Dienst ICT Uitvoering
Ministerie van Economische Zaken en Klimaat

Handleiding certificaatwissels op TVS

Versie: 1.2

Datum: 24-04-2024

Status: Definitief

Auteur: Fatih Yilmaz

Inhoud

1 Inleiding

Dit document is opgesteld voor alle aangesloten organisaties op ToegangVerleningService (TVS) die meer informatie willen over het certificaatwisselproces. Na het doornemen van dit document zal uw organisatie een duidelijker beeld hebben van hoe certificaatwisselingen plaatsvinden op TVS en hoe deze kunnen worden uitgevoerd met behulp van certificate rollover zonder dat er sprake is van dienstonderbreking.

Vragen of suggesties?

Heeft u na het doornemen van dit document nog vragen? Neem dan contact op via tvs@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.

2. Certificaatwissels op TVS

2.1 Wat is een certificaatwissel?

Onder een certificaatwissel verstaan wij een proces waarbij certificaten met een aflopende geldigheid worden vervangen door certificaten met een geldigheid van minimaal één jaar.

Verlopen certificaten zullen voor onbeschikbaarheid van uw dienst zorgen. Om dit te voorkomen moet een certificaat op tijd verwisseld worden. Er zijn mechanismes beschikbaar die eventuele dienstonderbrekingen tijdens een certificaatwissel voorkomen.

Technische specificaties van de gebruikte certificaten en algoritmes zijn te vinden in hoofdstuk 9 *Technical requirements and recommendations* van de Koppelvlakspecificatie eID SAML 4.4.

2.2 Wat is een certificate rollover?

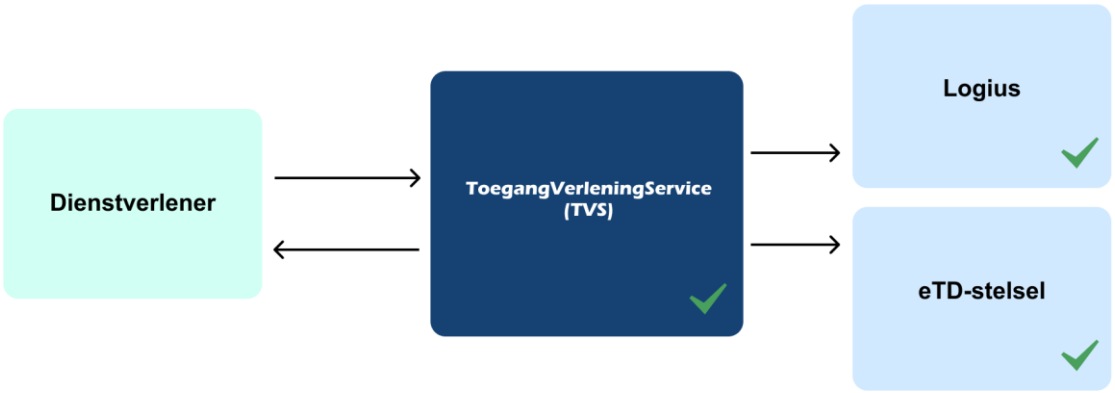
Een certificate rollover is een proces waarmee certificaatwissels zonder dienstonderbreking uitgevoerd kunnen worden. Bij een certificate rollover is het de bedoeling om een "gesynchroniseerde" wissel van certificaten bij TVS, authenticatiediensten en aangesloten organisaties te voorkomen. Dit is mogelijk als men meer dan één geldig certificaat toestaat gedurende een bepaalde periode van de certificaatwissel. Als beide partijen dit principe ondersteunen, hoeven ze niet op exact hetzelfde moment een wissel van certificaat te doen.

Binnen de gehele keten wordt certificate rollover ondersteund door de volgende ketenpartners:

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

Het is belangrijk dat uw aansluiting ook certificate rollover ondersteund. Door het ondersteunen van certificate rollover functionaliteit is het mogelijk om:

- zonder dienstonderbreking certificaatwissels uit te voeren
- certificaatwissels te doen zonder dit in te hoeven plannen met TVS en achterliggende authenticatiediensten



Figuur 1: Certificate rollover ondersteuning binnen de keten.

Bij een certificate rollover dient u ook om te kunnen gaan met dubbele encrypted response op basis van beide encryptiecertificaten.

Let op! Bij TVS verwachten we dat alle aangesloten organisaties ondersteuning bieden voor certificate rollovers. Het niet ondersteunen van deze functionaliteit kan grote impact hebben op de beschikbaarheid van uw dienst(en) tijdens deze momenten.

DICTU behoudt het recht om aansluitingen te weigeren als de rollover-functionaliteit voor certificaten ontbreekt.

2.3 Welke certificaatwisselmomenten zijn er op TVS?

Op TVS kennen we de volgende metadata-bestanden waar ieder jaar een certificaatwisselmoment op plaatsvindt.

TVS Metadata	Endpoint	Omgeving
Bevat het Preproductie signing-certificaat	https://pp2.toegang.overheid.nl/kvs/rd/metadata	Preproductie
Bevat het Productie signing-certificaat	https://rd2.toegang.overheid.nl/kvs/rd/metadata	Productie

De certificaten van TVS worden vervangen door nieuwe certificaten met een geldigheid van minimaal 1 jaar. Het is de bedoeling dat u deze certificaten op tijd vertrouwt om dienstonderbreking te voorkomen. Het functioneel beheer team zal u tijdig over deze certificaatwisselmomenten informeren. Tijdens dit communicatiemoment wordt u via de mail en via eFlash gevraagd om tijdig de nieuwe certificaten te vertrouwen. Ook wordt het exacte moment van de certificaatwissels in de communicatie aangegeven.

