Functionele beschrijving ToegangVerleningService (TVS)

Versie: 1.0

Datum: 11-11-2022

Status: Definitief

Auteur: Fatih Yilmaz

Inhoud

1 Inleiding

Dit document heeft tot doel om de functie van TVS voor dienstverleners (de afnemers van TVS die een digitale dienst aan burgers en bedrijven leveren) uiteen te zetten. Ook een schetsmatige uitleg van de werking van TVS maakt hier onderdeel van uit. Daarnaast zal ook duidelijk worden wie mag of welke organisaties mogen aansluiten op TVS.

Deze pagina bevat geen technische documentatie over het aansluiten op TVS, die kunt u vinden op Koppelvlak specificatie eID SAML 4.4.

Vragen of suggesties?

Heeft u suggesties om dit document verder te verbeteren? Neem dan contact op via tvs@dictu.nl.

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 Achtergrond

We doen steeds meer online. Daardoor wisselen we ook steeds meer informatie digitaal uit. Vaak gaat het om persoonlijke, privacygevoelige gegevens. Veiligheid staat voorop. Nu, en in de toekomst. Als overheid zorgen we voor veilige manieren van inloggen. Daarom stelt de overheid stapsgewijs hogere eisen aan de inlogmiddelen die zorgaanbieders en overheidsinstellingen gebruiken om toegang te bieden tot digitale diensten.

TVS (ToegangVerleningService) is in het leven geroepen om overheidsinstellingen, dienstverleners en hun ICT-leveranciers te ondersteunen bij het implementeren van een verhoogd betrouwbaarheidsniveau van inlogmiddelen en tegelijk te waarborgen dat partijen goed zijn voorbereid op de komst van nieuwe, erkende inlogmiddelen.

1.2 Wat is TVS?

TVS fungeert als koppeling naar alle - onder de (nog te bekrachtigen) Wet Digitale Overheid (WDO) - erkende inlogmiddelen. Door aan te sluiten op TVS beschikt een zorgaanbieder of overheidsinstelling in één keer over een aansluiting op alle beschikbare erkende inlogmiddelen zoals DigiD, DigiD Machtigen, eHerkenning, Europese erkende inlogmiddelen (eIDAS-verordening), inclusief toekomstige erkende inlogmiddelen. Kortom: door aan te sluiten op TVS hebben dienstverleners dit deel van hun infrastructuur toekomstbestendig ingericht.

Een belangrijk voordeel van TVS: u heeft slechts één koppeling nodig voor aansluitingen op alle (toekomstige) erkende inlogmiddelen.

1.3 Wie mogen aansluiten op TVS?

TVS is beschikbaar voor de volgende organisaties.

- ICT Leveranciers van SAAS-oplossingen binnen het zorgdomein voor een TVS Clusteraansluiting
- Overheidsinstellingen
- Zorgverleners

1.4 Hoe sluit ik aan op TVS?

Om als dienstverlener aan te kunnen sluiten op TVS zijn een aantal stappen noodzakelijk. Op deze pagina wordt hier niet verder op ingegaan. De handleidingen voor aansluiten op TVS zijn te vinden op dictu.nl/tvs onder Documentatie & Links.

