Dienst ICT Uitvoering
Ministerie van Economische Zaken en Klimaat

Certificaatgebruik binnen TVS

Versie: 2.0

Datum: 17-10-2025

Status: Definitief

Inhoud

1. Inleiding

1.1 Doel en doelgroep van dit document

Dit document is opgesteld voor alle organisaties die zijn aangesloten op de ToegangVerleningService (TVS) of een aansluiting overwegen. Het biedt een complete gids voor het beheer van certificaten binnen de TVS-omgeving, van de eerste implementatie tot en met het dagelijks beheer en periodieke vervanging.

Na het doornemen van dit document heeft uw organisatie:

- Een duidelijk begrip van de rol van certificaten binnen TVS
- Kennis van de verschillende certificaattypen en hun toepassingen
- Inzicht in de vereisten en specificaties voor certificaten
- Een handleiding voor het uitvoeren van certificaatwissels zonder dienstonderbreking

Dit document richt zich op verschillende rollen binnen uw organisatie:

- ICT-beheerders die verantwoordelijk zijn voor de technische implementatie
- Informatiebeveiligingsmedewerkers die certificaatbeleid opstellen en monitoren
- Projectleiders die TVS-implementaties aansturen
- Leveranciers die namens organisaties TVS-aansluitingen beheren

1.2 Overzicht van certificaten binnen TVS

Certificaten vormen de basis voor veilige communicatie binnen de TVS-infrastructuur. Ze maken gebruik van Public Key Infrastructure (PKI) om digitale identiteiten te verifiëren en gegevens te beveiligen tijdens uitwisseling tussen verschillende systemen.

In de TVS-omgeving worden certificaten gebruikt voor:

- Authenticatie: Het bewijzen van de identiteit van systemen en organisaties
- Versleuteling: Het beschermen van gevoelige gegevens tijdens transport
- Digitale ondertekening: Het waarborgen van de integriteit en herkomst van berichten
- Mutual TLS: Het opzetten van beveiligde, wederzijds geauthentiseerde verbindingen

De TVS-infrastructuur werkt samen met verschillende authenticatiediensten zoals DigiD, eHerkenning en eIDAS. Elke partij in deze keten heeft specifieke certificaatvereisten die op elkaar afgestemd moeten zijn voor een betrouwbare en veilige werking.

1.3 Relatie met andere TVS-documentatie

Dit document vormt onderdeel van de complete TVS-documentatieset en verwijst naar:

- Koppelvlakspecificatie eID SAML 4.4: Voor technische certificaatvereisten
- Functionele beschrijving MijnTVS: Voor het beheren van certificaten via het selfserviceportaal
- Algemene aansluitvoorwaarden TVS: Voor juridische aspecten van certificaatgebruik

Voor de meest actuele versies van alle documentatie verwijzen we naar:
https://www.dictu.nl/toegangverleningservice/documentatie-en-links

1.4 Vragen of suggesties?

Heeft u na het doornemen van dit document nog vragen over certificaatbeheer op TVS? Neem dan contact op via tvs@dictu.nl. Ons team helpt u graag verder met technische vragen, implementatie-uitdagingen of specifieke certificaatproblemen.

Kleinere wijzigingen aan dit document communiceren we niet breed, dus controleer regelmatig of er een nieuwere versie van dit document beschikbaar is op onze documentatiepagina.

2. Certificaten op TVS - Overzicht

2.1 Wat zijn certificaten?

Certificaten zijn digitale documenten die de identiteit van een organisatie, systeem of dienst verifiëren en cryptografische sleutels bevatten voor beveiligde communicatie. Ze werken volgens het principe van Public Key Infrastructure (PKI), waarbij een vertrouwde derde partij (Certificaat Autoriteit of CA) de echtheid van de digitale identiteit garandeert.

