PKIoverheid

Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling

Colofon

DATUM	13-3-2019
VERSIE	1.0
PROJECT REFERENTIE	BZK – Onderzoek PKIoverheid
VERTROUWELIJKHEID	Publiek
STATUS	Definitief
BEDRIJF	InnoValor
AUTEUR(S)	Henny de Vos & Bob Hulsebosch

Synopsis

Dit rapport beschrijft de resultaten van het onderzoek naar gebruik van PKIoverheid certificaten en analyse van mogelijkheden om het gebruik te vergroten, bijvoorbeeld door verplichten. Het onderzoek is uitgevoerd in opdracht van het Ministerie van BZK.

Inhoudsopgave

Management samenvatting

Public Key Infrastructure (PKI) voor de overheid, kortweg PKIoverheid of PKIo, maakt betrouwbare digitale communicatie mogelijk met, door en binnen de Nederlandse overheid. PKIoverheid is een infrastructuur, gebaseerd op digitale certificaten. Publieke en private Trust Service Providers (TSP) binnen het PKIoverheid stelsel realiseren een betrouwbare uitgifte van PKIo-certificaten. Deze uitgifte gebeurt onder strikte voorwaarden en toezicht van de Policy Authority PKIoverheid, belegd bij Logius. PKIo-certificaten kennen verschillende toepassingen: authenticatie van personen, website beveiliging, veilige versleutelde berichtenuitwisseling tussen servers en digitaal ondertekenen of waarmerken.

Doel en aanpak van het onderzoek
In 1999 besloot de minsterraad te starten met PKIoverheid met als doel veilige overheidscommunicatie. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor het beheer en toezicht op het PKIoverheid stelsel en heeft de opdracht gegeven om het huidige gebruik van PKIo-certificaten te inventariseren en de mogelijkheden en omstandigheden voor verdere adoptie te verkennen. Ofwel, op welke manier kan PKIoverheid een stevigere basis krijgen als essentiële voorziening voor veilige communicatie met en binnen de overheid. Specifiek wordt gekeken naar verplichting. Het voorliggende rapport schrijft de uitkomsten van het onderzoek. De opdracht is uitgevoerd middels documentatie onderzoek, 16 interviews met belanghebbenden en een brede expertconsultatie. Het onderzoek is uitgevoerd in de periode december 2018 – februari 2019.

Huidig gebruik PKIo
In 2017 waren er 658.000 geldige PKIo certificaten in omloop. Deze certificaten worden toegepast voor website beveiliging, veilige servercommunicatie, digitaal waarmerken en authenticatie van gebruikers. Het is niet bekend hoe de certificaten zijn verdeeld over deze toepassingen.

Website beveiliging. Het al dan niet toepassen van PKIo hangt af van beleid van de overheidsorganisatie en/of van de leverancier. Websites onder beheer van het Ministerie van Algemene Zaken hebben standaard PKIo. Een ruwe inschatting is dat ongeveer 40% van de overheidsdomeinen een PKIo-certificaat toepast. Een specifiek probleem hier is dat de nieuwste generatie PKIo-certificaten (EV) niet werken bij oudere browserversies en men terug moet vallen op andere gekwalificeerde certificaten.

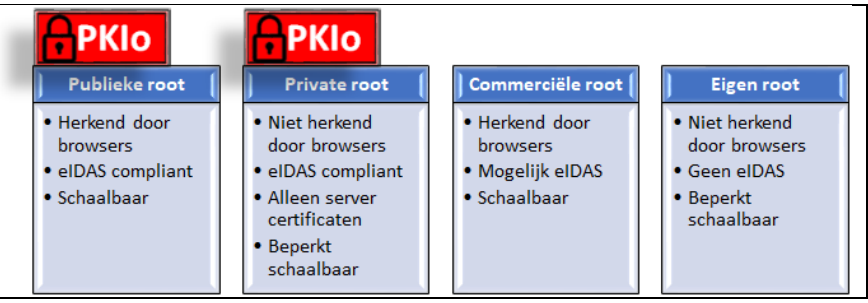
Veilige communicatie (tussen servers). De dienstverleningsvoorwaarden bepalen of PKIoverheid moet worden toegepast. Logius diensten eisen in de regel een PKIo servercertificaat, voor andere diensten is dit niet per se het geval. Grootgebruikers van diensten, zoals gemeenten, hebben meerdere PKIo-certificaten nodig en gebruiken daarnaast ook andere PKI-certificaten. Andere redenen voor toepassing van PKIo-overheid servercertificaten zijn standaarden (bijv. Digikoppeling) en stelsels (zoals eHerkenning en MedMij). Een servercertificaat is ook beschikbaar met een ‘private’ root, dat wil zeggen dat deze niet herkend wordt door de browsers.

Digitaal waarmerken. Voor waarmerken zoals digitale handtekeningen worden persoonlijke certificaten (en beroepscertificaten) toegepast. Dat kan zowel PKIo zijn als anderszins. Het Ministerie van Defensie past bijvoorbeeld een PKIo-certificaat op de Defensiepas waarmee waarmerken mogelijk is. Ministerie van Justitie en Veiligheid kiest ervoor om een eigen PKI te gebruiken voor waarmerking binnen het eigen domein en PKIo voor erbuiten. Uittreksels uit het diplomaregister van DUO of het handelsregister van de Kamer van Koophandel zijn met een PKIo-certificaat gewaarmerkt.

Authenticatie. Voor breed toegankelijke algemene dienstverlening voor bedrijven en personen wordt meestal DigiD of eHerkenning toegepast. Hier wordt PKIo nauwelijks voor gebruikt. Er zijn ook domeinspecifieke authenticatieoplossingen. Sommige van deze middelen bevatten PKIo-certificaten (Taxipas, UZI-pas), anderen niet (RDW voor garages, DUO voor scholen).

Conclusie. *Ten aanzien van toepassing van certificaten zien we een heel gevarieerd gebruik. In sommige gevallen wordt PKIo toegepast in andere gevallen een eigen of alternatieve (commerciële) PKI oplossing. Gebruik wordt bijvoorbeeld afgedwongen door de Baseline Informatiebeveiliging Rijksoverheid, in*

afsprakenstelsels, door standaarden en voor rechtsgeldigheid. Desondanks wordt PKIo (nog) niet in de volle breedte toegepast. Er is ruimte voor PKIo om te groeien.



Binnen de context van communicatie met, door en binnen de overheid worden verschillende PKI's toegepast, zowel PKIo, commerciële als eigen certificaten.

Voor welke toepassingen is verplichting van PKIo relevant en haalbaar?

De ervaringen en visies met PKIo die zijn opgehaald in het onderzoek zijn gestructureerd door middel van een SWOT-analyse. Er ontstaat een wisselend beeld over nut en noodzaak van PKIo, met veel sterke punten en kansen en nog meer zwaktes en bedreigingen. Met deze beelden als uitgangspunt is per toepassing van PKIo onderzocht wat de haalbaarheid is van verplichtstelling om het gebruik te stimuleren.

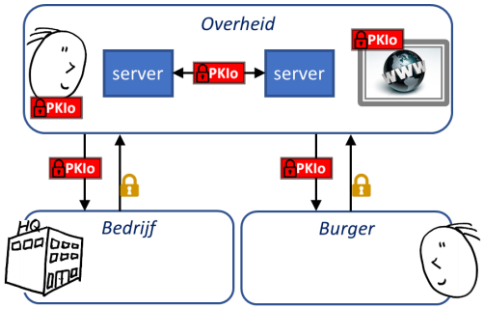
Website beveiliging. Verplichting van PKIo is wenselijk om de websites van de overheid een veilige en betrouwbare uitstraling te geven. Verplichting bij voorkeur overheidsbreed, dus ook voor lagere overheden. Merk op dat de beveiligingsmeerwaarde ten opzichte van andere certificaten beperkt is; het is vooral een kwestie van uitstraling en om te voorkomen dat overheidswebsites middels onduidelijk gekwalificeerde certificaten worden beveiligd.

Veilige communicatie (tussen servers). De meerwaarde van PKIo ten opzichte van andere certificaten is ook hier beperkt. Verplichten van PKIo neemt deze beperking niet weg. Bovendien moeten in het kader van de Europese eIDAS verordening ook andere gekwalificeerde certificaten geaccepteerd worden ten behoeve van de single European digital market. Verstandiger is om voor communicatie met de overheid in te steken op betrouwbaarheidsniveaus: geef aan welke niveau vereist is om te koppelen met een overheidsvoorziening. Het toepassen van het specifieke Organisatie Identificatie Nummer (OIN) in dienstverlening is een knelpunt om deze visie te realiseren. Voor veilige intra-overheidscommunicatie tussen servers is het verstandig om PKIo-certificaten die onder de private root zijn uitgegeven wel verplicht te stellen.

Digitaal waarmerken. PKIo biedt meerwaarde in termen van uitstraling, vooral bij communicatie van de overheid naar buiten. Digitaal waarmerken heeft groeipotentie. Verplichting van PKIo kan hierbij bijdragen aan harmonisatie van oplossingen. De kosten van PKIo zijn een potentiële showstopper. Verplichting kan helpen om schaalvoordelen te bereiken die doorwerken in de kosten. Om de kosten te verlagen valt ook te overwegen om digitale zegels in te zetten en om goed te beoordelen wanneer een gekwalificeerde digitale handtekening nodig is. Sinds medio 2017 is een dergelijke zegel binnen PKIo mogelijk (eSeal) – de bekendheid daarvan bij afnemers is nog beperkt.

Authenticatie van personen, beroepen of bedrijven. Het verplichten van PKIo is niet haalbaar. Er zijn teveel andere publieke en private oplossingen die 'last' krijgen van een eventuele verplichting van PKIo. Het is zaak hier te focussen op het vaststellen van betrouwbaarheidsniveaus van authenticatie voor toegang tot diensten. Het is dan aan de gebruiker om hiervoor een bijpassend en erkend authenticatiemiddel te selecteren. Dit kan een PKIo-certificaat zijn, maar ook een ander erkend middel.

Scope van verplichting. De toepassing van PKI binnen het overheidsdomein is zeer gevarieerd. Geadviseerd wordt om een keuze te maken voor de context van verplichting. Wenselijk is om bij verplichtstelling te focussen op communicatie binnen de overheid en vanuit de overheid naar buiten. Binnen de overheid is het wenselijk te opteren voor een PKIo-private-root certificaat voor veilige server-to-server communicatie. Voor communicatie van bedrijven en burgers richting de overheid is PKIo een optie, maar kan ook een ander middel worden gekozen, mits deze voldoet aan betrouwbaarheidseisen. Voor communicatie vanuit de overheid ligt PKIo voor de hand. De figuur hieronder schetst deze verschillende situaties.