2. Waar bestaat TVS uit?

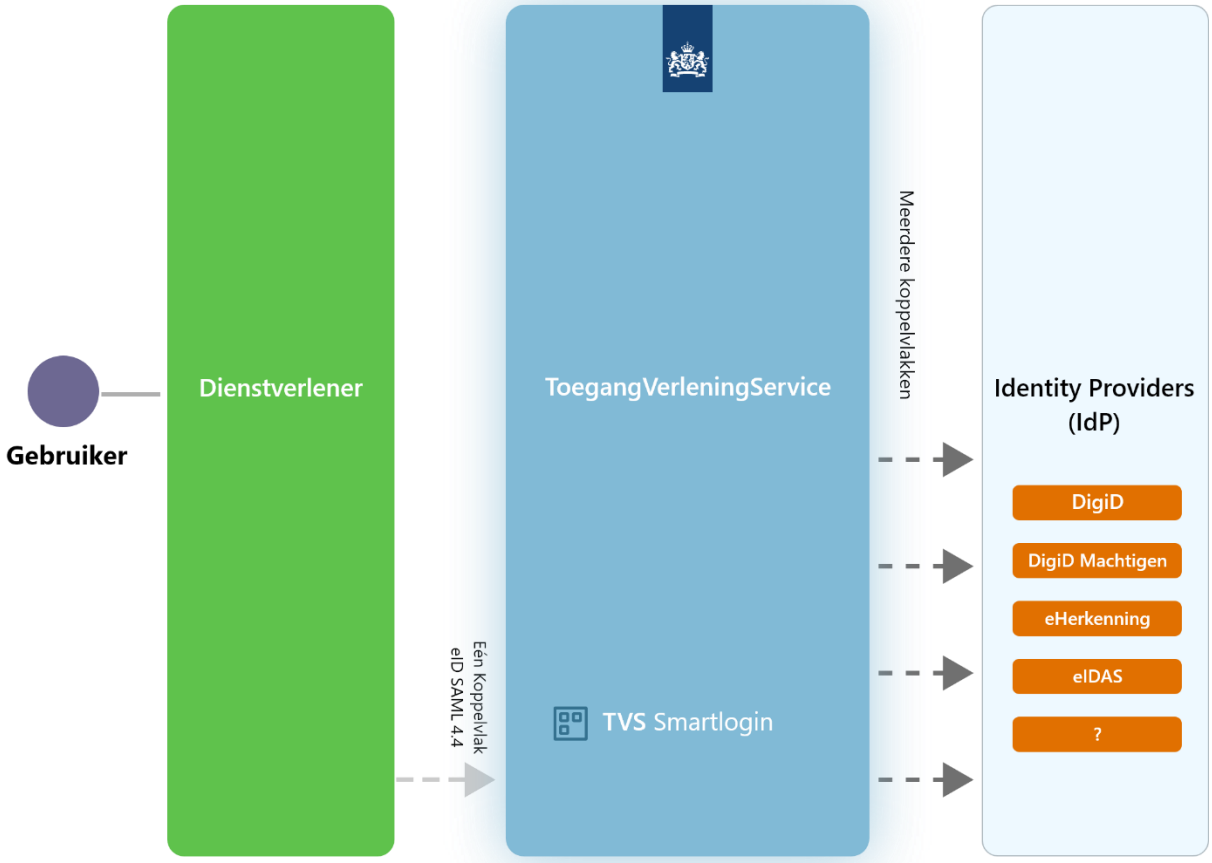
Dit hoofdstuk geeft inzicht in waar TVS uit bestaat en wat een dienstverlener krijgt na het aansluiten op TVS.

2.1 Type aansluitingen

Er zijn twee aansluit-varianten beschikbaar op TVS: een clusteraansluiting of een directe aansluiting.

