Dienst ICT Uitvoering
Ministerie van Economische Zaken en Klimaat

Functionele beschrijving TVS

Versie: 2.0

Datum: 12-06-2026

Status: Definitief

Inhoud

1. Inleiding

Dit hoofdstuk beschrijft de functie en werking van de ToegangVerleningService (TVS). Daarnaast wordt toegelicht voor welke organisaties TVS bedoeld is en hoe het aansluitproces verloopt.

1.1 Achtergrond

De digitalisering van de samenleving zorgt ervoor dat steeds meer dienstverlening online plaatsvindt. Hierbij worden in toenemende mate persoonsgegevens en andere privacygevoelige gegevens uitgewisseld. Het is daarom van groot belang dat de toegang tot digitale diensten op een veilige en betrouwbare manier wordt geregeld.

De overheid stelt stapsgewijs hogere eisen aan de betrouwbaarheid van inlogmiddelen die worden gebruikt voor digitale dienstverlening. Deze eisen zijn vastgelegd in de Wet digitale overheid (WDO) en het bijbehorende stelsel van erkende inlogmiddelen.

De ToegangVerleningService (TVS) ondersteunt overheidsinstellingen, zorgorganisaties en andere dienstverleners bij het implementeren van deze erkende inlogmiddelen en bij het voldoen aan de gestelde betrouwbaarheidsniveaus.

1.2 Wat is TVS?

TVS functioneert als een centrale routeringsdienst voor erkende inlogmiddelen binnen het Stelsel Toegang. Door aan te sluiten op TVS kunnen dienstverleners gebruikmaken van meerdere authenticatiediensten via één technische koppeling.

TVS ondersteunt onder andere de volgende authenticatiediensten:

- DigiD
- DigiD Machtigen
- eHerkenning
- eIDAS

Het belangrijkste voordeel van TVS is dat dienstverleners slechts één koppeling hoeven te realiseren om gebruik te kunnen maken van zowel bestaande als toekomstige erkende inlogmiddelen. Hierdoor is er sprake van een toekomstbestendige inrichting van de authenticatievoorziening.

1.3 Voor wie is TVS?

TVS is beschikbaar voor de volgende typen organisaties:

Publiekrechtelijke organisaties

- (Semi) Overheden
- Overheidsinstellingen
- Uitvoeringsorganisaties

Zorgverleners

- Ziekenhuizen
- Huisartsen
- Tandartsen
- Fysiotherapeuten
- Andere zorgverleners die niet onder genoemde categorieën vallen

Private organisaties met een publieke taak

- Organisaties met een publieke taak die geen onderdeel zijn van de overheid, maar wel verantwoordelijk zijn voor het uitvoeren van taken die een maatschappelijk belang dienen of een publieke functie hebben.

Overig

- Software- en ICT leveranciers die namens voornoemde organisaties beheer- en ontwikkelwerkzaamheden verrichten.

1.4 Hoe werkt het aansluitproces?

Het aansluiten op TVS verloopt via het portaal MijnTVS. MijnTVS is een selfserviceportaal waarin aansluithouders hun TVS-aansluitingen kunnen registreren, configureren en beheren.

Het aansluitproces bestaat uit vier fasen:

Preproductiefase

In deze fase wordt de aansluiting geregistreerd, worden de technische configuraties vastgelegd en kan de implementatie worden getest in de preproductie omgeving.

Checklist testen

Tijdens deze fase wordt gecontroleerd of de implementatie correct functioneert en voldoet aan de technische eisen voor aansluiting op TVS.

Aanvullende gegevens

Na goedkeuring van de checklist worden aanvullende organisatie- en contactgegevens aangeleverd die nodig zijn voor productiegebruik.

Productiefase

Wanneer alle gegevens zijn aangeleverd en goedgekeurd kan de aansluiting worden geactiveerd in de productie omgeving. Indien van toepassing wordt in deze fase ook het DigiD-assessment doorlopen.

Een gedetailleerde beschrijving van deze stappen is opgenomen in de Handleiding MijnTVS.

Indien MijnTVS voor een organisatie nog niet beschikbaar is, kunnen aanvragen voorlopig worden ingediend via de bestaande aanvraag- en wijzigingsformulieren op de TVS-website.

1.5 Kosten gebruik TVS

Aan het gebruik van TVS in de productie omgeving zijn kosten verbonden. Hoewel TVS onderdeel is van de Generieke Digitale Infrastructuur (GDI), verloopt de facturatie momenteel via DICTU.

Organisaties die gebruik willen maken van de productie omgeving moeten een dienstverleningsovereenkomst (DVO) afsluiten.