Figuur 1: Contexten voor (verplicht) gebruik van PKIo.

Conclusie. *Voor drie PKIo-toepassingsgebieden is verplichting van PKIo relevant: websites, digitaal waarmerken/ondertekenen en veilige communicatie tussen servers van overheidsorganisaties onderling. Voor de andere toepassingsgebieden, authenticatie van personen en veilige communicatie met servers buiten het overheidsdomein, kan worden gewerkt met betrouwbaarheidsniveaus en gebruik worden gemaakt van middelen die daarbinnen passen.*

Mogelijkheden voor verplichten

Verplicht stellen genereert een groter gebruik van PKIo. Verplichten is geen doel op zich, maar een middel dat tot doel heeft om de digitale communicatie met de overheid betrouwbaarder en veiliger te maken. Een belangrijke consequentie van verplicht stellen is dat kosten voor afnemers sterk kunnen stijgen i.v.m. aanschaf van (meer) PKIo certificaten, met daarbij een grotere certificatenbeheerlast en noodzaak tot opbouwen van specifieke expertise. De verwachting is wel dat er schaalvoordelen ontstaan doordat vergroting van gebruik de prijzen kunnen laten dalen. Verplicht stellen vereist dat gebruik van PKIo wordt gemonitord en dat er zicht is op waar en door wie PKIo certificaten op een juiste manier worden toegepast.
Verplichten kan op verschillende manieren: verankering in wetgeving, opnemen in handreikingen of via de Pas-toe-of-leg-uit lijst. Daarnaast is 'verleiden' een logische aanvulling en kan gedacht worden aan toepassen in andere contexten dan overheidsdienstverlening.

Verankering in wetgeving. De wet Digitale Overheid (wet DO) of onderliggende regelgeving lijkt op het eerste gezicht passend om het verplicht gebruik van PKIo te verankeren voor de relevante toepassingsgebieden. Het wetsvoorstel bevat onderdelen zoals de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid, het stellen van regels over informatieveiligheid en de digitale toegang tot publieke dienstverlening voor burgers en bedrijven op basis van erkende middelen. Echter de wet DO is deels gebaseerd op de Europese eIDAS. Afbakenen naar een Nederland-specifieke PKI druist in tegen het uitgangspunt van de eIDAS verordening, namelijk een unieke digitale Europese markt. De Nederlandse overheid zal daarom ook andere erkende certificaten uitgegeven onder eIDAS gekwalificeerde TSPs moeten accepteren. Verplicht stellen via wetgeving van alleen PKIo-certificaten is derhalve niet haalbaar.

Opnemen in baselines, handreikingen of richtlijnen. Informatie beveiligingsrichtlijnen werken de uitvoering van een wet uit voor een specifiek domein, eventueel aangevuld met aanvullend beleid. Bijvoorbeeld de BIR (Baseline Informatiebeveiliging Rijksoverheid) of de VIRBI (Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie). De BIR is een interdepartementaal kader waaraan alle ministeries zich hebben gecommitteerd en is dus verplichtend op basis van een onderlinge interdepartementale afspraak. In de BIR wordt PKIo al verplicht voor communicatie betreffende gevoelige gegevens. CISO's (in de regel) van de departementen houden hier toezicht op. Desondanks departementen ruimte zien om buiten PKIo om te werken voor hun specifieke toepassingen. VIRBI is een doelstellende regeling met minimumeisen voor het te ontwikkelen beveiligingsbeleid en implementatie maatregelen binnen een ministerie. Alhoewel de VIRBI technologieneutraal is, zijn er aanknopingspunten waar PKIo een manier is om eisen adequaat in te vullen. De 'rijksbeveiligingsambtenaar' is verantwoordelijk voor de realisatie van rijksbreed toezicht op de naleving van de Rijksbrede kaders.
We bevelen aan om gebruik van PKIo nader te specificeren in de bestaande vigerende beveiligingsrichtlijnen en deze op beleidsniveau wederom onder de aandacht te brengen om toepassing van PKIo te vergroten. De uitdaging hierbij is om dat waar nodig technologieneutraal te realiseren.

Opnemen in de Pas-toe-of-leg-uit lijst van verplichte standaarden. Een minder verplichtend alternatief voor verplichtstelling is de pas-toe-of-leg-uit-lijst (PTOLU) van het Forum Standaardisatie. In beginsel is toepassing van standaarden op deze lijst verplicht, tenzij er (goede) redenen zijn om er van af te wijken. Voor PKIo zou dit ruimte geven aan andere alternatieven als PKIo toch niet passend is. Opname van PKIo op de lijst is haalbaar voor specifieke toepassingen: website certificaten, waarmerken en/of veilige communicatie tussen overheidsservers. Voordeel van de PTOLU lijst is dat toepassing van PKIo dan wordt gemonitord, tenminste als het wordt benoemd als één van de belangrijke standaarden. Een aandachtspunt is dat PKIo-versies en de PTOLU lijst met elkaar in lijn blijven.

Verleiden. Naast verplichten is het ook wenselijk om PKIo beter te positioneren en (ervaren) zwaktes en weerstanden weg te nemen. Communicatie is daarbij essentieel. Die is nu vaak moeizaam vanwege de complexiteit van het stelsel. Het creëren van ruimte voor innovaties binnen PKIo helpt, zoals het op afstand kunnen identificeren van gebruikers in plaats van fysieke verschijning aan de balie tijdens de uitgifte.

Verbreding van de context. Het toepassen van PKIo-certificaten voor andere communicatie dan met, door en binnen de overheid is een andere manier om het gebruik ervan te vergroten. De Taxipas en UZI-pas zijn hier al voorbeelden van. Gedacht kan worden aan het verplicht gebruik van PKIo-certificaten in kritische of vitale infrastructuren, bijvoorbeeld op basis van de wet beveiliging netwerk- en informatiesystemen (Wbni). Dit zal kostenverlagend en bewustzijnsverhogend werken.

Conclusie. *Wettelijke verankering lijkt minder haalbaar vanwege interferentie met eIDAS regelgeving. De focus van verplichting ligt op een gecombineerde aanpak van opname in richtlijnen en de PTOLU-lijst en activering van gebruik. In combinatie met verleiding door middel van verbeterde communicatie en het wegnemen van enkele zwaktes en weerstanden moet dit er toe leiden dat PKIo binnen de overheid vanzelfsprekend wordt. Daarnaast kan worden overwogen om PKIo te introduceren in kritische of vitale infrastructuren.*

Herijken PKIo

In diverse interviews en tijdens de expertconsultatiesessie kwam naar voren dat herijking van het PKIo stelsel nodig is. Destijds is de overheid gestart met PKIo op basis van een aantal uitgangsprincipes en doelstellingen. In de loop der jaren is veel veranderd: meer focus op server certificaten, een publieke en private root, veel aandacht voor het CAB-forum, en de komst van de Europese eIDAS verordening. Ook voor het eventueel verplichten van PKIo toepassingen is een herijking wenselijk. Na een herijking zal het eenvoudiger zijn om bepaalde onderdelen van PKIo te verplichten.

Herijking is meer dan alleen ‘de stofkam’ door het stelsel halen om het weer ‘lean and mean’ te maken. Het zou ook een andere opzet van het stelsel kunnen betekenen. Zoals de uitgifte van PKIo-certificaten centraliseren onder eigen (overheids)beheer en gebruik te beperken voor de eigen overheidsorganisaties. Een eigen overheidsbrede-TSP zou bijvoorbeeld door de huidige TSP van Defensie kunnen worden ingevuld of door een meer neutrale partij als Logius of DICTU. Daarmee wordt de rol van de private TSPs voor het overheidsdomein beperkt tot het leveren van infrastructuur componenten. Het verstrekken van certificaten door de private TSPs zal dan voor een andere root CA zijn. Potentiële afnemers van PKIo zijn dan private organisaties die met de overheid moeten communiceren of gebruikers die een authenticatiemiddel op een hoog betrouwbaarheidsniveau nodig hebben. Dit scenario lijkt in strijd met de uitgangspunten van de Wet Markt en Overheid en behoeft nader onderzoek.

Conclusie. *Een herijking van PKIo is wenselijk maar niet triviaal en raakt diverse aspecten die van grote invloed kunnen zijn op een toekomstige andere inrichting ervan. Nader onderzoek is nodig naar de mogelijkheden van verschillende inrichtingen van PKIo en de beleidsmatige impact die hiermee gepaard gaat. De eigenaar zal moeten kiezen voor een bepaalde inrichting van PKIo en hier naar gaan handelen. Herijking is wenselijk om beter duiding te kunnen geven aan verplichtende onderdelen van PKIo op langere termijn.*

Samenvattend*:*

- Verplichting PKIo voor beveiliging van overheidswebsites, digitaal waarmerken vanuit de overheid en server-to-server communicatie binnen overheid.
- De mogelijkheid om PKIo toe te passen voor andere toepassingen is niet verplicht maar wel mogelijk.
- Verplichting vooralsnog via handreikingen en richtlijnen (bijv. BIR) en opname in Pas-toe-of-leg-uit lijst.

- Verplichting laten samengaan met een communicatiecampagne, o.a. richting afnemers in het algemeen over de voordelen van PKIo, en specifiek ook richting beleid.
- Herijking PKIo afsprakenstelsel om complexiteit te reduceren en ruimte te creëren voor vernieuwing (zoals bijv. in het uitgifte proces).
- Bij herijking hoort ook een keuze maken rond de scope van verplichting van PKIo: PKIo voor alle overheidsdiensten in een publiek-privaat stelsel, PKIo alleen binnen het overheidsdomein met publieke en private TSPs of PKI alleen binnen het overheidsdomein met een publieke TSP.
- Keuze om toepassing van PKIo buiten het overheidsdomein te laten groeien, typisch voor kritische of vitale infrastructuren (zoals nu voor de zorgsector of taxibranche).

