Ministerie van Volksgezondheid,
Welzijn en Sport

**Secretaris Generaal / plv. Secretaris Generaal**
Directie Informatiebeleid / CIO
Cluster iBeleid team A

**Bezoekadres:**
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34

www.rijksoverheid.nl

**Inlichtingen bij**
O. Koeroo
*CISO concern VWS*

Oa.koeroo@minvws.nl

**Datum**
13 oktober 2021

**Aantal pagina's**
4

# memo

Beleid discontinueren uitgifte PKIO publieke server certificaten

Beste collega,

Logius stopt met de uitgifte van publiek vertrouwde PKIOverheid (PKIO) webserver certificaten. Op 8 december 2022 verloopt namelijk het stamcertificaat 'Staat der Nederlanden EV Root CA'. Doordat ook tussenliggende certificaten verlopen zal in theorie het laatste certificaat kunnen worden uitgegeven tot 4 december 2022. Naar verwachting houdt de uitgifte ruim voor die tijd op. Het is nog onbekend wanneer, omdat dit nog niet bepaald is door Logius en de Trust Service Providers (TSPs). Deze certificaat typen worden voor een jaar uitgegeven. Dat betekent dus voor partijen die na 4 december 2021 een certificaat ontvangen dat dit het laatste certificaat is dat ze krijgen en dat deze een einddatum heeft van 4 december 2022. Voor de zorgsector heeft dit zeer grote gevolgen.

Zonder tijdige oplossing vervallen de publieke PKIO-servercertificaten met als gevolg dat diverse zorgsystemen niet meer met elkaar kunnen communiceren. Voor de beeldvorming, dit betekent dat er diverse data uitwisselingen tussen systemen en contacten tussen patiënt en zorgverlener niet meer digitaal kunnen worden uitgevoerd. De eerste analyse gaat er vanuit dat zorg(informatie)systemen en stelsels zoals onder andere MedMij, Koppeltaal en DigiD hier in scope zijn. Mogelijk moeten aanbieders van software in de zorg ook hun oplossingen hierop aanpassen. Daarnaast heeft software binnen de zorgsector een update cyclus van eens per kwartaal of eens per half jaar. Dit in combinatie met het feit dat partijen na 4 december 2021 al het laatste certificaat ontvangen, met vaste einddatum 4 december 2022, maakt dat VWS gekozen heeft om met een eigen beleidslijn te komen en niet te wachten op interdepartementale afstemming.

*Tijdslijn*
Doordat het dossier nog sterk ontwikkelt, kan alleen een grove tijdslijn worden vastgesteld. De stappen die nodig zijn om dit met minimale impact op te lossen zijn wel vrij helder. Wanneer de tijdslijnen continue blijven veranderen in de beoogde oplossingen zal dit voor de zorgsector tot een significante impact kunnen leiden voor zorgverleners en –behoevenden.

1. *2 augustus 2021*: Publicatie PKI Overheid publiek vertrouwde certificaten stopt.
2. *4 september 2021*: NCSC publiceert "Factsheet PKIoverheid verandert".
3. *13 september 2021*: Logius publiceert "Uitfasering uitgifte publiek vertrouwde webcertificaten PKI Overheid".

**Secretaris Generaal / plv. Secretaris Generaal**
Directie Informatiebeleid / CIO
Cluster iBeleid team A

**Datum**
18 oktober 2021

4. *Eind oktober 2021*: VWS beleid in potlood gereed voor het zorgveld, VWS organisaties, ZBO's en voor afhankelijke aanbieders.
5. *Eind november 2021*: Communicatie plan moet gereed zijn voor de zorgveld stelsel- en softwareaanbieders.
6. *Eind november 2021*: Helderheid over beleidsveranderingen VWS bij alle gelieerde of gekoppelde systemen met aansluitvoorwaarden en basisbeveiligingsmaatregelen, inclusief een vooruitblik hoe om te gaan met de beleidsverandering omtrent PKI Overheid.
7. *4 december 2021*: Uitgifte van certificaten uit de EV root CA zullen vanaf dit moment een einddatum krijgen van 4 december 2022. Deze einddatum is niet aan te passen, waardoor nieuwe certificaten steeds een dag korter geldig zullen zijn.
8. *Begin december 2021*: eerste PKI Overheid certificaten met publiek vertrouwen certificaten vervangen of uitgegeven voor PKI Overheid privaat vertrouwen of marktconform PKI certificaten en actief in de zorgsector.
    a. Zonder aanpassing op de aansluitvoorwaarden zijn de nieuwe certificaten niet geschikt voor het scenario waarin deze actief zijn. Effectief zijn er geen geschikte middelen ter beschikking zonder de benodigde aanpassingen.
    b. De risico's zijn dat op basis van ongewijzigde aansluitvoorwaarden portals voor burgers, dienstverleners, koppelvlakken en machine-to-machine koppelingen kunnen worden afgesloten of worden afgesloten zonder beschikbaar alternatief.
    c. Software die niet tijdig is aangepast kan niet koppelen met systemen die al wel de overstap naar de nieuwe certificaten soorten hebben gemaakt. Om continuïteit van de zorgdiensten te waarborgen blijven de volgende opties over:
        i. Onveilige verbindingen toe staan. De privacy garanties van dataoverdracht tussen zorgaanbieders, dienstverleners verleners en burgers vervalt.
        ii. Doorgaan met korter geldige PKI Overheid certificaten met publiek vertrouwen. Deze keuze is eindig en kan in theorie doorlopen tot 4 december 2022. In de praktijk zullen er andere zaken meespelen, zoals de beschikbaarheid van voldoende technici die systemen kunnen updaten. Het advies hierop is dat deze oplossing niet meer wordt ingezet na 1 juli 2022.
9. *Eerste en tweede kwartaal 2022 (prognose)*: Software die afhankelijk is en/of gebruik maakt van de PKI Overheid publiek vertrouwde certificaten moet zijn aangepast op het nieuwe beleid, uitgerold bij de zorgverleners en diensten platformen.
10. *Tweede en derde kwartaal (prognose)*: dienstenplatformen moeten volledig zijn overgeschakeld van PKI Overheid publiek vertrouwde certificaten naar enerzijds PKI Overheid privaat vertrouwde certificaten of marktconforme PKI certificaten.
11. *Derde en vierde kwartaal (prognose)*:
    a. TSP's zouden kunnen besluiten om de levering te stoppen van PKI Overheid publiek vertrouwbare certificaten onder de EV root CA met als motivatie de financiële rendabiliteit van de dienstverlening.
    b. crisis management actief door het zorgveld te monitoren en bewaken.