2.1.1 Directe aansluiting

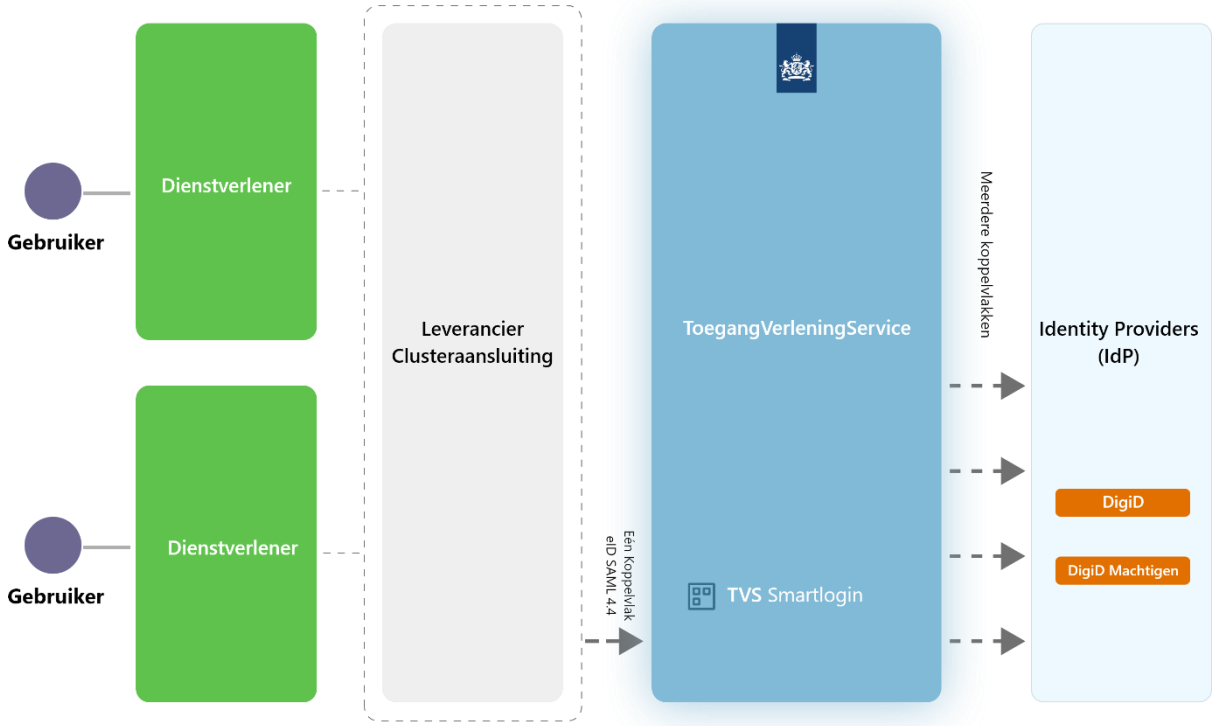
Bij een directe aansluiting sluit de dienstverlener zijn systeem direct aan op TVS. Er zijn geen andere dienstverleners die de aansluiting gebruiken zoals bij een clusteraansluiting van een ICT-leverancier.



Directe aansluiting op TVS

2.1.2 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 melden zich aan bij hun ICT-leverancier om aangesloten te worden op TVS.