Een certificaat bevat verschillende elementen:

- Publieke sleutel: Voor versleuteling en verificatie van digitale handtekeningen.
- Identiteitsgegevens: Zoals organisatienaam en domeinnaam.
- Geldigheidstermijn: Begin- en einddatum van de geldigheid.
- Digitale handtekening van de CA: Als bewijs van authenticiteit.
- Certificaattype en gebruiksdoel: Welke toepassingen toegestaan zijn.

In de context van digitale overheidscommunicatie spelen certificaten een cruciale rol voor:

- Het waarborgen van vertrouwelijkheid van gevoelige burgergegevens.
- Het garanderen dat berichten afkomstig zijn van de juiste afzender.
- Het voorkomen van man-in-the-middle aanvallen.
- Het voldoen aan wettelijke eisen voor informatiebeveiliging.

2.2 Welke certificaten worden gebruikt op TVS?

Binnen de TVS-infrastructuur worden verschillende typen certificaten gebruikt, elk met een specifiek doel:

Signing-certificaten (Ondertekening)

- Doel: Digitale ondertekening van SAML-berichten en metadata.
- Gebruik: Garandeert de integriteit en herkomst van uitgewisselde berichten.
- Locatie: Opgenomen in SAML metadata van alle partijen.

Encryptie-certificaten (Versleuteling)

- Doel: Versleuteling van gevoelige gegevens in SAML berichten.
- Gebruik: Beschermt burgergegevens zoals BSN en andere persoonsgegevens.
- Locatie: Opgenomen in metadata van dienstverleners.

mTLS-certificaten (Mutual Transport Layer Security)

- Doel: Wederzijdse authenticatie voor beveiligde verbindingen.
- Gebruik: Opzetten van versleutelde kanalen tussen TVS en aangesloten systemen.
- Locatie: Zowel in metadata als in TLS-configuratie.

2.3 Certificaattypen per doelgroep

Voor dienstverleners en clusteraansluitingen:

Directe aansluitingen hebben minimaal de volgende certificaten nodig:

- Signing-certificaat: Voor ondertekening van alle berichten en de metadata.
- Encryptie-certificaat: Voor ontvangst van versleutelde SAML assertions van authenticatiediensten.
- mTLS-certificaat: Voor beveiligde backchannel communicatie met TVS (ArtifactResolve).
- Metadata-integriteit: Signing-certificaat voor ondertekening van de complete metadata.

Clusteraansluitingen (Leveranciers Clusteraansluiting) beheren certificaten voor:

- Eigen infrastructuur: Signing en mTLS certificaten voor communicatie met TVS.
- Aangesloten dienstverleners: Encryptie-certificaten voor elke individuele dienstverlener.
- Metadata-integriteit: Signing-certificaat voor ondertekening van de complete cluster-metadata.

Voor elk van deze functionaliteiten kan de organisatie ervoor kiezen om een uniek certificaat te gebruiken (wat aanbevolen wordt voor extra beveiliging en flexibiliteit bij certificaatwissels), maar het is ook toegestaan om hetzelfde certificaat te gebruiken voor meerdere of zelfs alle bovengenoemde functionaliteiten. Minimaal is dus één certificaat nodig dat voor alle doeleinden wordt gebruikt, maar de voorkeur gaat uit naar specifieke certificaten per functie.

Voor TVS-infrastructuur:

TVS beheert de volgende certificaten:

- IdP signing-certificaten: Voor ondertekening van SAML responses en assertions.
- Metadata signing-certificaten: Voor ondertekening van TVS metadata.
- TLS-certificaten: Voor HTTPS-endpoints van de routeringsvoorziening.

Deze certificaten zijn opgenomen in de TVS metadata en moeten door alle aangesloten partijen worden vertrouwd.

Voor authenticatiediensten:

Authenticatiediensten zoals DigiD, eHerkenning en eIDAS beheren hun eigen certificaten:

- IdP signing-certificaten: Voor ondertekening van AuthNRequests en Assertions.
- Metadata signing-certificaten: Voor ondertekening van hun metadata.