Voor zorgorganisaties die vallen onder de DVO van het Ministerie van Volksgezondheid, Welzijn en Sport worden geen afzonderlijke kosten in rekening gebracht.

De preproductie omgeving kan kosteloos worden gebruikt voor het ontwikkelen en testen van een TVS-aansluiting.

Voor vragen over kosten kan contact worden opgenomen met TVS via tvs@dictu.nl.

1.6 Relatie met andere documentatie

Deze functionele beschrijving maakt deel uit van een bredere documentatieset:

- **Functionele beschrijving MijnTVS**: Beschrijft de functionaliteiten van het MijnTVS portaal waarmee u uw aansluitingen op TVS kunt registreren en beheren.
- **Handleiding MijnTVS**: Bevat praktische instructies voor het gebruik van MijnTVS.
- **Koppelvlakspecificaties SAML eID 4.4**: Bevat de technische specificaties van het koppelvlak.
- **Handleiding certificaatwissels**: Bevat instructies voor het vervangen van certificaten.

2. Architectuur en Werking

Dit hoofdstuk beschrijft de architectuur van TVS en de werking van de routeringsdienst binnen het authenticatielandschap. Hierbij wordt ingegaan op de rol van TVS in de authenticatieketen en de interactie met dienstverleners en authenticatiediensten.

2.1 TVS als routeringsdienst

TVS functioneert als een centrale routeringsdienst tussen dienstverleners en authenticatiediensten. De dienst faciliteert de uitwisseling van authenticatieverzoeken en -responses, maar voert zelf geen authenticatie of autorisatie uit.

De belangrijkste kenmerken van TVS zijn:

- TVS routeert authenticatieverzoeken en -responses tussen dienstverleners en authenticatiediensten.
- De daadwerkelijke authenticatie vindt plaats bij de betreffende authenticatiedienst (bijvoorbeeld DigiD of eHerkenning).
- De autorisatie van de gebruiker wordt door de dienstverlener zelf uitgevoerd.
- TVS is voor eindgebruikers grotendeels onzichtbaar, behalve tijdens de keuze van een authenticatiedienst via de TVS Smartloginpagina.

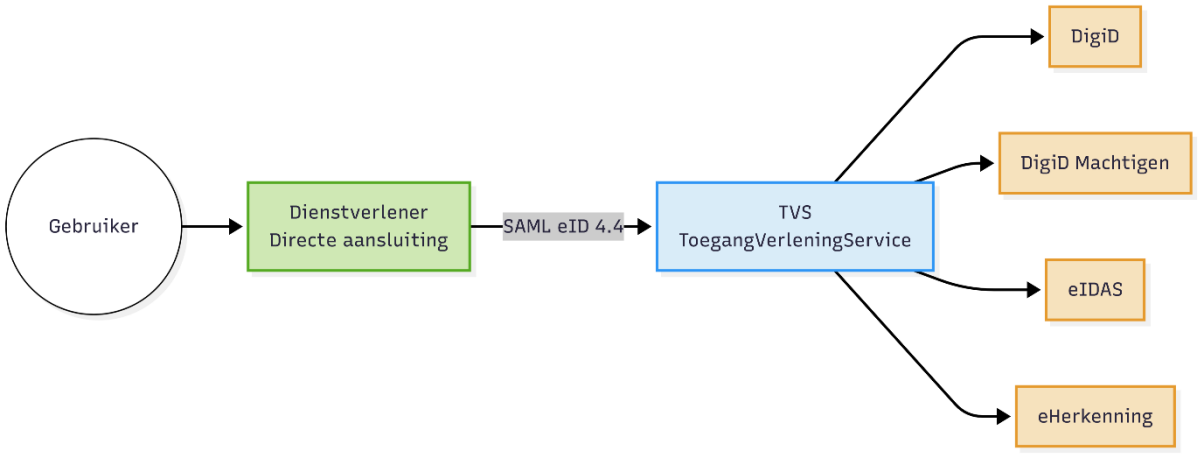
Een standaard authenticatieproces via TVS met DigiD verloopt als volgt:

1. De gebruiker bevindt zich op de website van de dienstverlener en kiest ervoor om in te loggen.
2. De gebruiker kiest een authenticatiedienst (bijvoorbeeld DigiD), of wordt - wanneer er geen keuze is - direct door gerouteerd naar de authenticatiedienst.
3. De dienstverlener stuurt een authenticatieverzoek naar TVS.
4. TVS stuurt de gebruiker door naar de authenticatiedienst.
5. De authenticatiedienst valideert de inloggegevens van de gebruiker.
6. Na succesvolle authenticatie ontvangt TVS een authenticatieresponse van de authenticatiedienst.
7. TVS stuurt de response met de relevante identiteitsgegevens en het betrouwbaarheidsniveau door naar de dienstverlener.
8. De dienstverlener bepaalt op basis van deze gegevens of de gebruiker geautoriseerd is om de gevraagde dienst te gebruiken.