De metadata van TVS wordt 14 aantal dagen voordat de certificaten verlopen uitgebreid met nieuwe certificaten. Dit betekent dat er een periode is waarbij in de metadata zowel de huidige als de nieuwe certificaten zijn opgenomen.

Let op! De nieuwe certificaten zijn dan nog niet in gebruik maar kunnen alvast vertrouwd worden voor een overgang zonder dienstonderbreking op de nieuwe certificaten.

Figuur 2: Visualisering van het certificaatwisselproces.

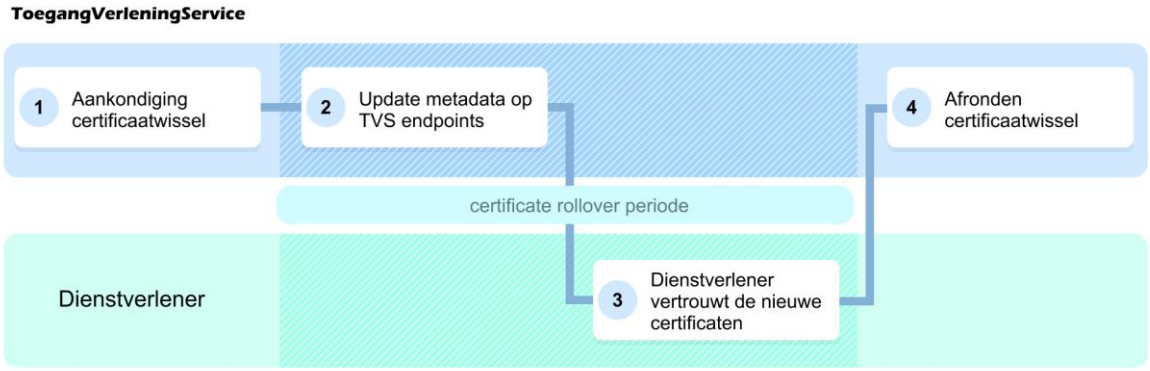
Als uw software om kan gaan met twee certificaten in de metadata, dan hoeft u geen verdere actie te ondernemen dan de metadata tijdig inlezen en de nieuwe certificaten vertrouwen. Zodra de oude certificaten verlopen zijn, zullen ze uit de metadata worden verwijderd.

Indien uw software niet om kan gaan met twee certificaten in de metadata, dan kunt u de volgende parameters toevoegen aan onze endpoints:

- Preproductie huidige certificaat:
  - https://pp2.toegang.overheid.nl/kvs/rd/metadata?certs=active
- Preproductie nieuwe certificaat:
  - https://pp2.toegang.overheid.nl/kvs/rd/metadata?certs=future
- Productie huidige certificaat:
  - https://rd2.toegang.overheid.nl/kvs/rd/metadata?certs=active
- Productie nieuwe certificaat:
  - https://rd2.toegang.overheid.nl/kvs/rd/metadata?certs=future

Via de ***active*** URL kunt u de metadata ophalen met enkel het huidige certificaat. Met de ***future*** URL haalt u het certificaat binnen dat het huidige certificaat zal vervangen. De ***future*** URL is alleen beschikbaar als er een rollover certificaat beschikbaar is.

2.3.1 Samengevat



2.4 Welke Certificaatwisselmomenten zijn er voor dienstverleners en leveranciers?

Naast de certificaten die door TVS worden vernieuwd, zijn er ook certificaten die door aangesloten dienstverleners moeten worden vernieuwd. Deze certificaten zijn opgenomen in de metadata van de aangesloten leverancier/dienstverlener.

2.4.1 Type certificaten

Type	Uitleg	Bron	Toepassing
mTLS	Mutual TLS, of kortweg mTLS, is een methode voor wederzijdse authenticatie.	Metadata leverancier/dienstverlener	TVS
Encryptie	Wordt gebruikt voor de versleuteling van berichten	Metadata leverancier/dienstverlener	Authenticatiediensten (DigiD, eHerkenning, eIDAS)
Signing	Wordt gebruikt voor het digitaal ondertekenen van berichten	Metadata leverancier/dienstverlener	TVS

Om dienstonderbreking aan uw aansluiting te voorkomen dient u certificaatwissels tijdig aan TVS door te geven. De nieuwe certificaten neemt u op in uw SAML metadata (of in het JWKS voor legacy OAuth-aansluitingen). De encryptiecertificaten moeten ook door authenticatiediensten verwerkt worden. Hier is extra verwerkingstijd voor nodig.

2.4.2 Aanvragen certificaatwissel

Voor het doorgeven van wijzigingen kunt u gebruik maken van het online TVS wijzigingsformulier, te bereiken via https://dictu.nl/tvs-wijzigingsformulier

Ga hiervoor als volgt te werk:

- Update uw metadata met de nieuwe certificaten
- Ga naar https://dictu.nl/tvs-wijzigingsformulier en dien een aanvraag in voor een certificaatwissel
- Upload of geef de URL op van uw metadata

Uw aanvraag wordt binnen 2 werkdagen in behandeling genomen.

Let op! Indien uw software geen ondersteuning heeft voor certificate rollover functionaliteit is er een grote kans dat er dienstonderbreking zal ontstaan op uw aansluiting bij het wisselen van certificaten.

Let op! Vanaf 01-05-2024 is het niet meer mogelijk om een certificaatwisselmoment in te plannen.

2.4.3 Samengevat