PKIOverheid G4-transitie

Status: in uitvoering **Waar:** #kring-techniek-pub

Wat het is

Vanaf 12 november 2026 geven het UZI-register en de andere PKIoverheid-uitgevers een nieuwe generatie certificaten uit: G4. Daarbij verandert de CA-hiërarchie en wijzigen velden en attributen in de UZI-certificaten, onder meer het veld met het URA-nummer.

De vraag is langs twee wegen bij de kring gekomen. Diana Demmer (ActiZ) vroeg op 14 juni via Sergej van Middendorp of, en zo ja in hoeverre, de PKIO-migratie die VZVZ aankondigt ook impact heeft op applicaties die met Nuts werken, en of wij daar iets mee moeten. Jorrit Spee stelde de vraag op 25 juni rechtstreeks aan de kring: hoe moeten wij ons hierop voorbereiden?

Relevantie voor Nuts

PKIoverheid-certificaten zijn in het Nuts-netwerk in gebruik voor TLS en mTLS, en UZI-certificaten worden gebruikt om Verifiable Credentials uit te geven en te valideren. Dat laatste is beschreven in RFC023 X509Credential: de houder van een UZI-certificaat geeft een `X509Credential` uit vanuit een `did:x509`, waarbij het vertrouwen wordt verankerd in de `ca-fingerprint`, de hash van de root- of intermediate-CA. Attributen uit het certificaat, waaronder het URA-nummer in `san:otherName`, komen daarmee in de credential terecht.

Dat heeft drie soorten gevolgen.

Trust anchors. Een nieuwe CA-hiërarchie betekent nieuwe hashes. Waar wij of een toepassing een `ca-fingerprint` vastleggen, moet die worden aangevuld of vervangen. Truststores en intrekkingscontrole moeten met de nieuwe hiërarchie overweg kunnen.

Toepassingen en hun presentation definitions. Per use case staan de geaccepteerde trust anchors in de presentation definition. Bij ACP/PZP is het G4 UZI-testcertificaat op 30 juni toegevoegd, zie PR 3 op application-on-nuts-acp-pzp. Dezelfde stap is nodig voor de andere toepassingen, waaronder Huisartsinzage, en de bijbehorende documentatie moet met de nieuwe hashes worden bijgewerkt. Zolang dat niet gebeurd is, worden credentials op basis van een G4-certificaat niet geaccepteerd.

Attributen en validatie. Wijzigt de plaats of de vorm van het URA-nummer of van andere attributen, dan raakt dat de opbouw van de `did:x509`, de `credentialSubject` en de validatieregels die daarop zitten.

Er is al enige praktijkervaring: in de PoC's rond de generieke functies is in april 2026 met G4 TRIAL-certificaten gewerkt en zijn de TRIAL- en productie-G4-roots in truststores opgenomen.

De datum ligt vast en is niet te beïnvloeden, dus dit is een van de weinige punten op deze lijst met een harde deadline.

Voorgestelde opdracht

De kring stelt een opdracht in om de impact van de PKIOverheid G4-transitie in beeld te brengen en de benodigde aanpassingen te laten plaatsvinden.

Doel. Zorgen dat deelnemers en toepassingen vóór 12 november 2026 klaar zijn om met G4-certificaten te werken in het Nuts-netwerk, en dat helder is wat wij daarvoor leveren en wat deelnemers zelf doen.

Scope. De opdracht richt zich op:

- **Vergelijking van de certificate practice statements** van de huidige en de nieuwe generatie, op techniek én op governance. Aandachtspunten: de manier waarop intrekking wordt gepubliceerd en gecontroleerd, welke claims en attributen in de certificaten staan en waar, de ondersteunde cryptografie en sleutellengtes, de opbouw van de hiërarchie en de wijze van uitgifte. Uit die vergelijking volgt wat er werkelijk verandert en niet alleen wat er anders heet.
- **De nuts-node en het knooppunt**: truststore, certificaatvalidatie en intrekkingscontrole met de G4-hiërarchie, en de plekken waar attributen uit het certificaat worden uitgelezen.
- **RFC023 en de X509Credential**: of de specificatie en de validatieregels ongewijzigd bruikbaar blijven onder G4.
- **De toepassingen op Nuts**: welke presentation definitions en welke documentatie per use case moeten worden aangepast, met de nieuwe hashes, en wie dat per toepassing doet. ACP/PZP en Huisartsinzage zijn in elk geval in beeld.
- **Testbaarheid**: of onze omgevingen en die van deelnemers met G4-certificaten te testen zijn, en langs welke weg.
- **Handelingsperspectief voor deelnemers**: wat verandert er, wat moeten zij doen en voor wanneer.

Buiten scope vallen: het aanvragen en beheren van certificaten door individuele deelnemers, de transitie binnen hun eigen infrastructuur, en het beleid van Logius en het UZI-register.

Resultaat. Een analyse met de verschillen tussen de oude en nieuwe generatie en de gevolgen daarvan, een lijst met aanpassingen per component en per toepassing, en een korte tekst richting deelnemers. Terugkoppeling in de kring.

Belegging. Het onderzoek is opgepakt vanuit het producteigenaarschap van de nuts-node en loopt via issue 4355. Voorstel is om die lijn te bevestigen en de opdracht daar formeel te beleggen. De aanpassingen per toepassing liggen bij de toepassingen zelf; onze rol daar is signaleren wat er moet gebeuren en ondersteunen.