2.2 Type aansluitingen

TVS biedt twee typen aansluitingen om verschillende implementatiescenario's te ondersteunen. De keuze voor het type aansluiting hangt af van de structuur en behoeften van uw organisatie.

2.2.1 Directe aansluiting



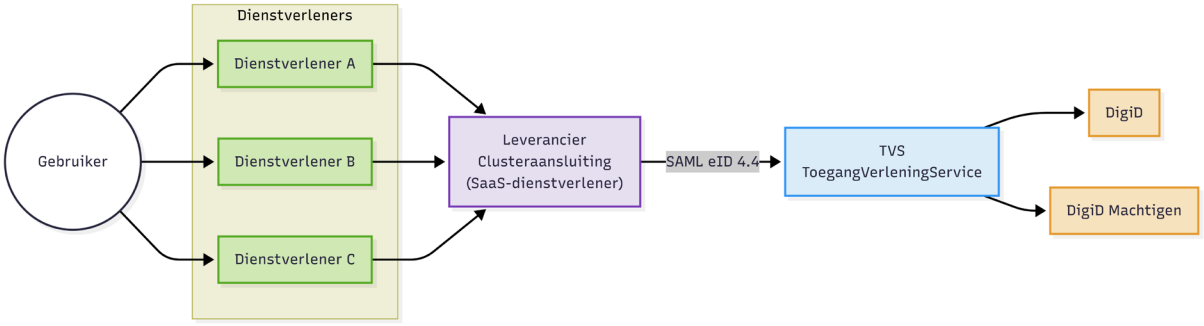
Figuur 1: Visuele weergave van een directe aansluiting op TVS

Bij een directe aansluiting communiceert de organisatie rechtstreeks met TVS via het eID SAML 4.4 koppelvlak. De organisatie stuurt een authenticatieverzoek naar TVS. TVS fungeert daarbij als tussenpartij en leidt het verzoek door naar de authenticatiedienst (AD), die de identiteit van de gebruiker vaststelt met behulp van een erkend inlogmiddel. Na succesvolle authenticatie retourneert de authenticatiedienst (AD) een SAML-response met de vastgestelde identiteitsgegevens. TVS ontvangt deze response en routeert deze door naar de organisatie.

- De aansluiting is bestemd voor één individuele organisatie.
- Per aansluiting wordt één webdienst ondersteund.
- Voor het gebruik van het BSN moet de organisatie zijn opgenomen op de Autorisatielijst BSN-gerechtigden (ALB-lijst).

Een directe aansluiting is geschikt voor organisaties die de koppeling zelf realiseren of daarvoor een ICT-leverancier inschakelen. Organisaties die het aansluitproces willen vereenvoudigen, kunnen kiezen voor aansluiting via een clusteraansluiting (zie §2.2.2).

2.2.2 Leverancier Clusteraansluiting



Figuur 2: Visuele weergave van een clusteraansluiting op TVS

Een clusteraansluiting is bedoeld voor ICT-leveranciers die een gestandaardiseerde SaaS-oplossing aanbieden aan meerdere dienstverleners. Bij deze aansluitvorm realiseert de ICT-leverancier één technische koppeling met TVS, waarvan meerdere dienstverleners gebruik kunnen maken via dezelfde applicatie of dienst.

De ICT-leverancier treedt hierbij op als Leverancier Meervoudig Assessment (LMA) en beheert de gedeelde technische infrastructuur en koppeling met TVS. De organisaties die gebruikmaken van deze dienst worden aangeduid als aansluithouders.

Binnen de clusteraansluiting wordt bij een authenticatieverzoek vastgelegd namens welke aansluithouder de gebruiker inlogt, zodat TVS weet voor welke organisatie de authenticatie wordt uitgevoerd.

Kenmerken van een clusteraansluiting

- De aansluiting wordt gerealiseerd en technisch beheerd door een ICT-leverancier (LMA).
- Meerdere aansluithouders kunnen via één aansluiting gebruikmaken van de koppeling met TVS.
- Alle aansluithouders maken gebruik van dezelfde technische configuratie en implementatie van de koppeling.
- Voor clusteraansluitingen is een meervoudig ICT-beveiligingsassessment verplicht.
- Bij een meervoudig assessment wordt de SaaS-dienst van de ICT-leverancier beoordeeld. Het assessmentrapport kan vervolgens worden gebruikt door alle aansluithouders die gebruikmaken van deze dienst.
- Iedere aansluithouder moet zijn opgenomen op de Autorisatielijst BSN-gerechtigden (ALB-lijst) indien gebruik wordt gemaakt van het BSN.
- De ICT-leverancier die optreedt als LMA hoeft zelf niet op de ALB-lijst te staan.