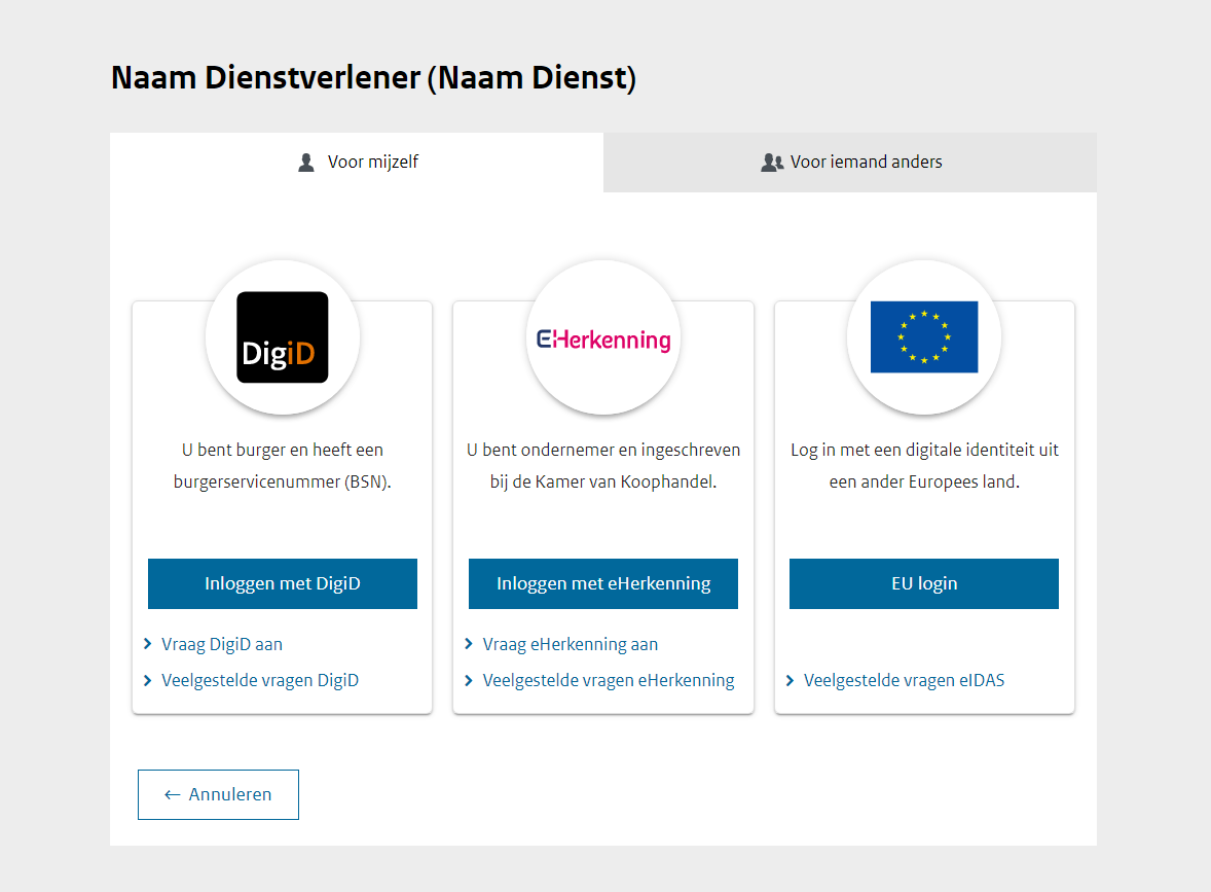
Een clusteraansluiting op TVS

Onderdeel	**Uitleg**
Gebruiker	Dit is de eindgebruiker (een burger) die gebruik gemaakt 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.

2.2 TVS 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 waarmee hij of zij wil inloggen.



De TVS Smartloginpagina met DigiD, DigiD Machtigen, eHerkenning en eIDAS als authenticatiemiddelen.

Het gebruik van de smartloginpagina is niet verplicht. Indien een dienstverlener enkel gebruik maakt van één authenticatiedienst zal de pagina niet getoond worden. Door gebruik te maken van Scoping in het autorisatieverzoek kan de Smartloginpagina overgeslagen worden. Dit maakt het voor een dienstverlener mogelijk om eigen inlogknoppen te gebruiken. Meer informatie over Scoping is te vinden in hoofdstuk 7.3 SAML AuthnRequest in Koppelvlak specificatie eID SAML 4.4.

3 Routeringsdienst

In dit hoofdstuk wordt uiteengezet wat de functionaliteiten van TVS als routeringsdienst zijn. We spreken hier over routeren, aangezien dit de TVS-functionaliteit is die dienstverleners gebruiken om aangesloten te worden bij één of meerdere authenticatiediensten (IdP's).

3.1 Hoe werkt TVS als routeringsdienst?

Zoals gezegd is TVS een routeringsdienst. Dit houdt in dat TVS niet authentiseert en ook niet autoriseert. De authenticatie en autorisatie vindt plaats bij de authenticatiediensten en dienstverleners. TVS stuurt de ontvangen authenticatieverzoeken door naar achterliggende authenticatiediensten en de reactie hierop terug naar de dienstverleners. TVS is hierdoor onzichtbaar voor de eindgebruikers. Een standaard routeringsflow op TVS ziet er als volgt uit:

Stap 1. Gebruiker

De burger bevindt zich op de website van een dienstverlener. De burger wil deze dienst gebruiken maar moet zich daarvoor authentiseren door middel van een erkend inlogmiddel.