Deze certificaten worden via de keten doorgegeven en zijn zichtbaar in de advice-sectie van SAML-assertions die via TVS worden uitgewisseld. Dienstverleners die op TVS zijn aangesloten maken geen gebruik van deze certificaten. In sommige gevallen wordt echter alleen gebruikgemaakt van de KeyName, waardoor er geen certificaat in de advice aanwezig is.

Certificaat-afhankelijkheden in de keten:

Het is belangrijk te begrijpen dat certificaatwijzigingen impact kunnen hebben op meerdere partijen:

- Wijzigingen aan TVS-certificaten vereisen updates bij alle aangesloten organisaties.
- Wijzigingen aan encryptie-certificaten van dienstverleners moeten worden doorgegeven aan authenticatiediensten.
- Metadata-wijzigingen propageren door de gehele keten en kunnen verwerkingstijd vereisen.

Deze onderlinge afhankelijkheden maken het essentieel om certificaatbeheer zorgvuldig te plannen en tijdig te communiceren met alle betrokken partijen.

3. Certificaatvereisten en -specificaties

3.1 Technische vereisten

PKI-eisen conform SAML eID 4.4

Alle certificaten die worden gebruikt binnen de TVS-infrastructuur moeten voldoen aan de technische vereisten zoals beschreven in hoofdstuk 9 "Technical requirements and recommendations" van de Koppelvlakspecificatie eID SAML 4.4. Deze vereisten waarborgen dat alle communicatie voldoet aan de Nederlandse overheidsstandaarden voor informatiebeveiliging.

Certificaatautoriteit en vertrouwensketen:

- Certificaten moeten uitgegeven zijn door een erkende PKIoverheid Trust Service Provider (TSP).
- Voor zorgorganisaties: UZI-certificaten zijn toegestaan conform het UZI-register.
- De volledige certificaatketen moet geldig en traceerbaar zijn naar een vertrouwde root-CA.

Organisatie-identificatie:

Het certificaat moet correcte identificatiegegevens bevatten:

- Het juiste Organisatie Identificatienummer (OIN) in het Subject.serialNumber veld.
- Voor zorgverleners met een UZI-certificaat: Het abonneenummer moet correct zijn opgenomen.

Certificaatvaliditeit en levenscyclus:

De levenscyclus van certificaten is zorgvuldig gereguleerd om continuïteit te waarborgen:

- Minimale geldigheidsduur: 1 jaar.
- Maximale geldigheidsduur: 3 jaar.
- Vervangingstiming: Minimaal 30 dagen voor expiratie.
- Intrekkingscontrole: CRL of OCSP ondersteuning is verplicht.

Meer informatie over PKIoverheidcertificaten is te vinden op de volgende website:
https://www.logius.nl/onze-dienstverlening/toegang/pkioverheid/wat-een-pkioverheidcertificaat

3.2 Metadata-integratie

Opname in SAML metadata

Certificaten worden op gestandaardiseerde wijze geïntegreerd in SAML metadata. De functie van elk certificaat wordt aangegeven door het "use" attribuut, en elk certificaat bevat zowel een identifier als het volledige X.509 certificaat.

Signing-certificaten:

```
xml<md:KeyDescriptor use="signing">
  <ds:KeyInfo>
    <ds:KeyName>certificaat-identifier</ds:KeyName>
    <ds:X509Data>
      <ds:X509Certificate>BASE64-encoded-certificate</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
```

Encryptie-certificaten:

```
xml<md:KeyDescriptor use="encryption">
  <ds:KeyInfo>
    <ds:KeyName>certificaat-identifier</ds:KeyName>
    <ds:X509Data>
      <ds:X509Certificate>BASE64-encoded-certificate</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
```

mTLS-certificaten:

Deze worden opgenomen als signing-certificaten.

