bij het ontbreken van een goedgekeurd assessment rapport kan de aansluiting door Logius worden stopgezet.

5.6 Inbeheername van de aansluiting

Zorg voor een goed afgestemd plan voor inbeheername. Denk hierbij aan:

- De gebruikersondersteuning van de dienst. Deze handleiding vertelt alleen wat u nodig heeft om te kunnen aansluiten op TVS. Zodra de aansluiting met TVS in productie is, moet uw organisatie zelf de aansluiting van TVS kunnen beheren.
- Voor algemene vragen over DigiD en DigiD Machtigen kunnen burgers terecht bij de helpdesk van DigiD. Wij raden u aan voor vragen van eindgebruikers binnen uw organisatie gebruikersondersteuning in te richten met kennis van uw eigen processen en techniek.
- De verantwoordelijkheid voor het functioneel beheer, inclusief het informeren van TVS bij belangrijke wijzigingen aan de aansluiting en dienst.
- Het begeleiden van het jaarlijkse ICT-beveiligingsassessment.
- Het beheer van de PKI-overheid- en UZI-certificaten.

U kunt altijd wijzigingen door laten voeren aan de aansluiting nadat deze is opgeleverd. Hiervoor kunt u gebruik maken van het wijzigingsformulier op de TVS website. Mocht u er niet uit komen, neem dan gerust contact op via tv@dictu.nl

5.7 Blijf geïnformeerd

Bij belangrijke wijzigingen aan TVS wordt u altijd via de mail en de eFlash-app geïnformeerd. Zorg er dus voor dat de email-adressen die bij het TVS-team bekend zijn ook actueel zijn. Wij raden aan om gebruik te maken van postbussen waar meerdere personen in uw organisatie bij kunnen. Ook is het belangrijk dat u de eFlash-app download op uw telefoon. De eFlash-app kunt u downloaden via de volgende link <https://apps.dictu.nl/eflash>