

Te hanteren PKloverheid-certificaten op test-omgevingen van Edukoppeling API's

We lopen bij Eduarte tegen een issue aan wat we graag onder de aandacht van de Edukoppeling-werkgroep willen brengen.

Edukoppeling op test-omgevingen

Voor ons als SIS-leverancier is een belangrijk voordeel van Edukoppeling-gebaseerde API's de consistentie tussen die API's. Zo gelden bijvoorbeeld dezelfde eisen en 'spelregels' rondom het gebruik van PKloverheid-certificaten, omdat die worden voorgeschreven door Edukoppeling (en/of Digikoppeling). Het afgelopen jaar merken we dat er wat ruis en inconsistentie ontstaat in de keten(s) rondom de certificaten die gebruikt dienen te worden op test-omgevingen. Dit levert zowel technisch als in de afstemming met andere partijen frictie op, waarvan wij hopen dat die weg te nemen is door uitspraken of 'regels' vanuit de Edukoppeling-werkgroep.

Oude test-certificaten

Tot een jaar geleden was de consensus die wij in de praktijk zagen dat je op een test-omgeving gebruik maakt van een certificaat dat afstamt van '*Staat der Nederlanden Private Root CA - G1*'. Dit is dus de gewone, reguliere root waar ook de productie-certificaten van afstammen. Om te zorgen dat je niet met het test-certificaat een productie-omgeving kunt benaderen (en andersom) gebruikte je als organisatie niet je echte OIN, maar een test-OIN. In geval van Eduarte is ons echte OIN 00000003743434240000 en was ons test-OIN 00000099743434240000, conform [deze OIN-systematiek](#).

Nieuwe test-certificaten

Ongeveer een jaar geleden ontvingen alle softwareleveranciers die met test-omgevingen van DUO koppelen het bericht dat er overgestapt zou moeten worden op het gebruik van certificaten die afstammen van de '*TRIAL PKloverheid Root CA - G3*' root. Omdat Digikoppeling dat eigenlijk al jaren scheen voor te schrijven, onder punt 3 van [deze eisen](#). Bij die Trial-certificaten wordt gebruik gemaakt van het reguliere OIN, in plaats van het test-OIN. Dus DUO hanteert als OIN 00000001800866472000 en Eduarte 00000003743434240000.

Ingebruikname en inconsistentie in de keten

Afgelopen zomer heeft Eduarte het nieuw aangeschafte certificaat succesvol in gebruik genomen in diverse koppelingen, zoals die met de test-omgevingen van RIO, ROD, Verzuim en Centraal Aanmelden MBO. Er zijn echter ook een aantal koppelingen waarbij we tegen problemen aan lopen in het gebruik van dit nieuwe certificaat. Voorbeelden daarvan zijn:

- SBB's BPV-API, zij accepteren geen certificaten die afstammen van de Trial-root
- Facet, zij lijken er niet mee overweg te kunnen dat een leverancier een certificaat met hetzelfde OIN hanteert op de test- en productie-omgeving

Op dit moment gebruiken we voor deze 2 koppelingen (op onze test-omgeving) nog ons oude test-certificaat, omdat dit certificaat nog enkele maanden geldig is. Dat is voor nu dus nog even werkbaar, maar we willen natuurlijk voorkomen dat we in de toekomst 2 verschillende test-certificaten moeten kopen en onderhouden, terwijl de betrokken API's allemaal Edukoppeling-gebaseerd zijn.

Wel of geen intermediates meeleveren

Daarnaast zien we ook vaak inconsistentie in de ondersteuning van het meeleveren van de intermediate-certificaten. De ene partij vereist juist dat we deze meeleveren en de ander kan er niet mee overweg wanneer we dat doen. Dit zorgt er dus ook voor dat we op dit vlak verschillende configuraties en 'certificaatbundels' moeten hanteren voor API's die beiden op Edukoppeling-gebaseerd zijn. Dit geldt overigens niet alleen op test-omgevingen, maar ook voor productie-omgevingen.

We zijn benieuwd hoe de werkgroep tegen deze kwesties aan kijkt en wat zij hierin kan betekenen. Mocht er verdere toelichting nodig zijn dan geven we die uiteraard graag.

Mede namens mijn collega's (zie cc),

Met vriendelijke groet,

Luke Niesink

Kees.van.Ginkel

Tom Kirchjunger

Met opmerkingen [RR1]: Ben hier ook benieuwd naar. Vooral hoe hier richting Facet mee om te gaan. Zelf hebben we de pragmatische keuze gemaakt om voor BPV-API in alle tst/acc en prd situaties de BPV-API productie omgeving te gebruiken vanwege data inconsistenties op hun TST en ACC omgevingen.