Certificaat-referenties in signatures:

In SAML-berichten kunnen certificaten op twee manieren worden gerefereerd:

- KeyName: Verwijzing naar een identifier (aanbevolen voor prestaties).
- X509Certificate: Volledige certificaat opgenomen in het bericht.

De KeyName-methode heeft de voorkeur omdat deze de berichtgrootte beperkt en de prestaties verbetert.

JWKS voor legacy OAuth-aansluitingen

Voor organisaties met legacy OAuth-implementaties wordt JSON Web Key Set (JWKS) ondersteund:

```
json{
  "keys": [
   {
    "kty": "RSA",
    "use": Gebruik “sig”, of “enc”, of weglaten indien beide hetzelfde certificaat zijn
    "kid": "certificaat-identifier",
    "x5c": ["BASE64-encoded-certificate"],
    "alg": "RS256"
   }
  ]
}
```

Validatie en controles

Bij het opnemen van certificaten voert TVS uitgebreide automatische controles uit:

Technische validatie:

- Certificaatformaat en -structuur volgens X.509 standaard.
- Geldigheidstermijn.
- Cryptografische algoritmes en sleutelsterkte.
- Certificaatketen validatie.
- OIN/KVK/UZI-nummer controle tegen geregistreerde gegevens.

Metadata-integriteit:

Na elke certificaatwijziging wordt de volledige metadata opnieuw ondertekend om integriteit te waarborgen.

Bij validatiefouten worden specifieke foutcodes teruggegeven die helpen bij het identificeren en oplossen van problemen. Een overzicht van veelvoorkomende validatiefouten en hun oplossingen worden behandeld in de functionele beschrijving van MijnTVS.

4. Certificaatwissels op TVS

4.1 Wat is een certificaatwissel?

Een certificaatwissel is het proces waarbij certificaten met een aflopende geldigheid worden vervangen door nieuwe certificaten met een geldigheid van minimaal één jaar. Dit proces is essentieel voor het onderhouden van een veilige en betrouwbare TVS-aansluiting.

Verlopen certificaten zorgen voor onbeschikbaarheid van uw dienst omdat de cryptografische validatie faalt. Wanneer een certificaat verloopt, kunnen systemen de digitale handtekeningen niet meer verifiëren en wordt versleutelde communicatie onmogelijk. Om dienstonderbreking te voorkomen moet een certificaat tijdig worden vervangen.

Redenen voor certificaatvervanging:

- Natuurlijke expiratie: Certificaten hebben een beperkte geldigheidsduur (meestal 1-3 jaar).
- Beveiligingsincidenten: Compromittering van private keys vereist onmiddellijke vervanging.
- Organisatiewijzigingen: Naamswijzigingen of herstructureringen maken nieuwe certificaten noodzakelijk.
- Cryptografische updates: Overgang naar sterkere algoritmes of langere sleutellengtes.
- Compliance-vereisten: Wijzigingen in regelgeving of standaarden.

Gelukkig zijn er mechanismes beschikbaar die eventuele dienstonderbrekingen tijdens een certificaatwissel kunnen voorkomen, met name het certificate-rollover-principe.

4.2 Certificate-rollover principe

Een certificate-rollover is een proces waarmee certificaatwissels zonder dienstonderbreking kunnen worden uitgevoerd. Het principe voorkomt dat alle partijen in de keten op exact hetzelfde moment moeten overschakelen naar nieuwe certificaten door tijdelijk meerdere geldige certificaten toe te staan.

Hoe certificate-rollover werkt:

Bij een rollover-proces is er een overlappingsperiode waarin zowel het oude als het nieuwe certificaat geldig zijn en geaccepteerd worden door alle partijen. Dit stelt organisaties in staat om op hun eigen tempo over te schakelen zonder dat dit leidt tot dienstonderbreking of gecoördineerde "big bang" overgangen.