1. Inleiding

Public Key Infrastructure (PKI) voor de overheid, kortweg PKIoverheid of PKIo, maakt betrouwbare digitale communicatie mogelijk binnen en met de Nederlandse overheid. PKIoverheid is een zeer hoogwaardige en veilige infrastructuur, gebaseerd op digitale certificaten. Het PKIoverheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort. Het bevat gegevens die nodig zijn voor beveiligd internetverkeer. Digitale certificaten zijn een onmisbare schakel in beveiligd internetverkeer.

PKIoverheid zorgt voor een veilige en betrouwbare uitgifte van PKIo-certificaten door Trust Service Providers (TSP) die zijn aangesloten op het PKIoverheid stelsel. De uitgifte van PKIo-certificaten gebeurt onder strikte voorwaarden van de Policy Authority PKIoverheid die wordt gerealiseerd door Logius. PKIo-certificaten kennen verschillende toepassingen: authenticatie van personen, websites en systemen, veilige versleutelde berichtenuitwisseling tussen en met de overheid en gekwalificeerde elektronische handtekeningen en digitaal waarmerken.

Sinds het besluit van de minsterraad in 1999 om met PKIoverheid te starten met als doel om overheidscommunicatie veilig te maken, worden PKIo-certificaten inmiddels door een groot aantal partijen gebruikt. Echter, het gebruik ervan is zeker nog geen gemeengoed. Gebruik is te zien bij o.a. eHerkenning, Digipoort, SBR, DigiD, Mijn overheid, DigiInkoop en op persoonsgebonden smartcards in bijvoorbeeld de zorg, de taxibranche en Defensie. Andere PKI-oplossingen zijn er ook, hier maken o.a. RDW, DUO en het Ministerie van Justitie en Veiligheid gebruik van.

Dit rapport bevat de resultaten van een verkennend onderzoek naar het huidige gebruik van PKIo-certificaten en mogelijkheden om gebruik te verbreden, bijvoorbeeld via verplichtstelling.

1.1 DOEL

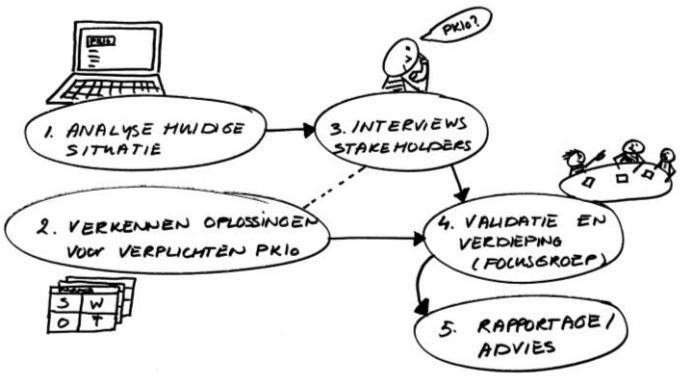
Het doel van het onderzoek in dit rapport is om een afwegingskader te realiseren ten behoeve van de uitgifte en (verplicht) gebruik van PKIo-certificaten. Het onderzoek richt zich op het inventariseren van het huidige gebruik van PKI-certificaten en de omstandigheden waaronder de adoptie ervan kan worden vergroot. Ofwel, op welke manier kan PKIoverheid een stevigere basis krijgen als essentiële voorziening voor veilige communicatie met en binnen de overheid.

Daarbij wordt op hoofdlijnen ingegaan op juridische aspecten van gebruik en verplichting van PKIo certificaten, op huidige werkwijzen voor authenticatie, berichtenuitwisseling en waarmerken, voor- en nadelen van PKIo. Daarnaast verkennen we mogelijkheden om PKIo te verplichten.

Specifieke onderzoeksvragen die zullen worden beantwoord zijn:

1. Wat zijn redenen om PKIo wel of niet toe te passen?
2. Hoe kan het bredere gebruik van PKI overheidscertificaten het best worden afgedwongen?
3. Is een verplichting via de wet Digitale Overheid opportuun?
4. Zijn er andere kaders waarop ingehaakt kan worden om het gebruik af te dwingen?

1.2 AANPAK



Het onderzoek is uitgevoerd in de periode december 2018 – februari 2019 en bestaat uit in vijf onderdelen die iteratief zijn aangepakt:

1. Analyse van de huidige situatie: In deze activiteit is de huidige situatie van PKIo in kaart gebracht en geanalyseerd. Dit is gedaan via bureauonderzoek vooral gericht op het in kaart brengen van het gebruik van PKIo-certificaten: wie gebruikt het, op welke manier en waarvoor. Een belangrijke bron voor het in kaart brengen van het gebruik van PKIo-website certificaten is het register https://crt.sh/. Ook is onderzocht waarom PKIo-certificaten in bepaalde ketens of sectoren niet wordt gebruikt terwijl dat wel voor de hand zou liggen vanwege de gevoeligheid van de uit te wisselen gegevens.
2. Verkennen oplossingen voor verplichten PKIo: Per PKIo-toepassing is een overzicht van mogelijke oplossingen om het verplicht gebruik ervan mogelijk te maken verkent, met daarbij aanbevelingen van manieren om PKIo verder te versterken danwel het succes van de oplossingsrichting te vergroten.
3. Interviews onder stakeholders (zie bijlage 1): Via interviews met stakeholders is een verdere verdieping en validatie van de resultaten uit de eerste twee activiteiten gerealiseerd.
4. Validatie en verdieping via een expertconsultatie (zie bijlage 2): De uitkomsten uit de vorige activiteit zijn nader gevalideerd en geduid in een interactieve discussiesessie met een bredere focusgroep. Een belangrijk doel van deze discussiesessie was het creëren van consensus voor mogelijke oplossingsrichtingen aangaande het stimuleren van het gebruik van PKIoverheid.
5. Rapportage en advies. Het verwerken van alle resultaten en inzichten uit de focusgroep in het onderliggende definitieve adviesrapport. Dit rapport bevat tevens de antwoorden op de specifieke onderzoeksvragen en geeft aanbevelingen voor verdere adoptie van PKIoverheid. De concept rapportage is voorgelegd aan alle geïnterviewden en deelnemers aan de expertconsultatie ter review. Opmerkingen en suggesties uit deze reviewronde zijn verwerkt in dit eindverslag.

1.3 LEESWIJZER

Hoofdstuk 2 vat PKIoverheid en de toepassingen samen. In hoofdstuk 3 geven we een overzicht van de mate van gebruik van PKIoverheid voor de verschillende toepassingen. Hoofdstuk 4 behandelt de sterke en minder sterke elementen van PKIoverheid en de kansen en bedreigen en geeft aanknopingspunten voor verbreding van gebruik. Hoofdstuk 5 geeft mogelijkheden om verplichting vorm te geven. In Hoofdstuk 6 beschrijven we de conclusies en aanbevelingen voor het stimuleren van het gebruik van PKIoverheid.

2. PKIo in een notendop

PKIoverheid is een afsprakenstelsel voor het verstrekken en gebruiken van PKI-certificaten met extra eisen vanuit de overheid. Met PKIoverheid certificaten kan veilig met, door en binnen de overheid worden gecommuniceerd. Voor de verschillende gebruikstoepassingen zijn meerdere typen PKIoverheid certificaten. Dit hoofdstuk vat PKIoverheid samen.

2.1 WAT IS PKIoverheid?

PKIoverheid is de Public Key Infrastructure (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een afsprakenstelsel om digitale certificaten uit te geven en te beheren. PKIoverheid wordt beheerd door Logius, de policy authority.

PKIo-certificaten bieden aanvullende zekerheden ten opzichte van algemene digitale certificaten. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.

De techniek van PKIoverheid is identiek aan andere PKIs. Het verschil zit in de technische hoogste autoriteit (root CA). In een commerciële PKI wordt de root geleverd door een commerciële organisatie, bijvoorbeeld DigiCert of Commodo. De root is de bron van het certificaat, de partij die het certificaat heeft geautoriseerd. Bij PKIoverheid is de root de Staat der Nederlanden. De Nederlandse overheid is verantwoordelijk voor het stamcertificaat op de root CA, waardoor PKIoverheid niet afhankelijk is van (buitenlandse) commerciële partijen.

PKIoverheid is een stelsel van voorwaarden voor het uitgeven van certificaten. Commerciële en gecertificeerde CA's (Certificate Service Providers genoemd, sinds eIDAS worden deze leveranciers Trusted Service Providers of TSPs genoemd) kunnen aansluiten bij PKIoverheid. De CA van deze TSP wordt dan opgenomen in de hiërarchie van PKIoverheid. PKIoverheid geeft zelf geen eindgebruikerscertificaten uit, alleen certificaten aan de TSP's. De TSP’s verstrekken de certificaten aan de eindgebruikers. PKIoverheid stelt voorwaarden voor uitgifte van deze certificaten. Deze zijn onder meer overeenkomstig aan de voorwaarden voor gekwalificeerde certificaten. Eén van die voorwaarden is dat de aanvrager zich op een betrouwbare manier moet identificeren. De voorwaarden gelden niet alleen voor de persoonsgebonden certificaten, maar ook voor de certificaten op organisatieniveau. Met PKIoverheid streeft de Rijksoverheid naar één hoog betrouwbaarheidsniveau voor alle certificaattypen.

Onder PKIoverheid worden ook uitgebreid gevalideerde certificaten (Extended Validation Certificates) uitgegeven. Bij een geldig EV-certificaat verschijnt een groene balk in de adresbalk. eHerkenning maakt bijvoorbeeld gebruik van zo'n type PKIoverheid certificaat. Tevens worden er PKIoverheid Qualified Website Authentication Certificates (QWAC certificaat) uitgegeven, die aan de Europese eIDAS verordening voor vertrouwensdiensten voldoen.

2.2 HOE WERKT HET?

Een PKIoverheid-certificaat wordt gebruikt voor:

- Authenticatie van personen, websites en servers;
- Waarmerken door middel van gekwalificeerde elektronische handtekeningen of zegels;
- Versleuteling van elektronische berichten.

Er zijn verschillende soorten PKIoverheid-certificaten:

1. PKIoverheid persoonsgebonden certificaat om een bepaald persoon de mogelijkheid te geven elektronische (internet-)transacties te beveiligen. Een persoonsgebonden certificaat kan voor meerdere toepassingen worden gebruikt, bijvoorbeeld voor beveiliging van persoonlijke e-mail, sterke gebruikersauthenticatie en rechtsgeldig digitaal ondertekenen van documenten.