Een clusteraansluiting is geschikt wanneer een ICT-leverancier dezelfde SaaS-oplossing aanbiedt aan meerdere organisaties die gebruikmaken van TVS.

Door gebruik te maken van één gedeelde koppeling en een meervoudig assessment worden implementatie, beheer en audit efficiënter ingericht.

2.2.3 Vergelijkingstabel

Kenmerk	**Directe aansluiting**	**Clusteraansluiting**
Beheer	Dienstverlener	ICT-leverancier (LMA)
Aantal organisaties	1	Meerdere
Technische koppeling	Per organisatie	Gedeeld
Assessment	Per organisatie	Meervoudig assessment
Gebruik	Eigen applicatie	SaaS oplossing

2.3 Authenticatiediensten

TVS ondersteunt de volgende authenticatiediensten:

DigiD

- Voor authenticatie van burgers.
- Beschikbaar op de betrouwbaarheidsniveaus laag, substantieel en hoog.
- Vereist een periodiek DigiD-ICT-beveiligingsassessment.

DigiD Machtigen

- Maakt het mogelijk om personen te machtigen.
- Volgt het betrouwbaarheidsniveau van DigiD.
- Is uitsluitend beschikbaar in combinatie met DigiD.

eHerkenning

- Voor authenticatie van organisaties en bedrijven.
- Beschikbaar op betrouwbaarheidsniveaus 2+ (midden), 3 (substantieel) en 4 (hoog).

eIDAS

- Voor Europese persoonlijke en zakelijke inlogmiddelen.
- Alleen beschikbaar op niveau Hoog.

2.4 TVS Smartlogin

De TVS Smartloginpagina is een belangrijk onderdeel van de klantreis bij het inloggen. Als centrale routeringspagina zorgt deze voor een uniforme en herkenbare klantreis bij alle aangesloten organisaties.

Waar gebruikers voorheen verschillende inlogschermen tegenkwamen bij verschillende dienstverleners, biedt de TVS Smartloginpagina nu één consistent beeld. Of een burger nu wil inloggen bij een overheidsinstelling, zorgverlener, of andere aangesloten organisatie, de keuze voor het inlogmiddel verloopt altijd via hetzelfde, vertrouwde scherm.

De TVS Smartloginpagina:

- vormt een herkenbare en uniforme schakel in de klantreis voor alle aansluitingen;
- wordt uitsluitend getoond wanneer meerdere authenticatiediensten beschikbaar zijn;
- toont alleen de authenticatiediensten die voor de betreffende dienst zijn geactiveerd;
- is beschikbaar in het Nederlands en Engels;
- wordt automatisch bijgewerkt wanneer nieuwe authenticatiediensten worden geactiveerd.

Belangrijk: De Smartloginpagina is voor alle dienstverleners identiek en kan niet worden aangepast. Het gebruik van eigen authenticatiemiddelen via de Smartloginpagina wordt niet ondersteund.

Figuur 3: Voorbeeld van de TVS Smartloginpagina met 4 authenticatiediensten

De pagina wordt door TVS weergegeven nadat een dienstverlener een authenticatieverzoek heeft gestart en er meerdere authenticatiediensten beschikbaar zijn voor de betreffende dienst.

2.4.1 Scoping

TVS biedt dienstverleners de mogelijkheid om de Smartloginpagina over te slaan door gebruik te maken van Scoping in het authenticatieverzoek. Met Scoping kan een specifieke authenticatiedienst direct worden geselecteerd.

De technische details over het gebruik van Scoping zijn opgenomen in hoofdstuk 7.3 SAML AuthnRequest van de Koppelvlakspecificatie eID SAML 4.4.

Scoping kan worden toegepast wanneer een dienstverlener op de eigen website aparte inlogknoppen voor verschillende authenticatiemiddelen aanbiedt.

2.4.2 Taal en informatie

De TVS Smartloginpagina biedt ondersteuning voor meerdere talen en aanvullende informatie over de beschikbare authenticatiediensten.

Taalondersteuning

- Automatische taalselectie op basis van de browserinstellingen van de gebruiker (Nederlands of Engels).
- Mogelijkheid voor de gebruiker om handmatig van taal te wisselen.

Informatievoorziening

- Per authenticatiedienst is aanvullende informatie beschikbaar.
- De pagina bevat links naar relevante externe informatiebronnen over de betreffende inlogmiddelen.