Typische rollover-timeline:

- Voorbereiding: Nieuwe certificaten worden aangevraagd en getest.
- Rollover-start: Nieuwe certificaten worden toegevoegd aan metadata (naast bestaande).
- Overlappingsperiode: Beide certificaten zijn geldig en worden geaccepteerd.
- Geleidelijke overgang: Partijen schakelen over naar nieuwe certificaten.
- Cleanup: Oude certificaten worden verwijderd na volledige overgang.

Voordelen van certificate-rollover:

- Geen gecoördineerde wisselmomenten: Partijen hoeven niet synchroon te handelen.
- Flexibele planning: Certificaatwissels hoeven niet tijdens reguliere onderhoudsvensters uitgevoerd worden.
- Risicoreductie: Minder kans op operationele problemen door haast of tijdsdruk.
- Betere testmogelijkheden: Nieuwe certificaten kunnen worden getest voordat oude certificaten verlopen.
- Bij problemen kan snel worden teruggevallen op het oude certificaat.

Ondersteuning in de TVS-keten:

Certificate-rollover wordt volledig ondersteund door alle belangrijke ketenpartners:

- TVS: Ondersteunt meerdere geldige certificaten gedurende rollover-perioden.
- Logius (voor DigiD en DigiD Machtigen): Accepteert zowel oude als nieuwe certificaten tijdens overgang.
- eTD-stelsel (voor eHerkenning en eIDAS): Volledig rollover-compatibel.

Vereisten voor uw implementatie:

Het is cruciaal dat uw aansluiting ook certificate-rollover ondersteunt. Uw systeem moet kunnen omgaan met:

- Meerdere geldige certificaten in metadata van TVS.
- Dubbele encrypted responses op basis van zowel oude als nieuwe encryptie-certificaten.
- Flexibele certificate stores die dynamisch kunnen worden bijgewerkt.

⚠	**Waarschuwing**: TVS verwacht dat alle aangesloten organisaties ondersteuning bieden voor certificate-rollovers. Het niet ondersteunen van deze functionaliteit kan grote impact hebben op de beschikbaarheid van uw diensten tijdens certificaatwissels.

4.3 TVS certificaatwisselmomenten

TVS beheert verschillende metadata-bestanden die elk jaar onderhevig zijn aan geplande certificaatwisselmomenten. Deze wissels zijn essentieel voor het onderhouden van de beveiligingsintegriteit van de gehele TVS-infrastructuur.

TVS metadata-endpoints per omgeving:

- Preproductie
  - https://pp2.toegang.overheid.nl/kvs/rd/metadata
- Productie
  - https://rd2.toegang.overheid.nl/kvs/rd/metadata

Communicatie over certificaatwissels

Het TVS-beheerteam informeert aangesloten organisaties tijdig over aankomende certificaatwisselmomenten via meerdere kanalen:

- E-mail notificaties: Directe communicatie naar geregistreerde contactpersonen
- eFlash berichten: Officiële communicatie via het eFlash-systeem van de rijksoverheid

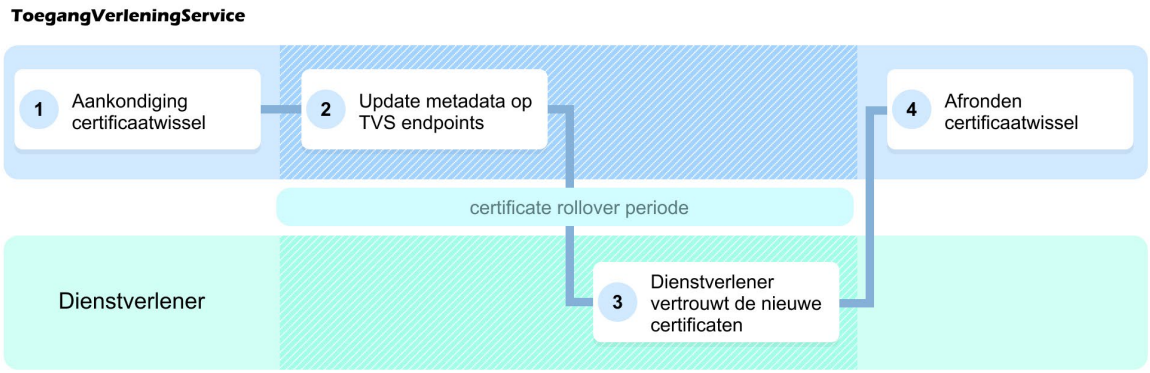
In deze communicatie wordt het exacte moment van de certificaatwissel aangegeven, samen met gedetailleerde instructies voor de benodigde acties van aangesloten organisaties. Doorgaans wordt deze communicatie 14 dagen voor de geplande wissel verstuurd.