12. *4 december 2022*: Alle certificaten zijn verlopen in de keten van "Staat der Nederlanden EV Root CA"

**Secretaris Generaal / plv. Secretaris Generaal**
Directie Informatiebeleid / CIO
Cluster iBeleid team A

**Datum**
18 oktober 2021

*Beleidslijn*
Het nieuwe beleid zal de vereisten aan de PKI servercertificaten voor de zorgsector normeren op certificeringsvereisten voor de certificaatuitgevers, technische vereisten aan de certificaten en het niveau van zekerheid aan het proces op de uitgifte van de certificaten.

Voor 'machine-to-machine'-koppelingen is de overstap naar een privaat PKIO certificaat een veilige overstap en logische overstap. Deze bieden een vergelijkbaar betrouwbaarheidsniveau en zijn nu drie jaar geldig.
Voor burger-naar-zorgverlener contact is een publiek PKI certificaat noodzakelijk. De publieke certificaten kunnen ook toegepast worden voor 'machine-to-machine'-koppelingen. Dat kan gemak opleveren in de uitrolfase met eveneens de operationele risico's die voort kunnen komen uit de toepassing van publieke certificaten. Er moet rekening worden gehouden met de veranderingen die buiten de technische verschillen liggen, waaronder het uitgifte proces en de vaststellingen op (organisatorische) identiteitsvaststelling. Het uitvoeren van een risicoanalyse en/of impactanalyse wordt geadviseerd om een ketenbrede impact te kunnen bepalen.

De (server)certificaten mogen worden geaccepteerd en gebruikt in de zorg wanneer deze voldoen aan de volgende eisen:

1. De vereisten aan de certificaat leverancier voor PKI certificaten zijn:
    a. De meest up-to-date WebTrust audit is succesvol doorlopen en de certificering is geldig voor de 'Certificatie Authority' op iedere schakel in de keten van ondertekeningen tot en met de uitgifte processen.
    b. De private certificaten moeten afkomstig zijn van PKI Overheid geaccrediteerde certificaat ketens.
2. De technische vereisten zijn:
    a. De 'private key' moet worden gegenereerd op het doelplatform waar het PKI certificaat wordt toegepast.
    b. Bij gebruik van publieke PKI certificaten is de toepassing van 'Certification Authority Authorization Resource Record' vereist.
    c. Het toepassen van DNSSEC op de gebruikte domeinen is vereist onder de voorwaarden van pas-toe-of-leg-uit. Strengere eisen kunnen worden gesteld vanuit aanvullende kaders, zoals aansluitvoorwaarden.
    d. Het gebruik van wildcard certificaten wordt niet toegestaan.
    e. Het gebruik van 'multi-domain'-certificaten is toegestaan, onder de voorwaarde dat de eigenaar van het certificaat gelijk is aan de eigenaar van alle domeinen die opgenomen zijn in de Subject Alt Name DNS waarden van het certificaat.
3. Uitgifte:
    a. Het zekerheidsuitgifte niveau moet minimaal op het OV-niveau (Organisation Validated) of met hogere zekerheid zijn uitgegeven voor publieke PKI webserver certificaten wanneer persoonsgegevens van bijzondere aard worden verwerkt. Dit is relevant voor de aanschaf van het certificaat en dit valt achteraf te controleren op het bestaan van Policy Object

**Secretaris Generaal / plv. Secretaris Generaal**
Directie Informatiebeleid / CIO
Cluster iBeleid team A

**Datum**
18 oktober 2021

Identifiers (OIDs) die markeren welk type certificaat het betreft.

b. De uitgever van de PKI certificaten is verantwoordingsplichtig aan de AVG en/of GDPR.

4. Beheer:
   a. Veilig beheer moet zijn toegepast zoals toegelicht in 'Factsheet Veilig beheer van digitale certificaten'.
   b. Trust op zorgsystemen met systeem-systeem koppelingen al proactief de 'Staat der Nederlanden Private Root CA - G1' (te downloaden vanaf https://cert.pkioverheid.nl/) voor zover dat nog niet het geval is.

Met vriendelijke groet,

O. Koeroo
CISO Concern VWS

Met dank aan:
- CIBG
- VZVZ
- MinBZK
- NCSC