2.5 Betrouwbaarheidsniveaus

TVS ondersteunt verschillende betrouwbaarheidsniveaus die de mate van zekerheid bepalen over de identiteit van de gebruiker. We hanteren hierbij de eIDAS-niveaus:

- Laag – authenticatie met gebruikersnaam en wachtwoord, eventueel aangevuld met een tweede factor zoals sms, QR-code of een app. Er vindt geen ID-check plaats. Dit niveau biedt een beperkte mate van zekerheid over iemands identiteit en is geschikt voor minder gevoelige dienstverlening.
- Substantieel – authenticatie met twee factoren en een eenmalige ID-check. Bijvoorbeeld via een app waarbij een identiteitsdocument zoals een paspoort, rijbewijs of ID-kaart wordt gescand. Dit niveau biedt een behoorlijke mate van zekerheid over iemands identiteit en wordt gebruikt voor diensten met privacygevoelige gegevens of bijzondere persoonsgegevens.
- Hoog – authenticatie met een app, pas of ander middel waarbij bij elke inlog een ID-check op het toestel of via een fysiek middel plaatsvindt. Vaak is hierbij ook een persoonlijke pincode nodig. Dit niveau biedt de hoogste mate van zekerheid over iemands identiteit en is verplicht voor zeer gevoelige gegevens, zoals medische gegevens die onder het beroepsgeheim vallen.

Meer informatie over betrouwbaarheidsniveaus is te vinden op de pagina Betrouwbaarheidsniveaus DigiD en het Stelsel Toegang.

2.5.1 Bepalen betrouwbaarheidsniveau

De dienstverlener is zelf verantwoordelijk voor het bepalen van het juiste betrouwbaarheidsniveau op basis van het risicoprofiel van de aangeboden diensten. Bij het configureren van een dienst in MijnTVS kan worden aangegeven wat het minimale betrouwbaarheidsniveau is dat een gebruiker moet hanteren voor het inloggen.

Voor hulp bij het bepalen van het juiste betrouwbaarheidsniveau kan er gebruik worden gemaakt van de Regelhulp betrouwbaarheidsniveaus. Deze online tool helpt u stap voor stap bij het maken van de juiste keuze op basis van uw specifieke situatie.

2.6 Sessiemanagement

Sessiemanagement is een belangrijk onderdeel van de authenticatieprocessen via TVS. Het bepaalt hoe lang een sessie geldig blijft en wanneer een gebruiker opnieuw moet inloggen. TVS volgt hierbij de richtlijnen van de afzonderlijke authenticatiediensten om de veiligheid te waarborgen. De eindverantwoordelijkheid voor het beheer van gebruikerssessies ligt bij de dienstverlener.

TVS hanteert de volgende waarde:

- Time-out op de Smartloginpagina: 15 minuten.

TVS biedt geen ondersteuning voor Single Sign-On (SSO). TVS zet het attribuut @ForceAuthn bij iedere authenticatieaanvraag standaard op ‘true’.

Dit betekent dat een bestaande sessie niet mag worden hergebruikt en dat de eindgebruiker bij elke authenticatieaanvraag opnieuw moet inloggen.

2.7 Beveiliging

De beveiliging van de communicatie tussen dienstverleners en TVS is van groot belang voor de bescherming van persoonsgegevens en voor het waarborgen van de integriteit van het authenticatieproces. TVS hanteert daarom specifieke beveiligingseisen waaraan alle aangesloten organisaties moeten voldoen.

Deze eisen verschillen per authenticatiedienst, maar omvatten in ieder geval:

- het gebruik van geldige certificaten, zoals PKIoverheid-certificaten;
- het veilig beheren van privésleutels en het tijdig vernieuwen van certificaten;
- het correct opstellen, ondertekenen en publiceren van metadata;
- het toepassen van actuele TLS-richtlijnen en andere beveiligingsrichtlijnen van het NCSC;
- het gebruik van digitale handtekeningen om de authenticiteit en integriteit van berichten te waarborgen.

Voor DigiD gelden daarnaast aanvullende beveiligingseisen, waaronder verplichte ICT-beveiligingsassessments. Voor eHerkenning en eIDAS zijn de beveiligingseisen vastgelegd in het Afsprakenstelsel Elektronische Toegangsdiensten. Aangesloten organisaties zijn zelf verantwoordelijk voor het naleven van deze eisen en voor het tijdig doorvoeren van wijzigingen daarin.