Certificate-rollover-proces bij TVS

TVS hanteert een zorgvuldig uitgewerkt rollover-proces om dienstonderbreking bij aangesloten organisaties te voorkomen:

Tijdlijn van het TVS rollover-proces:

- 14 dagen voor expiratie: Nieuwe certificaten worden toegevoegd aan de metadata.
- Rollover-periode: Beide certificaten (oud en nieuw) zijn beschikbaar.
- TVS schakelt op het gecommuniceerde moment over op het nieuwe certificaat. Vanaf dat moment is het oude certificaat niet meer in gebruik.
- Expiratie oude certificaat: Automatische verwijdering van verlopen certificaten uit metadata.
- Cleanup: Metadata wordt opgeschoond en opnieuw ondertekend.



Tijdens de rollover-periode bevat de TVS-metadata zowel de huidige als de nieuwe certificaten. Dit geeft aangesloten organisaties de tijd om hun systemen bij te werken en de nieuwe certificaten te vertrouwen zonder dat dit leidt tot dienstonderbreking.

Acties voor aangesloten organisaties

Als uw software compatible is met certificate-rollover, zijn de vereiste acties minimaal:

- Automatische verwerking: Laat uw systeem de TVS-metadata regelmatig inlezen (aanbevolen: dagelijks).
- Certificaatvertrouwen: Zorg dat nieuwe certificaten automatisch worden vertrouwd.
- Monitoring: Controleer dat de overgang succesvol verloopt via uw monitoringsystemen.

Alternatieve endpoints voor legacy-systemen

Voor organisaties waarvan de software niet overweg kan met meerdere certificaten in metadata, biedt TVS specifieke endpoints die slechts één certificaat per keer tonen:

Preproductie-omgeving:

- Huidig certificaat: https://pp2.toegang.overheid.nl/kvs/rd/metadata?certs=active
- Nieuw certificaat: https://pp2.toegang.overheid.nl/kvs/rd/metadata?certs=future

Productie-omgeving:

- Huidig certificaat: https://rd2.toegang.overheid.nl/kvs/rd/metadata?certs=active
- Nieuw certificaat: https://rd2.toegang.overheid.nl/kvs/rd/metadata?certs=future

Belangrijke opmerkingen over alternatieve endpoints:

- De "future" URL is alleen beschikbaar wanneer er een rollover-certificaat beschikbaar is.
- Gebruik deze endpoints alleen als uw systeem niet compatible is met standaard certificate - rollover.
- Plan om uw systemen te upgraden naar rollover-ondersteuning voor toekomstige flexibiliteit.

4.4 Klant certificaatwisselmomenten

Naast de certificaten die door TVS worden beheerd, zijn aangesloten organisaties verantwoordelijk voor het onderhouden van hun eigen certificaten. Deze certificaten zijn opgenomen in de metadata van de organisatie en vereisen periodieke vervanging volgens dezelfde principes als TVS-certificaten.

Voor een succesvolle certificate-rollover moet de organisatie zowel het huidige als het nieuwe certificaat opnemen in de metadata tijdens de overlappingsperiode. Dit geeft alle partijen in de keten de tijd om het nieuwe certificaat te vertrouwen, terwijl het oude certificaat nog steeds functioneel blijft. Na een succesvolle overgang en wanneer zeker is dat alle partijen het nieuwe certificaat accepteren, kan het oude certificaat worden verwijderd uit de metadata.