Stap 2. Dienstverlener

Vanuit de website van de webdienst wordt de burger doorverwezen naar TVS. TVS maakt op basis van de verkregen informatie een smartloginpagina aan en toont deze via de browser aan de gebruiker.

Stap 3. Gebruiker

De gebruiker kiest op de getoonde smartloginpagina een IdP, bijvoorbeeld DigiD. De gemaakte keuze van de gebruiker wordt door de webbrowser weer naar TVS gestuurd.

Stap 4. Gebruiker

De gebruiker wordt vervolgens door TVS doorverwezen naar de IdP, in dit geval DigiD. Dit gebeurt in de achtergrond en is niet zichtbaar voor de gebruiker. De gebruiker ziet op het inlogscherm van DigiD duidelijk ten behoeve van welke dienstverlener en dienst hij of zij zich gaat authentiseren. Dit is dezelfde dienstverlener en dienst als in stap 1.

Stap 5. Authenticatiedienst (IdP)

De IdP voert een controle uit op de inloggegevens en stuurt een antwoord terug naar TVS.

Stap 6. TVS

TVS controleert het ontvangen bericht en verifieert dit nogmaals bij de IdP. De IdP antwoord vervolgens definitief terug met de opgevraagde gegevens in een versleuteld formaat (het BSN van de burger bij stap 1).

Stap 7. Dienstverlener

Na een succesvolle authenticatie van de gebruiker ontvangt de dienstverlener van TVS het BSN en het betrouwbaarheidsniveau waarop de authenticatie heeft plaatsgevonden. Deze informatie is versleuteld en kan alleen ontcijfert worden door de dienstverlener. De dienstverlener kan op basis van de ontvangen identificatie bepalen of de gebruiker geautoriseerd is om gebruik te maken van de dienst. De gebruiker komt na authenticatie weer terug op de site van de dienst, welke dezelfde is als in stap1.

Stap 8. Gebruiker

De gebruiker kan verder met het gebruiken van de dienst.

3.2 Betrouwbaarheidsniveaus

TVS ondersteund 3 betrouwbaarheidsniveaus die de mate van zekerheid bepalen over de identiteit van de zich authentiserende gebruiker. Deze betrouwbaarheidsniveaus zijn direct gekoppeld aan de afgenomen authenticatiediensten. Onderstaande tabel geeft de relatie tussen de verschillende erkende inlogmiddelen, gerangschikt naar oplopende betrouwbaarheid.

3.2.1 Midden

Inlogmethode: 2-factorauthenticatie via gebruikersnaam en wachtwoord, in combinatie met sms-code of pincode via een token

Beschrijving: gaat uit van de combinatie van iets dat een persoon weet en iets dat een persoon heeft. Deze combinatie maakt het inlogmiddel veiliger. Midden kan gebruikt worden als het gaat om uitwisseling van financieel-economische gegevens van gebruikers of bijzondere persoonsgegevens (godsdienst, politieke gezindheid, gezondheid).

3.2.2 Substantieel

Inlogmethode: 2-factorauthenticatie via gebruikersnaam en wachtwoord, in combinatie met sms-code of pincode via een token of app met QR-code

Beschrijving: gaat uit van de combinatie van iets dat een persoon weet en iets dat een persoon heeft. Daarnaast is geverifieerd dat de persoon in het bezit is van een Nederlands paspoort, Nederlandse identiteitskaart of rijbewijs dat de opgegeven identiteit vertegenwoordigt. Substantieel kan gebruikt worden als het gaat om uitwisseling van gegevens die extra privacygevoelig zijn zoals medische gegevens.

3.2.3 Hoog

Inlogmethode: Via PKI-certificaat of 2-factorauthenticatie.

Beschrijving: gaat uit van de uitgifte van het inlogmiddel bij een balie (‘face-to-face’) en van de combinatie van iets dat een persoon heeft (inlogmiddel) en iets dat een persoon weet (bijbehorende pincode).