2.7.1 PKIoverheid certificaten

Voor het beveiligen van de berichtenuitwisseling met TVS zijn PKIoverheid-certificaten verplicht. PKIoverheid is een afsprakenstelsel voor digitale certificaten dat veilige en betrouwbare elektronische communicatie tussen overheidsorganisaties, burgers en bedrijven mogelijk maakt. Het afsprakenstelsel wordt beheerd door Logius en vormt een onderdeel van de Generieke Digitale Infrastructuur (GDI).

PKIoverheid-certificaten worden binnen TVS gebruikt voor:

- het ondertekenen van berichten;
- het versleutelen van berichten;
- het opzetten van mTLS-verbindingen.

TVS accepteert de volgende typen certificaten:

- PKIoverheid G1 Private Root
- UZI-servercertificaat (alleen voor zorgorganisaties)

2.7.2 Certificate rollover functionaliteit

Alle organisaties die op TVS aansluiten moeten certificate rollover ondersteunen. Certificate rollover is het proces waarbij een bestaand certificaat tijdig wordt vervangen door een nieuw certificaat, zonder dat de dienstverlening wordt onderbroken.

Hierbij zijn gedurende een overgangsperiode zowel het oude als het nieuwe certificaat geldig en opgenomen in de metadata. Hierdoor kunnen beide partijen het nieuwe certificaat alvast ophalen en vertrouwen, terwijl het oude certificaat nog actief blijft voor bestaande communicatie. Zodra beide partijen het nieuwe certificaat gebruiken, kan het oude certificaat worden verwijderd.

Door certificate rollover correct toe te passen wordt voorkomen dat koppelingen uitvallen bij het verlopen of vervangen van certificaten.

Ondersteuning in de keten

Certificate rollover wordt binnen de authenticatieketen ondersteund door:

- TVS
- Logius (voor DigiD en DigiD Machtigen)
- eTD-stelsel (voor eHerkenning en eIDAS)

Technische implicaties

Bij de implementatie van certificate rollover moet het systeem van de dienstverlener in staat zijn om:

- meerdere certificaten gelijktijdig te accepteren;
- versleutelde responses te verwerken die met verschillende certificaten zijn versleuteld;
- periodiek de TVS-metadata in te lezen om certificaatwijzigingen te detecteren.

Gedetailleerde technische instructies zijn te vinden in de handleiding Certificaatgebruik binnen TVS.

2.7.3 TVS Metadata endpoints

TVS stelt metadata beschikbaar via speciaal ingerichte endpoints. Deze metadata bevat essentiële technische informatie die nodig is voor een correcte en veilige communicatie met TVS.

De metadata bevat onder andere:

- informatie over de gebruikte certificaten;
- de beschikbare endpoints;
- identificatiegegevens van de TVS-entities.

Beschikbare metadata-endpoints

Preproductie omgeving

- https://pp2.toegang.overheid.nl/kvs/rd/metadata

Productie omgeving

- https://rd2.toegang.overheid.nl/kvs/rd/metadata

Parameters voor certificate rollover

Bij het opvragen van de metadata met bovenstaande URLs worden zowel actieve, als eventuele toekomstige certificaten geretourneerd. Voor ondersteuning van certificate rollover is dit noodzakelijk.

Bij het opvragen van de metadata kunnen eventueel de volgende parameters worden gebruikt:

- ?certs=active – retourneert alleen het momenteel actieve certificaat
- ?certs=future – retourneert alleen het toekomstige certificaat (indien beschikbaar)

Het wordt aanbevolen om de metadata minimaal één keer per 24 uur automatisch in te lezen en eventuele wijzigingen in de eigen systemen te verwerken. Bij de implementatie is het belangrijk rekening te houden met foutafhandeling en fallback-scenario's voor het geval de metadata tijdelijk niet beschikbaar is.

3. Operationeel beheer

Dit hoofdstuk beschrijft de operationele aspecten van TVS, waaronder monitoring, ketenafhankelijkheden en ondersteuning. Deze informatie helpt aansluithouders bij het beheren van hun TVS-aansluiting en bij het omgaan met operationele gebeurtenissen zoals storingen of onderhoud.

3.1 Monitoring

Voor het monitoren van de TVS dienst dient u de status endpoints die TVS biedt te gebruiken:

Productie:

- https://rd2.toegang.overheid.nl/status

Preproductie:

- https://pp2.toegang.overheid.nl/status

Deze endpoints hebben de volgende kenmerken:

- Geven de realtime status van belangrijke TVS-componenten weer.
- Kunnen worden geïntegreerd in monitoringsystemen.
- Zijn specifiek bedoeld voor statusmonitoring.
- Blijven beschikbaar tijdens onderhoudswerkzaamheden.