2. PKIoverheid-servicescertificaat dat is gebonden aan een organisatie en wordt uitgegeven aan apparaten of servers, of groepen individuen. Het certificaat wordt gebruikt om de communicatie te beveiligen tussen elektronische overheidsapplicaties en diensten. Specifiek kan onderscheid worden gemaakt tussen:
    a. Servercertificaten voor beveiligde communicatie tussen servers (SSL/TLS). Eén PKIoverheid servercertificaat kan worden gebruikt voor meerdere voorzieningen, bijvoorbeeld Digilevering, DigiInkoop en DigiPoort.
    b. Beroepscertificaten voor rechtsgeldig en veilig communiceren vanuit een erkend beroep.
    c. Groepscertificaten voor veilig communiceren, ondertekenen en inloggen met een algemeen e-mailadres.
    d. Extended Validation (EV) SSL-certificaten als extra zekerheid voor website en online transacties, (niet-persoonlijke) e-mailadressen en certificatie van elektronische documenten. Tevens worden er PKIoverheid Qualified Website Authentication Certificates (QWAC certificaten) uitgegeven, die aan de eIDAS verordening voldoen. PKIoverheid EV certificaten voldoen aan deze eisen, mits uitgegeven door een vertrouwde leverancier. Europese eIDAS verordening 910/2014 bepaald de eisen voor QWAC, de uitgifte daarvan en erkenning door alle lidstaten[1]. eIDAS biedt daarmee de mogelijkheid om QWACs te gebruiken. In de PSD2 (richtlijn 2015/2366) wordt QWACs verplicht gesteld binnen het financiële domein.

De echtheid van een digitaal certificaat wordt altijd afgeleid van een stamcertificaat. Bij een PKIoverheid-certificaat is dat het stamcertificaat 'Staat der Nederlanden Root CA', waarvoor de Nederlandse overheid verantwoordelijk is. Daarnaast is PKIoverheid gebaseerd op Nederlandse wet- en regelgeving. Dat maakt het een hoogwaardig en betrouwbaar certificaat. Het is bovendien gebaseerd op Europese standaarden en voldoet aan internationaal geaccepteerde richtlijnen.

Verder kent PKIoverheid voor servercertificaten een publieke en een private root. De publieke root CA is aangemeld bij de browserpartijen als Microsoft (voor Internet Explorer) en Google (voor Chrome). Dit betekent dat bezoekers van websites die beveiligd zijn met een PKIoverheid-certificaat, het certificaat automatisch kunnen vertrouwen. In ruil daarvoor dient de eigenaar van de Root CA (Logius) te voldoen aan regelgeving zoals deze door de browserpartijen via het CAB-forum[2] wordt vereist. Deze eisen zijn vooral toegespitst op het gebruik van SSL/TLS-certificaten voor het authentiseren en versleutelen van websites. Om minder afhankelijk te zijn van die eisen is er ook een private root. De certificaten die zijn uitgegeven onder deze root dienen alleen te voldoen aan de reguliere eisen die er aan PKIoverheid-certificaten worden gesteld. Daarbij moet worden aangetekend dat deze certificaten dus niet bruikbaar zijn voor publiek verkeer over het internet omdat deze niet automatisch vertrouwd worden door de browsers. Private servercertificaten zijn daarom gericht op toepassing in besloten gebruikersgroepen. Alle deelnemende partijen dienen dit certificaat dan handmatig te installeren en te vertrouwen. Voorbeelden van besloten gebruikersgroepen zijn het afsprakenstelsel eHerkenning en de Nederlandse Energiemarkt (EDSN).

De maximum geldigheidsduur van servicescertificaten, mits zij publiekelijk worden vertrouwd, is gemaximaliseerd op 2 jaar (825 dagen, inclusief marge). De andere typen PKIoverheid certificaten zijn langer geldig. Zo is de geldigheid van persoonsgebonden certificaten 5 jaar en die van private servicescertificaten 3 jaar.

Een wildcard certificaat beveiligt alle subdomeinen van één domein, ofwel er kunnen meerdere servers worden bediend met één certificaat. Dergelijke certificaten worden niet uitgegeven onder PKIoverheid. Wel mogen er Subject Alternative Name (SAN) velden worden gebruikt in PKIoverheid certificaten. Hierdoor kunnen meerdere subdomeinen in één certificaat worden ondergebracht.

[1] Zie ook toelichting op QWAC: https://www.communicatierijk.nl/vakkennis/r/rijkswebsites/verplichte-richtlijnen/qualified-website-authentication-certificates

[2] Het CA/Browser forum (Certification Authority Browser Forum) is een samenwerkingsverband tussen verkopers van internet browser software (Internet Explorer van Microsoft, Safari van Apple, Firefox van Mozilla, Chrome van Google en Opera) en een groot aantal uitgevers van certificaten, oftewel CA's (waaronder Sectigo (voorheen Comodo), GeoTrust, GlobalSign, Thawte en Symantec). Het forum is in het leven geroepen om standaarden en richtlijnen op te stellen voor certificaten. Meer informatie: https://cabforum.org/.

Naast officiële certificaten zijn er voor testdoeleinden in preproductie-omgevingen ook specifieke PKIo test-certificaten te verkrijgen.

2.3 WAT ZIJN SPECIFIEKE KENMERKEN?

Ten opzichte van 'normale' PKI's onderscheidt PKIoverheid zich als volgt:

- Exclusief keurmerk van de Staat der Nederlanden.
- Gebaseerd op Europese standaarden; de eIDAS verordening.
- Beheer van de standaard door de Rijksoverheid.
- Regie van incidenten of calamiteiten door de Rijksoverheid.
- Actief toezicht op de certificatiedienstverleners door de Rijksoverheid.
- (Verplichte) opname van het Overheid Identificatie Nummer (OIN) in de certificaten.
- Bij een calamiteit/crisis met PKIoverheid certificaten kan de Rijksoverheid hierover zelf de regie nemen. Dit is niet aan de orde bij overige PKI certificaten, waar de regie vooral bij commerciële root CA's ligt. Merk op dat hier ook een afhankelijkheid is met de regiemogelijkheden die het CAB-forum heeft.
- Nadere en eenduidige invulling van betrouwbaarheidseisen die vanuit bestaande wetgeving en standaarden niet zijn ingevuld, bijvoorbeeld aangaande eisen aan Certificate Revocation Lists (CRL).

Daarnaast zijn er meer algemene kenmerken waarin PKIoverheid zich niet onderscheid van een normale PKI:

- Mogelijkheid om een rechtsgeldige elektronische handtekening te zetten.
- Eén digitaal certificaat voor meerdere voorzieningen.
- Interoperabiliteit; alle certificaten zijn gebaseerd op de officiële X.509v3 standaard.

2.4 WIE DOET WAT?

Logius heeft de rol van Policy Authority (PA) van PKIoverheid. De taken van Logius zijn:

- het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader voor PKIoverheid, het zogeheten Programma van Eisen.
- het proces van toetreding door Trust Service Providers (TSP's) tot PKIoverheid begeleiden en voorbereiden van de afhandeling.
- controleren van de werkzaamheden van TSP's die onder de root van de PKIoverheid certificaten uitgeven.[3]

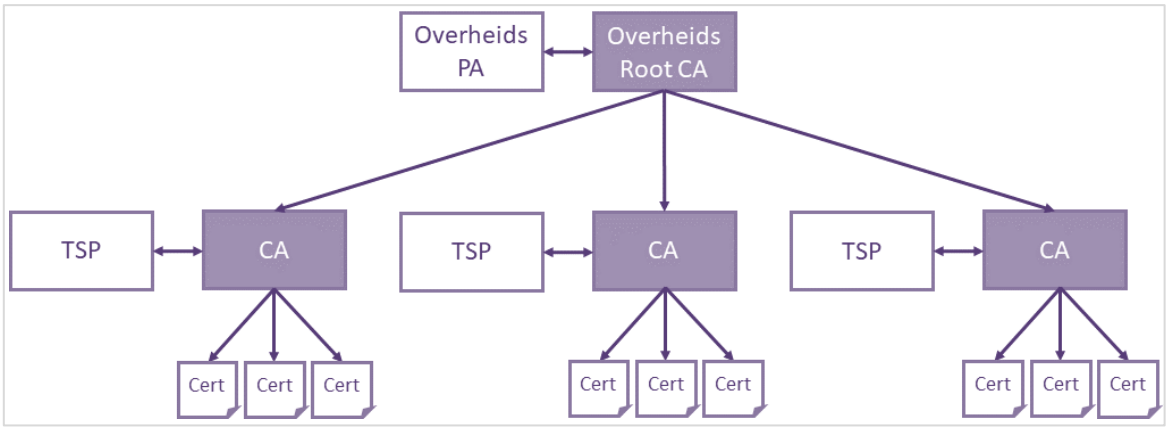
Een PKIoverheid-certificaat kan worden aangeschaft bij een vertrouwensdienstverlener, ofwel een Trust Service Provider (TSP). Een beperkt aantal partijen mag deze certificaten leveren. Op moment van schrijven zijn de volgende TSP's tot de hiërarchie van PKIoverheid toegetreden en verkopen PKIoverheidscertificaten:

- Cleverbase ID
- Digidentity
- ESG[4]
- KPN
- QuoVadis Trustlink
- CIBG (UZI-pas en servercertificaat, ZOVAR servercertificaat)
- Ministerie van Defensie
- Ministerie van Infrastructuur en Waterstaat (Taxi-pas)

Een vertrouwensdienstverlener (TSP) die PKIoverheid-certificaten wil uitgeven dient toe te treden tot de hiërarchie van PKIoverheid. Technisch betekent dit dat de publieke sleutel van de TSP wordt ondertekend door

[3] Logius is formeel gezien geen toezichthouder. Logius is verantwoordelijk voor het opstellen van PvE en heeft een controlerende taak op de partijen die op PKIo zijn aangesloten.
[4] Geeft per 1-1-2017 geen nieuwe certificaten meer uit

het stamcertificaat van PKIoverheid. De TSP krijgt dus een TSP CA-certificaat van PKIoverheid. De PKIoverheid hiërarchie is weergegeven in Figuur 1.



Figuur 2: PKIoverheid hiërarchie.