Bron: digid.nl

TVS	DigiD	eHerkenning	eIDAS
10	Basis	eH2	Geen ondersteuning
20	Midden	eH2+	Geen ondersteuning
25	Substantieel	eH3	Geen ondersteuning
30	Hoog	eH4	Hoog

Niveau Basis (10) wordt niet door TVS ondersteund op de productie-omgeving. eIDAS kan alleen gebruikt worden op beveiligingsniveau Hoog.

De dienstverlener kiest zelf het betrouwbaarheidsniveau dat past bij het risicoprofiel van zijn diensten. De dienstverlener kan aangeven wat het minimale betrouwbaarheidsniveau is dat de gebruiker moet gebruiken om in te loggen. Voor het bepalen van het juiste betrouwbaarheidsniveau kunt u gebruik maken van de Regelhulp betrouwbaarheidsniveaus
https://regelhulpenvoorbedrijven.nl/betrouwbaarheidsniveaus/

3.3 Authenticatiediensten (IdP)

TVS biedt ondersteuning voor alle door Wet Digitale Overheid erkende inlogmiddelen. Op dit moment zijn dit de volgende diensten.

DigiD

Met DigiD kunnen gebruikers gebruik maken van de online dienstverlening van overheidsorganisaties.

Meer informatie

DigiD Machtigen

Met DigiD Machtigen kan iemand digitaal zaken regelen namens een andere persoon. Het is mogelijk een persoon te machtigen, maar ook een bedrijf of organisatie.

Meer informatie

eHerkenning

eHerkenning is een gestandaardiseerd inlogsysteem, waarmee organisaties hun diensten veilig online toegankelijk kunnen maken

Meer informatie

eIDAS

eIDAS staat voor 'electronic IDentities And trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Dit kan alleen met een betrouwbare online identiteitscheck aan de voordeur.

Meer informatie

3.5 Eenmalig inloggen (SSO)

Single Sign-On (SSO) is een authenticatieschema waarmee een gebruiker zich met een enkele ID kan aanmelden bij verschillende gerelateerde, maar onafhankelijke softwaresystemen. TVS biedt geen ondersteuning voor eenmalig inloggen (SSO).

3.6 Sessieduur

Na het inloggen houdt de webdienst een sessie van de gebruiker bij. Na maximaal vijftien minuten zonder activiteit, verloopt de sessie en moet de gebruiker zichzelf opnieuw authentiseren.

Bij uitloggen of als alle actieve browserschermen afgesloten worden, vervalt de sessie ook. De afnemer is zelf verantwoordelijk voor het inregelen van deze sessieduur. Dit wordt aangegeven in de Checklist testen.

3.6.1 Time-out

Op elke inlogpagina geldt een time-out duur van 15 minuten. Als de gebruiker binnen deze periode geen actie onderneemt, dan vervalt de sessie en moet de gebruiker een nieuw autorisatieverzoek starten.

Omgeving	**Duur**
TVS Smartlogin	15 minuten
DigiD	15 minuten
eHerkenning	15 minuten
eIDAS	15 minuten

3.7 Veiligheid

TVS houdt het systeem veilig en betrouwbaar. Organisaties die willen aansluiten op TVS moeten altijd gebruik maken van PKIoverheid certificaten voor berichtenuitwisseling. Dit waarborgt de betrouwbaarheid van informatie uitwisseling via websites op basis van Nederlandse wetgeving. PKI staat voor Public Key Infrastructure.

3.8 Inlogmiddelen

Omdat TVS een routeringsdienst is kan het geen inlogmiddelen aanbieden. Voor gebruik en testen van aansluitingen dient de afnemer zelf authenticatiemiddelen te regelen. Dit kan bij de afgenomen authenticatiediensten.