Belangrijke richtlijnen

Het is niet toegestaan om:

- **de TVS productie- of preproductie omgeving direct te proben;**
- **load- of beschikbaarheidstests uit te voeren op TVS;**
- **penetratietests uit te voeren op TVS.**

Het niet naleven van deze richtlijnen kan leiden tot blokkering van uw aansluiting.

3.2 Ketenafhankelijkheden

TVS maakt deel uit van een bredere authenticatieketen waarin verschillende organisaties en diensten samenwerken om gebruikers veilig te laten inloggen bij aangesloten dienstverleners. Voor een aantal functionaliteiten is TVS afhankelijk van externe ketenpartners.

Storingen, onderhoud of wijzigingen bij deze partners kunnen invloed hebben op de beschikbaarheid van de authenticatiediensten die via TVS worden aangeboden.

De belangrijkste ketenpartners van TVS zijn:

- Logius (DigiD en DigiD Machtigen)
- eHerkenning (via erkende makelaars en middelenleveranciers)
- eIDAS (Europese inlogmiddelen)

Voor een overzicht van de communicatiekanalen van deze ketenpartners en informatie over hoe u zich hiervoor kunt aanmelden, verwijzen wij naar het document TVS Keten communicatiekanalen op de TVS-website.

In de volgende paragrafen wordt per ketenpartner toegelicht welke afhankelijkheden bestaan en welke mogelijke impact storingen kunnen hebben op de dienstverlening. Deze verstoringen vallen buiten de verantwoordelijkheid van TVS.

3.2.1 Logius (DigiD en DigiD Machtigen)

Logius is verantwoordelijk voor DigiD en DigiD Machtigen. Een storing bij Logius kan de volgende impact hebben:

- Inloggen met DigiD en/of DigiD Machtigen is niet mogelijk.
- Er kan vertraging optreden in het aansluit- en wijzigingsproces.

Bij een storing bij Logius kan TVS alleen doorverwijzen naar andere beschikbare authenticatiediensten zoals eHerkenning. Voor de actuele status van DigiD kunt u de Logius communicatiekanalen raadplegen.

3.2.2 eHerkenning

Voor eHerkenning maakt TVS gebruik van twee makelaars, een primaire makelaar en een secundaire makelaar.

Bij een storing bij de primaire makelaar schakelt TVS automatisch over naar de secundaire makelaar. Dit gebeurt zonder tussenkomst van de dienstverlener of de eindgebruiker.

Let op: Bij gebruik van Scoping in het AuthnRequest is automatische failover niet mogelijk.

3.2.3 Middelenleveranciers

Een storing bij een eHerkenning middelenleverancier (zoals bijvoorbeeld KPN, Digidentity of anderen):

- treft alleen gebruikers die een inlogmiddel hebben van die specifieke leverancier;
- verloopt eventuele communicatie met betrekking tot de storing via de betreffende eHerkenning middelenleverancier.

3.2.4 eIDAS

eIDAS biedt toegang tot Europese inlogmiddelen. Een storing bij eIDAS kan leiden tot:

- onbeschikbaarheid van Europese inlogmiddelen;
- vertraging in het aansluit- en wijzigingsproces voor diensten die eIDAS gebruiken.

3.3 Support en communicatie

Voor vragen over uw TVS-aansluiting, het melden van storingen of andere operationele verzoeken kunt u contact opnemen met TVS Functioneel Beheer.

Contactgegevens

- E-mail: tvs@dictu.nl
- Website: https://tvs.dictu.nl

Bereikbaarheid: werkdagen van 08:00 tot 17:00 uur.

TVS Functioneel Beheer ondersteunt bij:

- operationele vragen over uw aansluiting;
- het melden van storingen of incidenten;
- algemene vragen over de dienstverlening van TVS.

3.3.1 Communicatiekanalen

TVS maakt gebruik van verschillende communicatiekanalen om aansluithouders te informeren over storingen, onderhoud en wijzigingen in de dienstverlening. De belangrijkste kanalen zijn:

- eFlash – app voor operationele meldingen zoals storingen en gepland onderhoud;
- E-mail – voor communicatie over specifieke aansluitingen;
- Website – voor algemene informatie, documentatie en nieuwsberichten.

eFlash-notificaties

TVS gebruikt de eFlash-app als primair kanaal voor operationele meldingen. Via deze app worden notificaties verzonden over onder andere:

- storingen en incidenten;
- gepland onderhoud;
- implementatie van nieuwe functionaliteiten;
- belangrijke wijzigingen in de dienstverlening.

Van alle aansluithouders wordt verwacht dat zij zich aanmelden voor eFlash-notificaties, zodat zij tijdig op de hoogte zijn van ontwikkelingen die invloed kunnen hebben op hun dienstverlening.