Voordat een TSP dit certificaat krijgt, gaat PKIoverheid na of de TSP aan alle geldende voorwaarden voldoet. Voor de beslissing over toetreding steunt PKIoverheid op het oordeel van een onafhankelijke auditor. Het gaat daarbij niet alleen om technische maar vooral ook om organisatorische en juridische voorwaarden, zoals vermeld in het Programma van Eisen (PvE, zie hieronder). De meeste TSPs volgen het ETSI normenkader en zij dienen te voldoen aan de eisen zoals gesteld in verordening 910/2014 (eIDAS). Voordat een TSP gekwalificeerde certificaten kan uitgeven, dient een TSP bij de toezichthouder Agentschap Telecom te zijn geregistreerd als uitgever van gekwalificeerde certificaten. Merk op dat deze registratie voor alle certificaten geldt en een wettelijke verplichting is vanuit eIDAS.

Op dit moment zijn er meerdere certificaathiërarchieën PKIoverheid. Na verloop van tijd zijn steeds sterkere algoritmes of andere functionaliteiten nodig om de betrouwbaarheid van certificaten te kunnen garanderen. Alle certificaten binnen eenzelfde hiërarchie zijn gebaseerd op hetzelfde algoritme. De oudste hiërarchie is gebaseerd op het SHA1-algoritme; de nieuwere hiërarchieën op SHA256. De EV-hiërarchie is speciaal ingericht om alleen certificaten voor Extended Validation uit te geven. De nieuwere hiërarchieën van PKIoverheid zijn te herkennen aan een toevoeging in de naam van een certificaat: G3 (de derde generatie), G2 (de tweede generatie) en EV (Extended Validation). Ook zijn er testcertificaten.

Het publieke PKIoverheid-stamcertificaat wordt ondersteund door alle grote browsers.

2.5 CERTIFICATION PRACTICE STATEMENT

In het Certification Practice Statement (CPS) van PKIoverheid staat welke procedures en maatregelen PKIoverheid hanteert bij de uitgifte van de stamcertificaten, het intermediair certificaat, de domeincertificaten en de TSP-certificaten. De Policy Authority geeft de CPS uit.

Het CPS biedt informatie aan vertrouwende partijen en certificaathouders over de manier waarop de dienstverlening van PKIoverheid is ingericht. De kwaliteit van deze dienstverlening ligt ten grondslag aan het vertrouwen dat in het PKIoverheid stelsel kan worden gesteld. Hierbij is ook de relatie met de TSP's van belang. De voorwaarden waaronder TSP's deel kunnen nemen aan het PKIoverheid-stelsel is in het CPS op hoofdlijnen beschreven. TSP’s zullen op basis van de PKIoverheid CPS een eigen CPS moeten maken waarin ze de procedures en maatregels beschrijven die ze in acht nemen bij het verstrekken van PKIo-certificaten.

PKIoverheid is voorzien van het WebTrust-zegel. Die is verleend na een door KPMG uitgevoerde audit van de hiërarchische structuur van de PKIoverheid tegen in de WebTrust-standaard[5] gestelde eisen. Het WebTrust zegel is nodig om in de lijst met vertrouwde certificaten te komen.

2.6 PROGRAMMA VAN EISEN

Hoeksteen van de PKI voor de overheid is het zogeheten Programma van Eisen (PvE). Dit programma is gebaseerd op Europese standaarden en Nederlandse wetgeving. Hiermee kunnen gebruikers erop vertrouwen dat zij gebruikmaken van een kwalitatief hoogwaardige en betrouwbare PKI-infrastructuur, die tevens voldoet aan internationaal geaccepteerde richtlijnen.

Het Programma van Eisen bevat normen ten aanzien van de betrouwbaarheid en kwaliteit van de dienstverlening, de formaten van certificaten en CRL's en de procedures die worden gevolgd als een organisatie als vertrouwensdienstverlener (TSP) wil toetreden tot de PKI voor de overheid.

Het PvE bestaat uit vier delen:

Deel 1. Introductie PvE en PKIoverheid in het algemeen. Er wordt o.a. aangegeven hoe de eisen voor PKIoverheid zijn opgebouwd.
Deel 2. Eisen voor TSPs: :
- hoe treedt een TSP toe tot de PKIoverheid
- hoe toont een TSP conformiteit aan de eisen aan
- aan welke formaliteiten moet een TSP voldoen
- hoe de Policy Authority toezicht houdt op de toegetreden TSP's

Deel 3. Certificate policies, dat wil zeggen de eisen aan de uitgifte van certificaten binnen een bepaald domein (voor handtekening, authenticatie en vertrouwelijkheid). Het bestaat uit de volgende onderdelen: Basiseisen. Aanvullende eisen, Verwijzingsmatrix PKIoverheid en ETSI en de specifieke Certificate Policies voor de verschillende PKIoverheid certificaten.
Deel 4. Toelichting op de definities en afkortingen in het PvE.

2.7 GOVERNANCE

Het stelsel PKIoverheid is eigendom van het ministerie van BZK en heeft tot doel om veilige elektronische communicatie door en tussen overheden te ondersteunen. De verantwoordelijkheid voor het beleid en de strategie voor PKIoverheid ligt bij het ministerie van BZK. Het tactisch beheer van PKIoverheid is belegd bij Logius, een agentschap van het ministerie van BZK. Het tactisch en operationeel beheer van het decentrale deel van PKIoverheid ligt bij meerdere commerciële- en overheidspartijen: de TSP's. Logius stelt, als Policy Authority, in overleg met het ministerie van BZK het Programma van Eisen (PvE) op waar de TSP's aan moeten voldoen. Logius houdt daarnaast ook toezicht op basis van het PKIo PvE. Het ministerie van BZK is hiervan de eigenaar en accordeert wijzigingen erop. Wijzigingen worden altijd eerst met de TSP's besproken. Conformiteit van certificatiedienstverleners met het PvE wordt vastgesteld door onafhankelijke auditors en de door hen opgestelde conformiteitsverklaringen worden door Logius gebruikt als basis voor toelating tot het stelsel. Het toezicht op TSPs die gekwalificeerde certificaten uitgeven is in Nederland belegd bij Agentschap Telecom. De wettelijke basis voor dit toezicht vindt zijn grondslag in de Europese eIDAS verordening voor vertrouwensdiensten. Merk op dat dit geldt voor alle uitgevers van gekwalificeerde certificaten, ongeacht of zij deelnemen aan PKIo of niet.

De sturing op PKIoverheid wordt door het mondiale karakter van internet beperkt. De acceptatie van PKIo-certificaten door de webbrowsers van de Nederlandse gebruikers wordt in de praktijk bepaald door de internationale browserleveranciers (via het CAB-forum). In PKIoverheid hebben zij geen formele rol, maar hun besluiten kunnen wel vergaande implicaties hebben. De afhankelijkheid van wereldwijd opererende browserleveranciers brengt het risico met zich mee dat zij de publieke PKIo-certificaten als onbetrouwbaar kunnen aanmerken. Logius is deelnemer in het CAB-forum en vertegenwoordigt PKIo in de overleggen van het forum over risico-mitigerende maatregelen.

[5] WebTrust is de dominante commerciële standaard om een waardeoordeel te bepalen over de kwaliteit en effectiviteit van een Certificaat Autoriteit. WebTrust vereist een jaarlijkse audit.

3. PKIo in de praktijk

PKIoverheid kent verschillende typen certificaten: website, server, persoons- en beroepsgebonden, zoals toegelicht in het vorige hoofdstuk. Met deze certificaten zijn verschillende toepassingen mogelijk: authenticatie, waarmerken, website beveiliging en server2server communicatie.

In 2017 waren er ca. 658.000 geldige PKIo certificaten (zie Figuur 3). Dat is een groei van ca. 10% t.o.v. 2016. De monitor Generieke Digitale Infrastructuur 2018 geeft geen verklaring voor de groei. Vermoedelijk wordt dit veroorzaakt door eHerkenning en versterking van digitale berichtenstromen via Logius waar PKIo een onderdeel is van de communicatie.

PKIOverheid	2014	2015	2016	2017	%
Aantal uitstaande PKIoverheidscertificaten	676.231	640.216	599.589	657.847	+10

Figuur 3 Aantallen actieve PKIo certificaten (Bron: BZK, Monitor Generieke Digitale Infrastructuur 2018).

In dit hoofdstuk schetsen we het gebruik van PKIo certificaten in de praktijk, gestructureerd naar type certificaat. In de laatste paragraaf geven we een overzicht van de wet- en regelgeving die relevant is voor gebruik van PKIo.

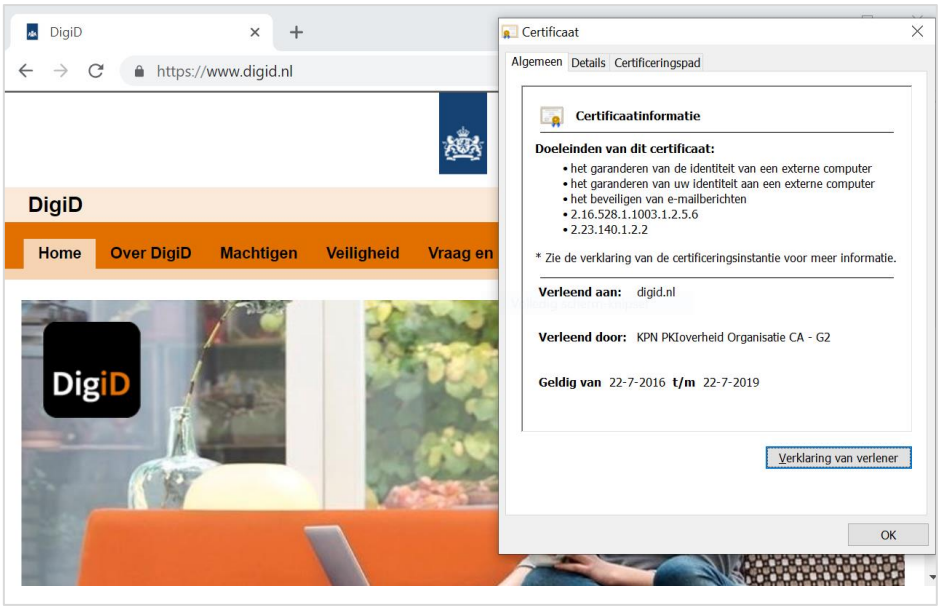
3.1 GEBRUIK WEBSITE CERTIFICATEN

Voor websites in het overheidsdomein worden PKIo SSL certificaten toegepast, maar ook andere certificaten (zoals van QuoVadis, Symantec of Comodo). Onder PKIoverheid worden ook uitgebreid gevalideerde certificaten (Extended Validation Certificates) uitgegeven. Tijdens het validatieproces wordt gecontroleerd of de verbinding met de browser uitkomt op de genoemde website, of de organisatie bevoegd is om de domeinnaam te gebruiken en wordt de organisatie zelf gevalideerd. De laatste validatie betreft zaken als het juridische, fysieke en operationele bestaan van de organisatie. De Uitgebreide Validatie SSL is de meest betrouwbare vorm van SSL; minder uitgebreide vormen zijn Domein Validatie en Organisatie Validatie SSL certificaten.