Werkwijze. Analyse eerst, dan pas ontwikkelwerk. Wat uit de analyse volgt aan aanpassingen komt op de backlog van de nuts-node en wordt langs de gebruikelijke weg geprioriteerd. Wat bij toepassingen ligt, gaat via de kring Toepassingen en het convergentieoverleg. Het handelingsperspectief voor deelnemers gaat via de gebruikelijke kanalen naar buiten, in afstemming met ActiZ waar dat helpt.

Input voor de opdracht

- RFC023 X509Credential, met de rol van `ca-fingerprint` en de validatieregels
- PR 3 op application-on-nuts-acp-pzp, waarin het G4 UZI-testcertificaat is vertrouwd voor ACP/PZP
- UZI-register, CA-certificaten G4 en de gepubliceerde CA-certificaten
- Logius, wees voorbereid op de nieuwe generatie PKIoverheidcertificaten
- PKI Partners, transitie G1 en G3 naar PKIoverheid G4 en het aanvragen van G4 TRIAL-certificaten, met een doe-het-zelfvariant via github.com/pkioverheid/g4-trial
- De certificate practice statements van de huidige en de nieuwe generatie
- De ervaring uit de GF-PoC's met TRIAL- en productie-G4-roots in truststores
- Het artikel dat ActiZ op 5 augustus publiceerde in haar community ICT en Informatiebeleid

VZVZ heeft op de Netwerkdag van 25 juni een sessie gehouden over de PKI G4-transitie, met aandacht voor de impact op zorgapplicaties, netwerkcommunicatie en authenticatie, en voor de ondersteuning die VZVZ zelf biedt. Het is de moeite waard om te weten wat daar is verteld voordat wij deelnemers apart gaan informeren.

Planning

Alleen de laatste stap heeft een vaste datum. De stappen daarvoor werken daar naartoe en krijgen hun data bij het beleggen van de opdracht.

Stap	Wat	Wanneer
1	Opdracht beleggen en scope bevestigen in de kring	eerstvolgende kringvergadering
2	Analyse opleveren: verschillen tussen de generaties, impact per component en per toepassing	nader te bepalen
3	Aanpassingen doorvoeren in de nuts-node en het knooppunt, en releasen	nader te bepalen
4	Presentation definitions en documentatie per toepassing bijwerken	nader te bepalen

Stap	Wat	Wanneer
5	Deelnemers informeren over wat zij zelf moeten doen	ruim voor stap 6
6	Start uitgifte van G4-certificaten	12 november 2026

Te besluiten

1. Geeft de kring consent op de opdracht zoals hierboven beschreven?
2. Klopt de scope, en met name de afbakening dat wij niet over de transitie bij deelnemers zelf gaan?
3. Bevestigt de kring de belegging bij het producteigenaarschap van de nuts-node, en met welke tijdsbesteding?
4. Welke einddata hangen we aan de stappen 2 tot en met 5?
5. Langs welke weg brengen we de aanpassingen per toepassing onder de aandacht bij de kring Toepassingen?

Samenhang met andere trajecten

- **v6-migratie.** Deelnemers die nog op v5 draaien krijgen twee wijzigingen tegelijk over zich heen. Het is de moeite waard om te weten of de G4-ondersteuning in beide versies gelijk is.
- **LSP x Nuts en de generieke functies.** Daar worden UZI-certificaten en de X509Credential gebruikt, dus wijzigingen in de hiërarchie en de attributen raken die trajecten direct.
- **Toepassingen op Nuts.** De aanpassing van presentation definitions en documentatie loopt per toepassing en raakt de convergentielijn met de kring Toepassingen.

Bronnen

Wat	Waar
Vraag van Diana Demmer via Sergej van Middendorp, 14 juni 2026	Slack, #kring-techniek-pub
Vraag van Jorrit Spee aan de kring, met de externe links, 25 juni 2026	Slack, #kring-techniek-pub
Onderzoek naar de impact op de nuts-node	nuts-node issue 4355
G4 UZI-testcertificaat vertrouwd voor ACP/PZP, 30 juni 2026	PR 3
Agendapunt VZVZ Netwerkdag over de PKI G4-transitie, 25 juni 2026	Slack, #gf-cot
Werken met G4 TRIAL-certificaten in de GF-PoC's, april 2026	Slack, #gf-poc-3-poc-12

Wat	Waar
ActiZ-artikel over de G4-certificaten, 5 augustus 2026	Slack, #haagsezaken, met pdf
Analyse van Edwin de Wit	Google Docs

Wie erbij betrokken zijn

Rol	Wie
Vraagstellers	Jorrit Spee en Diana Demmer (ActiZ)
Onderzoek en producteigenaarschap nuts-node	Rein Krul
Ervaring met G4 in toepassingen	Edwin Rozendom (Topicus), vanuit ACP/PZP
Communicatie richting deelnemers	nog te bepalen

Hoe haak je aan

Loop je zelf tegen vragen aan over de G4-transitie in combinatie met Nuts, of heb je al ervaring met G4-certificaten in je eigen omgeving, meld het in #kring-techniek-aanspreekpunt.

Revision #4
Created 2026-08-06 08:24:20 UTC by Steven van der Vegt
Updated 2026-10-14 08:56:12 UTC by Rein Krul