De eFlash-app is beschikbaar via de Rijksappstore:

https://rijksappstore.nl/eflash

DICTU adviseert aansluithouders om minimaal twee contactpersonen aan te melden voor eFlash-notificaties, de contactgegevens in MijnTVS actueel te houden en regelmatig de TVS-website te raadplegen voor updates en nieuwe documentatie.

3.3.2 Blijf geïnformeerd over de keten

TVS is een routeringsdienst en maakt deel uit van een bredere authenticatieketen. Via deze keten kunnen gebruikers met erkende inlogmiddelen toegang krijgen tot diensten van aangesloten organisaties.

Het is daarom belangrijk dat aansluithouders zich niet alleen informeren over de status van TVS, maar ook over de status van andere partners in de keten, zoals DigiD, eHerkenning en eIDAS.

A: Begrippenlijst

Begrip	Definitie
ALB-lijst	Autorisatielijst BSN-gerechtigden; register van organisaties die BSN mogen verwerken.
Authenticatiedienst	Dienst waarmee gebruikers kunnen inloggen (bijvoorbeeld DigiD).
AuthnRequest	SAML-bericht waarmee een dienstverlener via TVS een authenticatieverzoek start.
Betrouwbaarheidsniveau	Mate van zekerheid over de identiteit van de gebruiker (bijvoorbeeld Midden, Substantieel of Hoog).
BSN	Burgerservicenummer; uniek identificatienummer voor Nederlandse burgers.
Certificate rollover	Proces waarmee certificaatwissels kunnen worden uitgevoerd zonder dienstonderbreking.
Clusteraansluiting	Aansluiting waarbij een ICT-leverancier meerdere dienstverleners onder één technische koppeling bedient.
Dienstverlener	Organisatie die digitale diensten aanbiedt en gebruikmaakt van TVS voor authenticatie van gebruikers.
DigiD	Authenticatiedienst voor Nederlandse burgers.
DigiD Machtigen	Dienst waarmee burgers anderen kunnen machtigen om namens hen in te loggen.
Directe aansluiting	Aansluiting voor één individuele organisatie.
DVO	Overeenkomst tussen TVS/DICTU en een organisatie waarin de afspraken over het gebruik van de productieomgeving zijn vastgelegd.
eFlash	Communicatie-app voor operationele mededelingen zoals storingen en onderhoud.
eHerkenning	Authenticatiedienst voor organisaties en bedrijven.
eIDAS	European electronic Identification, Authentication and trust Services; Europees stelsel voor grensoverschrijdende digitale identificatie binnen de EU.
EntityID	Unieke identificatie van een partij binnen een SAML-federatie.
GDI	Het gezamenlijke stelsel van digitale voorzieningen waarmee Nederlandse overheidsorganisaties veilig gegevens uitwisselen en digitale diensten aanbieden.

LMA	ICT-leverancier die een clusteraansluiting beheert en namens meerdere aansluithouders één meervoudig beveiligingsassessment laat uitvoeren.
Metadata	XML-document met technische configuratiegegevens zoals certificaten, entityID's en endpoints die nodig zijn voor communicatie tussen partijen.
MijnTVS	Selfserviceportaal voor het registreren en beheren van TVS-aansluitingen.
mTLS	Mutual Transport Layer Security; beveiligingsmechanisme waarbij beide partijen in een verbinding zich met een certificaat authentiseren.
NCSC	Nederlandse overheidsdienst die organisaties helpt bij het voorkomen, opsporen en afhandelen van cyberdreigingen en digitale beveiligingsincidenten.
OIN	Organisatie Identificatie Nummer; unieke identifier voor organisaties.
PKIoverheid certificaat	Digitaal certificaat uitgegeven binnen het PKIoverheid-stelsel dat wordt gebruikt voor veilige communicatie tussen organisaties en systemen.
SAML	Security Assertion Markup Language; standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen systemen.
SAML eID 4.4	Koppelvlakspecificaties voor de uitwisseling van authenticatiegegevens.
Scoping	Functionaliteit waarmee dienstverleners specifieke authenticatiediensten kunnen selecteren.
SaaS	Software as a Service; softwaremodel waarbij applicaties als een online dienst worden aangeboden.
Smartloginpagina	Door TVS aangeboden pagina waarop gebruikers een authenticatiedienst kunnen selecteren wanneer meerdere authenticatiediensten beschikbaar zijn.
TVS	ToegangVerleningService; centrale routeringsdienst voor erkende inlogmiddelen.
UZI	Unieke Zorgverlener Identificatie; identificatiemiddel voor zorgverleners.
WDO	Wet Digitale Overheid; wettelijk kader voor digitale dienstverlening door de overheid.