Een geldig EV-certificaat kan de gebruiker herkennen aan de groene balk of groene letters in de adresbalk. De verschijning is afhankelijk van de browser. Deze optische kenmerken zullen mogelijk in de toekomst verdwijnen. Bijvoorbeeld eHerkenning maakt gebruik van een EV PKIoverheid certificaat. Tevens worden er PKIoverheid Qualified Website Authentication Certificates (QWAC certificaat) uitgegeven, die aan de eIDAS verordening voldoen.

Websites die door het Ministerie van Algemene Zaken worden beheerd zijn standaard uitgerust met een PKIo certificaat. Zie Figuur 4 voor een voorbeeld van een website onder beheer van Algemene Zaken. Merk op dat oudere (mobiele) browser versies (Android) en besturingssystemen niet om kunnen gaan met de nieuwe generatie (G3) EV-SSL PKIo certificaten[6]. Om toegankelijkheid voor een brede gebruikersgroep via verschillende devices en browserversies te garanderen wordt daarom door Algemene Zaken ook wel gekozen voor een gekwalificeerd QuoVadis certificaat met vergelijkbare garanties. Deze situatie wordt echter wel gezien als onwenselijk.

[6] “Het is mogelijk dat sterk verouderde browsersoftware en besturingssystemen PKIo-certificaten niet vertrouwen. In dat geval wordt aangeraden een recentere versie van de software te installeren.” Bron: https://www.logius.nl/diensten/pkioverheid/browserondersteuning.



Figuur 4 Voorbeeld website met Rijksoverheid uitstraling en PKIo.

In de BIR is gebruik van PKIo verplicht als het gaat om beveiliging van web- en mailcommunicatie over gevoelige gegevens, zoals documenten waar rechten aan kunnen worden ontleend. Een website zit in de 'grijze' zone. Algemene informatie kan niet worden bestempeld als gevoelig en dus is PKIo niet aan de orde. Daarentegen als een website persoonlijke dienstverlening faciliteert, bijvoorbeeld via een mijn-omgeving waarop de burger inlogt met DigiD, dan gaat het wel om gevoelige gegevens en is PKIo verplicht. Het lijkt erop dat in de praktijk toepassing van PKIo voor websites voortkomt uit eigen beleid van de overheidsinstelling of dat van de leverancier als beleid ontbreekt of geen onderdeel is van de opdracht.

Er is geen overzicht van verstrekte PKIo certificaten beschikbaar; deze informatie is commercieel gevoelig. Crt.sh is een register waar uitgegeven certificaten kunnen worden gecheckt door te zoeken op domeinnaam. Om een indruk te krijgen van het bereik van toepassing van PKIo website certificaten is steekproefsgewijs gecheckt welke overheidsdomeinnamen certificaten hebben geregistreerd in dit register. Een set van overheidsdomeinnamen is samengesteld uit de Almanak Overheidsdiensten (https://almanak.overheid.nl/) aangevuld met algemene rijksoverheid domeinen (mijnoverheid.nl, overheid.nl), keten- en centrale dienstverlening (BKWI, Inlichtingenbureau, GBI gemeenten, omgevingsloket, ….) en voorzieningen zoals genoemd in de monitor Open standaardenbeleid van ICTU over 2016 en 2017.

Tabel 1 geeft een overzicht van geregistreerde PKIo website certificaten uitgesplitst naar type overheidsorganisatie (toetsperiode 15-20 nov 2018).

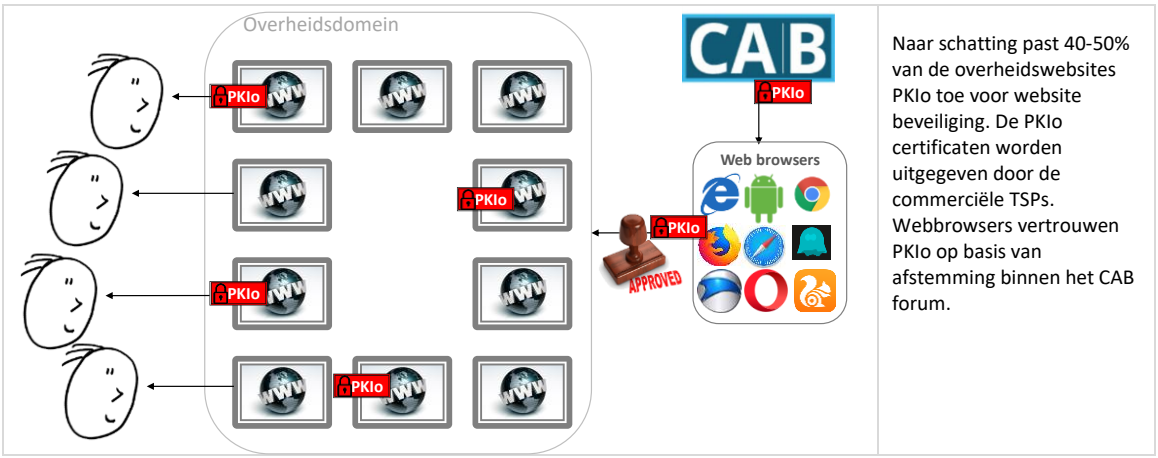
Tabel 1 Overzicht toepassing website-PKIo in het overheidsdomein.

Overheidsorganisatie	Totaal	Steekproef	Aantal in de steek-proef met geldig PKIo certificaat	Percentage geldig PKIo certificaat
Departement	6	100%	0	0%
Uitvoeringsorganisatie	67	39%	16	62%
Voorzieningen	15	100%	9	60%
Provincie	12	100%	2	17%
Gemeente	383	31%	74	62%
Gemeenschappelijke regeling	305	32%	17	17%
Ketenpartner	5	100%	4	80%
Hoge Colleges van Staat	7	100%	1	14%
Rechterlijke macht	2	100%	2	100%
Politie en Brandweer	3	100%	1	33%
Adviescollege	10	100%	1	10%
Beroepsorganisaties	5	100%	0	0%
Waterschap	22	100%	2	9%
Zelfstandig bestuursorgaan	94	39%	11	30%
TOTAAL	**936**		**140**	**38%**

Uit de analyse blijkt dat ‘slechts’ 38% van de domeinen uit de steekproef van 936 domeinen beveiligd is met een PKIo certificaat. Een kanttekening is dat een aantal rijksoverheidsdomeinen tijdelijk een ander certificaat gebruikt vanwege browserproblemen met de huidige generatie PKIo website certificaten, wat het gemiddelde iets omlaag brengt. Verder beperkt crt.sh zich tot publieke certificaten. Een andere kanttekening is dat er naar het hoofddomein wordt gekeken en niet naar subdomeinen die wellicht wel PKIo toepassen, bijvoorbeeld voor het ontsluiten van een portal waar DigiD wordt gebruikt. Dit zien we niet terug in de cijfers.
Vooral bij uitvoeringsorganisaties, gemeenten en hun gemeentelijke regelingen en ZBO’s is de toepassing van PKIo voor websitebeveiliging laag. Gemeentes zijn door het huis van Thorbecke vrij om al dan niet te kiezen voor PKIo-certificaten. De BIR is niet van toepassing voor ZBO’s, dus ook zij zijn vrij om andere certificaten dan PKIo te kiezen.

Het gebruik van niet-gekwalificeerde certificaten (die dus niet onder PKIoverheid vallen), bijvoorbeeld voor gemeentelijke websites, brengt het risico met zich mee dat de kans op incidenten groter is dan noodzakelijk. Gebruik van gekwalificeerde maar niet PKIo certificaten wordt in het geval van een incident niet via PKIoverheid beheersbaar gemaakt, maar door de internationale gemeenschap of middels een nationale crisissituatie.

Samenvattend: Binnen het overheidsdomein worden in beperkte mate PKIo-website certificaten toegepast. De schatting is rond de 40% van de websites (zie ook Figuur 5). In de BIR is PKIo verplicht wanneer het gaat om communicatie over gevoelige gegevens. Websites die digitale dienstverlening faciliteren zullen in de regel communiceren over gevoelige gegevens. Hieronder valt digitale dienstverlening door gemeentes, provincies, gemeentelijke regelingen, waterschappen en uitvoeringsorganisaties, waar de toepassing van PKIo beperkt is. We schatten dat voor 80% - 90% van de overheidswebsites geldt dat er dienstverlening aan burgers of bedrijven wordt geleverd en dat er derhalve een verdubbeling van PKIo certificaten voor websites mogelijk is.



Figuur 5 Toepassing van PKIo SSL certificaten in het overheidsdomein.

3.2 GEBRUIK SERVERCERTIFICATEN

Verplichting van het gebruik van een PKIo server certificaat wordt vaak opgelegd door de dienstverlener aan afnemers die gebruik willen maken van een server-koppeling. Als de dienstverlener een PKIo server-certificaat niet verplicht dan wordt er een ander certificaat gekozen, bijvoorbeeld een wildcard-certificaat van Comodo. Ook voor servercertificaten zijn eisen van de BIR van toepassing: PKIo verplicht toepassen wanneer het gaat om web- of mailverkeer over gevoelige gegevens.

Ook in bepaalde afsprakenstelsels voor gegevensuitwisseling zoals eHerkenning en MedMij is het gebruik van PKIo door de deelnemers verplicht.

Standaarden voor gegevensuitwisseling met de overheid, zoals Digikoppeling, eisen ook PKIo-certificaten voor het koppelen op Digipoort. Digipoort is een centrale voorziening in de infrastructuur van de e-overheid, waarop overheden en bedrijven kunnen aansluiten om gemakkelijk en betrouwbaar gegevens met elkaar te kunnen

uitwisselen. Via Digipoort kunnen partijen berichten aanleveren voor onder meer het CBS, Kamer van Koophandel, UWV, Belastingdienst, Douane, Voedsel- en Warenautoriteit, De Nederlandse Bank en ook voor digitaal factureren naar ongeveer 70 Ministeries en haar dienstverleners en vele lagere overheden. Zie overzicht in Tabel 2 voor de Digipoort diensten. Hierbij is het Organisatie Identificatie Nummer belangrijke identifier voor de authenticatie/authorisatie voor dienstverlening. Elk PKIoverheid server certificaat in gebruik voor Digipoort/Digikoppeling bevat daarom een OIN.