Timing en verwerkingstijd

Om dienstonderbreking te voorkomen is het essentieel dat certificaatwissels tijdig worden doorgegeven aan TVS en de authenticatiediensten. Verschillende certificaattypes hebben verschillende verwerkingstijden vanwege de complexiteit van de keten.

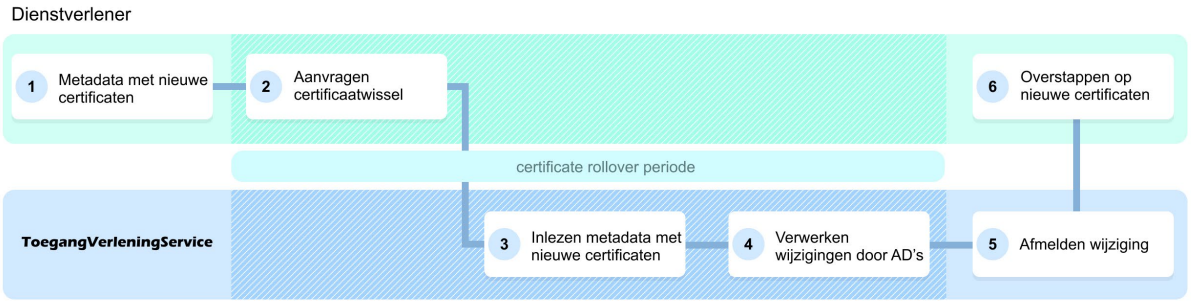
Verwerkingstijden per certificaattype:

- Signing en mTLS: Directe verwerking door TVS.
- Encryptie: Aanvullende verwerkingstijd door authenticatiediensten (binnen 5 werkdagen).

Begin het wisselproces minimaal 30 dagen voor expiratie van uw huidige certificaten. Dit geeft voldoende tijd voor alle verwerkingsstappen, testen en eventuele probleemoplossing.

Best practices voor organisatie-certificaatwissels:

- Stapsgewijze rollout: Implementeer certificaatwissels gefaseerd per omgeving.
- Monitoring intensiveren: Verhoog monitoring-frequentie tijdens en na certificaatwissels.
- Rollback-plan: Houd procedures gereed om terug te vallen op oude certificaten indien nodig.



4.5 Proces en procedures

4.5.1 Aanvraag via MijnTVS

Voor organisaties die gebruik maken van het MijnTVS-portaal is het certificaatwisselproces geïntegreerd in de selfservice-functionaliteit. Dit biedt de meest gestroomlijnde en gebruiksvriendelijke manier om certificaatwissels door te voeren.

Het MijnTVS-systeem waarschuwt direct voor mogelijke problemen zoals ongeldige certificaten, onjuiste OIN-nummers of metadata-formatering-fouten. Meer informatie over certificaatwissels via MijnTVS is te vinden in de handleiding en functionele beschrijving van MijnTVS.

4.5.2 Aanvraag via wijzigingsformulier

Voor organisaties die geen toegang hebben tot MijnTVS, blijft het online wijzigingsformulier beschikbaar als alternatieve route.

Proces via wijzigingsformulier:

- **Metadata voorbereiden:** Update uw metadata-bestand met nieuwe certificaten en test lokaal.
- **Formulier invullen:** Ga naar https://dictu.nl/tvs-wijzigingsformulier.
- **Upload of URL:** Verstrek metadata via directe upload of verwijzing naar uw metadata-URL.
- **Contactgegevens:** Verstrek actuele contactgegevens voor communicatie over de wijziging.
- **Aanvraag indienen:** Dien het complete formulier in met alle vereiste informatie.
- **Bevestiging:** Ontvang bevestiging van ontvangst binnen 1 werkdag.