4. Storingen

TVS is onderdeel van een keten om haar diensten aan te kunnen bieden. Hierdoor zijn er een aantal externe afhankelijkheden die invloed hebben op het optimaal functioneren van TVS. Niet elke externe afhankelijkheid heeft invloed op dezelfde functionaliteit van TVS. Onderstaand de externe afhankelijkheden die van invloed (kunnen) zijn op de functionaliteiten van TVS.

Externe afhankelijkheden:

- Logius (DigiD en DigiD Machtigen)
- eHerkenning Makelaar
- eHerkenning Middelen Leveranciers
- eIDAS

4.1 Storingen bij externe afhankelijkheden

In de volgende paragrafen is opgenomen welke functionaliteit niet of beperkt beschikbaar is zodra er een storing is bij een externe afhankelijkheid.

4.1.1 Logius

Een storing bij Logius heeft de volgende invloed op TVS:

- Niet mogelijk om in te loggen op DigiD
- Niet mogelijk om gebruik te maken van DigiD Machtigen
- Mogelijk vertraging in het aansluitproces DigiD en DigiD Machtigen
- Mogelijk vertraging in het wijzigingsproces DigiD en DigiD Machtigen

4.1.2 eHerkenning Makelaar

TVS communiceert met OneWelcome als de primaire makelaar. Bij een storing op de primaire makelaar wordt er automatisch overgeschakeld naar de secundaire makelaar voor de reguliere dienstverlening. De secundaire makelaar van TVS is Digidentity B.V.. Een storing bij de eHerkenning makelaar heeft de volgende invloed op TVS:

- Niet mogelijk om in te loggen op eHerkenning
- Niet mogelijk om in te loggen op eIDAS-verordening
- Mogelijk vertraging in het aansluitproces eHerkenning en eIDAS
- Mogelijk vertraging in het wijzigingsproces eHerkenning en eIDAS

Belangrijk! Bij het gebruik van Scoping in het *AuthnRequest* kan er niet worden overgeschakeld op de secundaire makelaar bij een verstoring bij de primaire eHerkenning makelaar. Meer informatie over Scoping is te vinden in hoofdstuk 7.3 SAML AuthnRequest in Koppelvlak specificatie eID SAML 4.4.

4.1.3 eHerkenning Middelenleveranciers

Een eHerkenning middelenleverancier is een door de overheid goedgekeurde private partij die inlogmiddelen mag leveren voor eHerkenning. Momenteel zijn dit de volgende partijen:

- KPN
- WeID
- Z-Login
- Digidentity
- Reconi
- Quovadis

Een storing bij de eHerkenning-middelenleveranciers heeft de volgende invloed op TVS:

- Niet mogelijk om in te loggen op eHerkenning via één of meerdere middelen leveranciers

TVS schakelt nooit direct met middelenleveranciers. Dit wordt gedaan door de primaire eHerkenning-makelaar.

4.1.4 eIDAS

Een storing bij eIDAS heeft de volgende invloed op TVS:

- Niet mogelijk om in te loggen op eIDAS
- Mogelijk vertraging in het aansluitproces op eIDAS
- Mogelijk vertraging in het wijzigingsproces op eIDAS

4.2 Service en support

TVS biedt service en support aan dienstverleners die een aansluiting hebben. De dienstverlener heeft de mogelijkheid om vragen te stellen over de aansluiting, contact op te nemen bij storingen of wanneer er een klacht is. TVS kan de dienstverlener hiermee verder helpen. De bereikbaarheid van TVS staat beschreven in het Statement of Service (te vinden op https://www.dictu.nl/tvs onder tabblad Documentatie & Links). Dit document beschrijft de dienstverlening die TVS haar klanten biedt. Er wordt in deze functionele beschrijving hier niet verder inhoudelijk op ingegaan.

4.2.1 Blijf op de hoogte

Via de app eFlash communiceert TVS over onderhoudsmomenten en verstoringen. eFlash is beschikbaar in de Apple Appstore (voor IOS) en de Google Playstore (voor Android).

Meer informatie over de eFlash app https://apps.dictu.nl/eflash.