Tabel 2 Dienstverlening via Digipoort (Bron: Logius - https://www.logius.nl/diensten/digipoort).

Overheidsdienst	Gebruiker	Voor:
Douane	Bedrijven	O.a. uitvoer, aangiftebehandeling AGS, vervoer, EMCS accijns, CID informatie
Grensbewaking	Bedrijven	Melding personen aan boord
Rijkswaterstaat	Bedrijven	O.a. meldingen aankomst / vertrek schip, stoffen, afval, inspectie
NVWA	Bedrijven	VWA cliënt, PD cliënt, e-logboek visvaartuigen
Belastingdienst	Bedrijven	Teruggaveverzoek BTW, grootwagenpark motorrijtuigenbelasting, country-by-country reporting
Belastingdienst	Fin. instellingen	Opgave diverse financiële producten
DNB	Fin. instellingen	Div. rapportages
UWV	Werkgevers	Verzuimrapportages en betermeldingen
KvK	Bedrijven	Jaarrekening
CBS	Overheden en bedrijven	Statistiekopgaven
SBR-wonen	Woningcorporaties	Prognose informatie
OCW	Onderwijsinstellingen	Jaarverantwoording

Digikoppeling van Logius ontsluit 20 diensten van verschillende overheidsorganisaties – zie Tabel 3.

Tabel 3 Voorzieningen via Digikoppeling (Bron: Logius - https://www.logius.nl/diensten/digikoppeling/landelijke-voorzieningen).

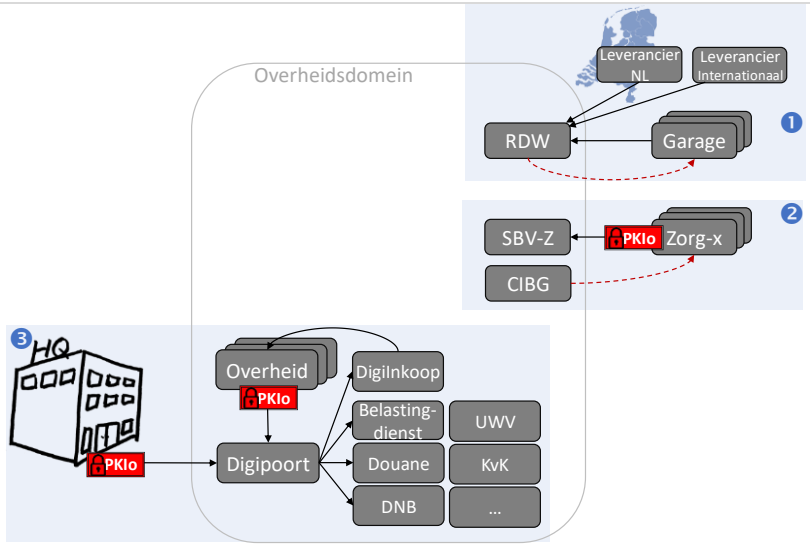
Organisatie	Voorziening
Justitie	CORV
Kadaster	BAG bevragen & mutaties, BRK levering mutaties, LVWOZ bevragen & levering
KvK	HR Dataservice (berichten)
Logius	DigiInkoop, Digilevering, E-factureren, MijnOverheid Berichtenbox, Lopende Zaken en WOZ inzage.
Ministerie van I&M	Omgevingsloket Online
Ministerie van I&M/Kadaster	BGT
RDW	BRV
RVO	MijnOverheid Berichtenbox Antwoord voor Bedrijven
VNG/Inlichtingenbureau	GGK WMO, Jeugdwet & WLZ toets

Ook Logius-voorzieningen als DigiD maken gebruik van PKIo-certificaten.

Voor dienstverlening zonder betrokkenheid van Logius is toepassing van PKIo voor server-to-server communicatie vaak afhankelijk van het beleid van de dienstleverancier. Zo kiest RDW ervoor om een eigen certificaat uit te geven aan leveranciers en garages. Het zelfde geldt bijvoorbeeld voor DUO aangaande koppelingen met leerling administratie of student informatie systemen bij onderwijsinstellingen[7] en Justid betreffende de strafrechtketen. Voor het zorg-domein (UZI-pas) is PKIo verplicht bij wet omdat er wordt

[7] DUO geeft een eigen ODOC-certificaat af aan geregistreerde onderwijsinstellingen voor veilige informatie-uitwisselen met de DUO voorzieningen als BRON. Zie https://duo.nl/zakelijk/primair-onderwijs/softwareleveranciers/softwareleveranciers-las.jsp.

bijzondere persoonsgegevens worden uitgewisseld (gezondheidsgegevens, BSN). In Figuur 6 werken we een aantal voorbeelden van gebruik van PKIo uit.



❶ RDW erkent (auto)leveranciers en garages. Deze bedrijven zijn in Nederland, maar ook buiten Nederland gevestigd. Erkende bedrijven ontvangen een eigen RDW-root servercertificaat om bijv. keuringen te melden.

❷ Erkende zorgverleners en zorgorganisaties kunnen een UZI-pas servercertificaat aanvragen. Zorgverzekeraars een ZOVAR certificaat. Deze wordt uitgegeven door CIBG. Met dit PKIo certificaat kan toegang worden verkregen tot SBV-Z voor BSN informatie.

❸ Bedrijven en overheden die berichten via Digipoort inschieten naar een overheidsdienst, communiceren met een PKIo servercertificaat. Dit certificaat wordt in het algemeen geleverd door een commerciële TSP.

Figuur 6 Gebruik van PKIo server certificaten

Gemeenten zijn grootgebruikers als het gaat om raadplegen en registeren, bijv. Jnet, KvK, BRP/RNI of Kadaster. Een schatting is 20-30 diensten per gemeente. Veel van deze diensten vragen een PKIo certificaat. Meestal heeft elke koppeling een eigen PKIo certificaat omdat een certificaat gekoppeld is aan een specifieke server die je gebruikt en je van te voren niet weet welke domeinnamen je gaat gebruiken. Het vereist in ieder geval een gedegen certificatenbeheer bij een gemeente.

Voor servercertificaten moet worden opgemerkt dat deze voor zowel websites als voor server-to-server communicatie kunnen worden gebruikt. Hergebruik van een certificaat voor beide toepassingen is mogelijk. De keuze hiervoor ligt bij de afnemer zelf.

Samenvattend: Of een PKIo servercertificaat verplicht is wordt bepaald door de dienstverlenende organisatie. Logius verplicht altijd PKIo voor diensten die zij faciliteren en heeft het OIN in de dienstverlening geïntegreerd. In andere gevallen wordt serverauthenticatie ook wel geregeld door een ‘eigen-root’ certificaat die is gekoppeld aan erkenningstraject (bijv. erkende garage, erkende onderwijsinstelling). PKIo servercertificaten worden uitgegeven door een commerciële TSP (KPN, Digidentity of QuoVadis) of de overheidsorganisatie is zelf de CA (Defensie, VWS, I&W). In de BIR wordt PKIo verplicht voor communicatie van ‘gevoelige’ gegevens. Ook Encryptiebeleid gemeenten beveelt beveiliging met PKIo aan. Desondanks wordt PKIo niet overal toegepast.

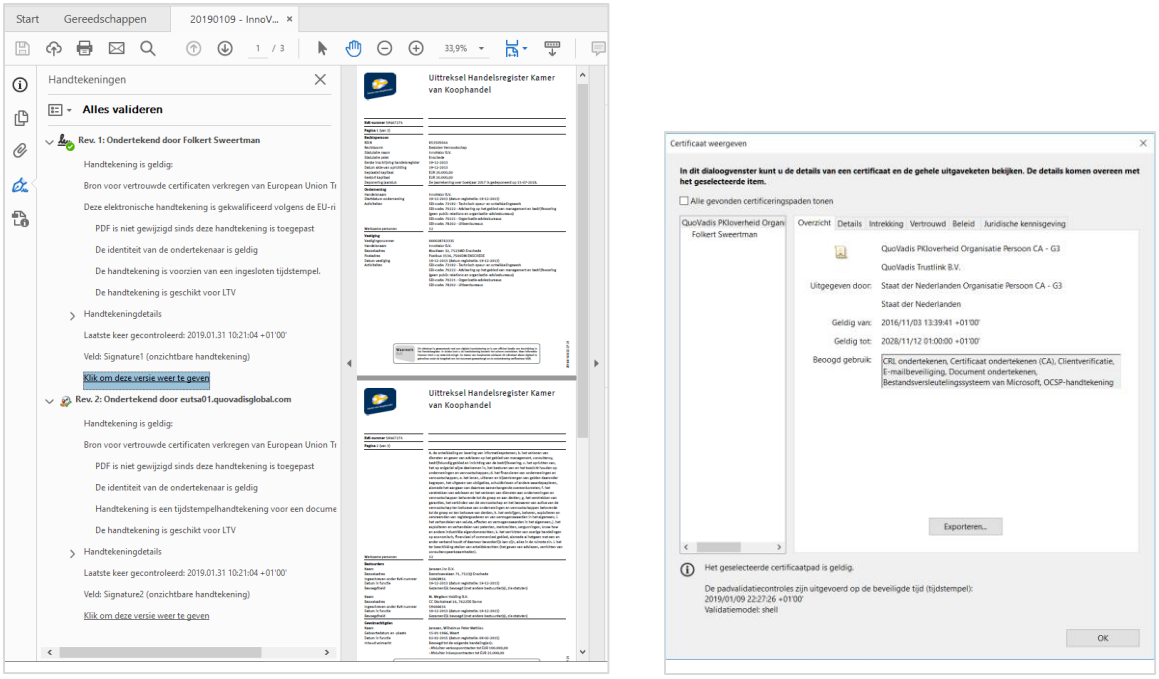
3.3 GEBRUIK PERSOONLIJKE CERTIFICATEN

Persoonlijke certificaten worden gebruikt voor authenticatie en elektronisch ondertekenen van berichten en documenten. Sommige overheidsinstellingen passen hiervoor PKIo overheid certificaten uitgegeven door een commerciële provider of via de eigen CA. Andere overheidsinstellingen hanteren een eigen-root PKI. Bijvoorbeeld voor het Ministerie van J&V regelt Justid de uitgifte en beheer van PKI certificaten voor alle onderdelen. Hiermee is specialistische kennis en kunde gecentraliseerd en worden de onderdelen ontlast. Voor interne communicatie wordt een interne eigen root PKI gehanteerd vanuit kostenoverwegingen. Het aanschaffen en jaarlijks vernieuwen van een PKIo certificaat voor alle 1.000-en J&V medewerkers is namelijk te kostbaar gegeven de prijs van een PKIo certificaat. Voor externe communicatie wordt wel een PKIo certificaat toegepast. Deze wordt betrokken van een commerciële provider. Defensie gebruikt persoonsgebonden PKIo certificaten op de Defensie-pas en is daarvoor zelf de CA om te kosten te beperken. Andere voorbeelden van persoonsgebonden PKIo-certificaten zijn de UZI-pas in de zorg en de Taxipas. De UZI-pas wordt bijvoorbeeld gebruikt bij het elektronisch ondertekenen van een digitaal geneesmiddelrecept of een digitaal verslag van een

ziekenhuisopname. Zorgverleners kunnen zo veilig elektronische patiëntgegevens uitwisselen. De Taxipas voor de boordcomputer van de taxi identificeert de bestuurder en registreert de rij- en rusttijden.