4.5.3 Verwerkingstijden en communicatie

TVS hanteert duidelijke verwerkingstijden voor certificaatwissels om organisaties in staat te stellen hun planning te maken. Deze tijden zijn gebaseerd op de complexiteit van validatie en distributie door de keten.

Standaard verwerkingstijden:

- Ontvangstbevestiging: Binnen 1 werkdag na ontvangst.
- TVS-verwerking: Binnen 2 werkdagen na succesvolle validatie.
- Authenticatiedienst-verwerking: binnen 5 werkdagen (afhankelijk van specifieke dienst).

Totale doorlooptijd: maximaal 7 werkdagen.

⚠	Let op: Deze verwerkingstijden zijn indicatief. Externe factoren zoals drukte, onderbezetting bij ketenpartners, storingen of geplande onderhoudswerkzaamheden kunnen de doorlooptijd verlengen. Belangrijke afwijkingen worden gecommuniceerd via eFlash (zie document "TVS Keten Communicatiekanalen").

Aanbeveling: Plan certificaatwissels minimaal 30 dagen voor de verloopdatum van uw huidige certificaat in. Dit biedt voldoende marge voor eventuele validatieproblemen, herstelprocedures of vertragingen in de keten. *Communicatie tijdens verwerking:*

- Ontvangstbevestiging: Bevestiging van aanvraag met referentienummer.
- Validatie-resultaten: Directe melding van eventuele validatieproblemen.
- Voltooiingsmelding: Bevestiging wanneer wissel volledig is doorgevoerd.

⚠	Let op: Het is niet mogelijk om certificaatwisselmomenten in te plannen voor specifieke tijdstippen. Alle certificaatwissels worden verwerkt volgens het "first-come, first-served" principe binnen de standaard verwerkingstijden.

Organisaties moeten hun eigen planning aanpassen aan deze werkwijze en tijdig certificaatwissels indienen om de gewenste timing te bereiken. Het wordt sterk aanbevolen om certificaatwissels in te dienen zodra nieuwe certificaten beschikbaar zijn, zelfs als de oude certificaten nog maanden geldig zijn.

5. Bronnen en Ondersteuning

De beschreven certificaatbeheerprocessen vormen de basis voor een veilige, betrouwbare en continue TVS-dienstverlening. Het zorgvuldig onderhouden van certificaten is cruciaal voor het waarborgen van de integriteit, vertrouwelijkheid en beschikbaarheid van de dienstverlening aan burgers en organisaties.

Door gebruik te maken van het certificate-rollover principe kunnen organisaties certificaatwissels uitvoeren zonder dienstonderbreking, wat essentieel is voor diensten die 24/7 beschikbaar moeten zijn. De TVS-infrastructuur en alle ketenpartners ondersteunen deze methodiek volledig.

De certificaten binnen de TVS-omgeving zijn onderhevig aan veranderingen in de PKIoverheid-infrastructuur. Om uw certificaatbeheer toekomstbestendig te maken, is het belangrijk op de hoogte te blijven van de laatste ontwikkelingen.

Voor aanvullende informatie over certificaten in relatie tot TVS:

- Logius PKIoverheid-certificaten - Algemene informatie over PKIoverheid
- Transitie naar G4 - Details over de nieuwe generatie certificaten
- Certificaataanvraag - Praktische aanvraaghulp

Door een proactieve benadering van deze certificaattransitie te hanteren en de certificate-rollover-principes uit eerdere hoofdstukken toe te passen, kunt u de continuïteit van uw dienstverlening tijdens deze belangrijke technologische vernieuwing waarborgen.

5.1 Contact en ondersteuning

Voor vragen over certificaatbeheer op TVS kunt u contact opnemen via tvs@dictu.nl.

Door de richtlijnen in dit document te volgen en gebruik te maken van de beschikbare ondersteuning, kunt u zorgen voor een veilige en stabiele TVS-aansluiting met minimale impact op uw dienstverlening tijdens certificaatwissels.