Communicatie tussen DUO en PKI-overheid:

DUO ervaart hetzelfde probleem en heeft vorig jaar bij Logius twee vragen hierover gesteld. Het antwoord dateert van 23-1-2026:

1. *Trial certificaten voor test lijkt DUO wenselijk, maar sommige ketenpartners lijken daar anders over te denken. Wat is het nu?*

Er zit een verschil tussen wat de Digikoppeling standaard aanbeveelt en wat het Programme of Requirements TRIAL PKI-overheid zegt:

- Digikoppeling:

Digikoppeling: Gebruik en Afschermend Certificaten 1.6.3

Bij het testen van applicaties is het van belang om certificaten te gebruiken waarvan de structuur overeenkomt met die van een PKI-overheid certificaat¹⁾. PKI-overheid kent een TEST hiërarchie voor dit doeleinde. Logius biedt daaraan zelf signed testcertificaten om haar voorstellingen te kunnen testen.

¹⁾ Een belangrijk kenmerk van PKI-overheid certificaten is behalve het ODN voor Digikoppeling dat deze een verlegstructuur hebben (persooncertificaat, domein, TSP en dienstcertificaat). Niet alle software kan standaard goed omgaan met een verlegstructuur. Het is daarom belangrijk dat dit goed getest wordt. Het is naar te verwachten om (kleinere) systemen uit te rusten met certificaten die zijn gegenereerd op basis van het overheid stamcertificaat, voor testen moet een testcertificaat gebruikt worden.

Digikoppeling: Bestanden en versies van versie 1.4.1

1. Certificaten voor productie wijken af van certificaten voor test doordat zij op verschillende 'soorten' zijn gebaseerd, respectievelijk 'Staat der Nederlandse Rand Private Root' en 'PKI TRIAL root'.

Een TRIAL certificaat kan worden uitgegeven door een TSP met prefix 99 zonder ODN registratie van het "testnummer", op basis van het hoofdnummer van een organisatie (conform het DGN40N van een organisatie).

ODN Status 2.1.1: Profiel tabel

ODN Status 2.1.1: Voorbereid ODN structuur

- PKI-overheid:

1.4.1-tpkio33

Description

Certificates issued within the PKI-overheid TRIAL hierarchy SHALL only be used for testing purposes.

Testing purposes for Personal certificates and Services certificates are as follows (please not that this is also not an exhaustive list):

- Usage of subscriber Personal/Services certificates by the TSP for own (internal) testing
- Usage of subscriber Personal/Services certificates to test a non-production application to test the process of implementing PKI-overheid personal/services certificates in workflows etc.

Comment: In case of doubt if an use case is deemed to be for "testing purposes" a TSP SHALL contact the PA to seek permission for issuance of PKI-overheid TRIAL certificates.

Reactie Logius:

Het standpunt vanuit PKI-overheid is met de overgang naar de 4e generatie

PKI-overheid certificaten (G4, meer informatie op

[https://www.logius.nl/actueel/wees-voorbereid-de-nieuwe-generatie-](https://www.logius.nl/actueel/wees-voorbereid-de-nieuwe-generatie-pkioverheidcertificaten-komen-era...)

[pkioverheidcertificaten-komen-era...](https://www.logius.nl/actueel/wees-voorbereid-de-nieuwe-generatie-pkioverheidcertificaten-komen-era...)) doorgetrokken. Dit betekent dat er voor G4

geen sprake meer is van een aparte TRIAL-hiërarchie waaronder TSP's TRIAL-

certificaten uitgeven aan eindgebruikers maar dat Logius via GitHub (zie

<https://github.com/pkioverheid/g4-trial>) scripting beschikbaar stelt waarmee

organisaties en eindgebruikers zelf certificaten kunnen genereren. Dit betekent

echter wel dat elke gebruiker in principe een eigen hiërarchie aanmaakt wat

ketentesten lastig maakt tenzij een partij binnen zijn eigen veld de

verantwoordelijkheid neemt om deze testcertificaten uit te geven. Tegelijkertijd

snapt Logius ook wel de pijn die wordt beschreven

☒ *Actiepunt Logius: Kijken of we hier toch nog iets kunnen faciliteren, bijvoorbeeld via het Logius aansluitteam en/of een portal.*

Actiepunt hieraan gerelateerd: De collega's van PKloverheid en Digikoppeling gaan kijken of we deze conflicterende eisen wat meer met elkaar in lijn kunnen brengen zodat er minder verwarring bestaat in het veld

2. Iets dergelijk geldt ook voor test-oins (prefix 99). Is het überhaupt nog zinvol als je trials hebt?

Reactie Logius:

Tot een tijdje geleden stond KPN (de enige uitgever van PKloverheid TRIAL momenteel) het toe om een test-OIN (met prefix 99) in productiecertificaten op te nemen. De prefix wordt voor een normaal OIN/HRN geplakt. Dat kan nu echter niet meer, vandaar de overstap naar PKloverheid TRIAL. Samen met het gebruik van TRIAL is het gebruik van een test-prefix een middel om de schade bij misconfiguraties (waarbij per ongeluk testomgevingen aan productieomgevingen worden gekoppeld) te beperken. De consensus tijdens de sessie is dat het gebruik van een productie-OIN niet noodzakelijk slecht is in testsituaties omdat dit zoveel mogelijk de productiesituatie benadert, mits er gebruik gemaakt wordt van niet-productiecertificaten.