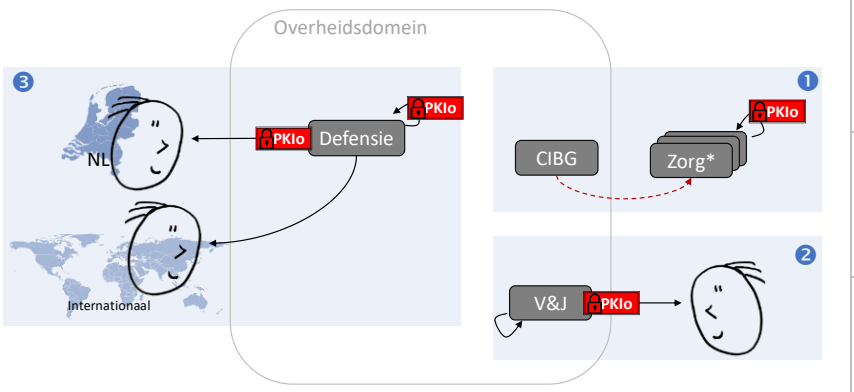
Waarmerken

Waarmerken gaat over het digitaal ondertekenen van documenten. Het digitaal ondertekenen vereist een PKI-certificaat. Bijvoorbeeld binnen de strafrechtketen worden beschikkingen en uitspraken gewaarmerkt met een PKIo persoonlijk certificaat wanneer deze buiten het J&V domein gecommuniceerd worden. Wanneer stukken binnen de keten blijven wordt er met het eigen J&V-certificaat gewaarmerkt. Organisaties als DUO en KvK kiezen ervoor om te waarmerken met PKIo-certificaten. Merk op dat KvK een ZBO is, waarvoor de BIR niet geldt en dus PKIo niet verplicht is. Bijvoorbeeld voor diploma's uit het diplomaregister en uittreksels uit het handelsregister. De handtekening kan worden geëvalueerd in de Adobe PDF reader, zie Figuur 7 voor een voorbeeld van een gewaarmerkt document. Merk op dat het waarmerk in dit voorbeeld is gebaseerd op een persoonlijk PKIo-certificaat op naam van een functionaris van KvK. Een eigendomsinformatiedocument van het Kadaster is daarentegen weer niet digitaal gewaarmerkt.



Figuur 7 Validatie van de digitale handtekening op een KvK-gewaarmerkt document met een PKIo-certificaat.

In Figuur 8 schetsen we enkele typische gebruikstoepassingen van PKIo-certificaten voor waarmerken.



❶ CIBG geeft een persoonlijke UZI-pas uit aan erkende zorgverleners en zorgorganisaties. Hiermee wordt bijv. onderlinge communicatie ondertekent, bijv. huisarts recept richting apotheek.
❷ In de interne J&V keten worden interne berichten met een eigen PKI ondertekent. Berichtgeving buiten de keten wordt door een PKIo certificaat gewaarmerkt.
❸ Defensie is CA voor de eigen PKIo certificaten. Deze worden toegepast voor waarmerken van zowel interne als externe berichten voor NL. Internationaal is de waarde van PKIo ook belangrijk, omdat het leunt op NL wetgeving en daarmee een invulling is van de wet.

Figuur 8 Gebruik van persoonlijke en beroepscertificaten voor waarmerken.

Samenvattend: Voor het waarmerken van berichten binnen het overheidsdomein worden zowel intern uitgegeven certificaten gebruikt als PKIo certificaten, uitgegeven door zowel commerciële TSPs als interne overheids-TSPs. Buiten het overheidsdomein wordt waarmerken met PKIo verplicht voor zorgverleners op basis van de UZI-pas met PKIo certificaat te gebruiken om onderlinge communicatie tussen zorgverleners / zorgorganisaties te waarmerken. Ook uittreksels uit de registers van DUO en KvK zijn met PKIo gewaarmerkt. Waarmerken is vooral relevant voor documenten en berichten waar de ontvanger en eventuele derden rechten aan kunnen ontlenen. De BIR is hier duidelijk over: PKIo is verplicht.

Authenticatie

Naast waarmerken worden persoonlijke certificaten toegepast voor authenticatie om toegang te krijgen tot diensten via mijn-omgevingen, voor toegang tot kantoor-ICT of voor toegang tot gebouwen en locaties. Authenticatie middelen zijn zeer divers, soms met PKIo, soms niet. De defensie-pas bevat persoonsgebonden PKIo-certificaten waarmee de gebruiker zich kan authentiseren. PKIo-certificaten hebben hun weg nog niet gevonden naar de Rijkspas door kosten en organisatorisch overwegingen. Rijkspas hanteert nu authenticatie certificaten uitgegeven onder een PKI van EZ. De UZI-pas authentiseert de zorgprofessionals en is op basis van PKIo. Het zelfde geldt voor de Taxipas. Qua betrouwbaarheidsniveau zijn op PKIo certificaten of, meer algemeen, op gekwalificeerde certificaten gebaseerde authenticatieoplossingen te classificeren als Hoog.

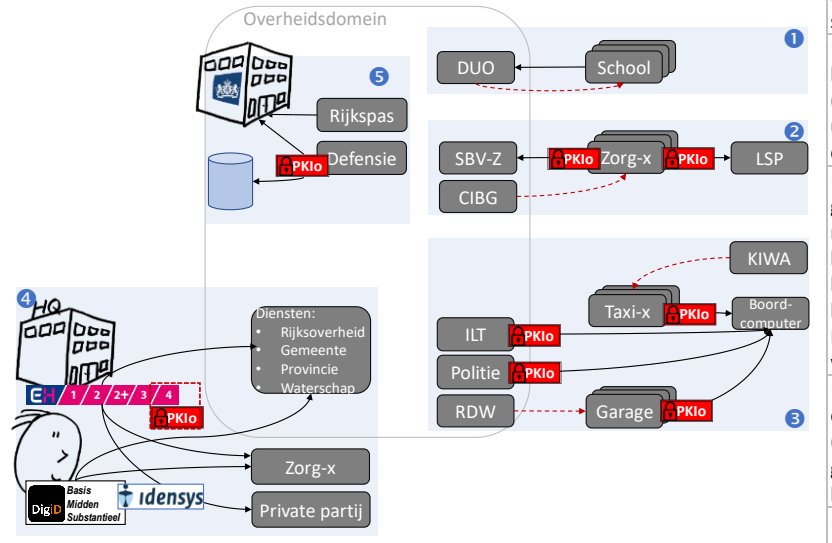
Daarnaast zijn er in Nederland diverse authenticatievoorzieningen voor het publieke domein zoals eHerkenning, Idensys en DigiD. Verstrekte eHerkenning- en Idensysmiddelen op het hoogste betrouwbaarheidsniveau zijn vaak gebaseerd op PKIo-certificaten. De onlangs stopgezette pilot met iDIN maakte geen gebruik van PKIo-certificaten. Figuur 9 illustreert de variëteit in authenticatie voor overheidsdiensten.

Ondanks dat de markt voor authenticatiemiddelen groot is, is het PKIo-aandeel hierin op dit moment relatief klein. Er zijn andere middelen, als DigiD, die onder burgers een veel grotere dekkingsgraad genieten en daardoor goedkoper en gewilder zijn bij overheidsorganisaties. DigiD telde in 2017 13.5 miljoen gebruikers die 280 miljoen keerde inlogden bij 623 aangesloten organisaties[8]. Daarnaast werkt het Ministerie van BZK hard aan het verhogen van de betrouwbaarheid van DigiD. DigiD Substantieel op basis van een mobiele app en een paspoort scan met NFC is operationeel en zal de SMS variant vervangen. Er lopen pilots met DigiD Hoog waarbij het rijbewijs als tweede authenticatiefactor dient. Bij eHerkenning genieten middelen op niveau eH3 in toenemende mate de voorkeur; deze middelen zijn niet gebaseerd op PKIo. Uit de stelselrapportage voor het Tactisch Beraad van december 2018 blijkt dat er 307 middelen op niveau 4 zijn die bij 403 aangesloten dienstaanbieders gebruikt kunnen worden[9]. Al deze middelen zijn gebaseerd op PKIo of gekwalificeerde certificaten. Mogelijk redenen voor de beperkte adoptie van dergelijke middelen zijn de kosten ervan en het feit dat er (nog) nauwelijks diensten zijn die niveau 4 of Hoog vereisen. Ook speelt mee dat gebruikers zich

[8] Logius 2017 jaarverslag, zie https://publicaties.logius.nl/nl/magazine/12019/823527/digid.html.
[9] Vergaderstukken tactisch beraad, zie https://www.eherkenning.nl/over-eherkenning/tactisch-beraad/.

fysiek moeten identificeren als onderdeel van het uitgifteproces van de certificaten; dit werkt drempelverhogend.

In 2017 tekenden een aantal grote overheidsuitvoerders, waaronder UWV, RDW, KvK en Belastingdienst, een intentieverklaring waarin ze aangaven eHerkenning te gaan gebruiken. Inmiddels zijn diverse van deze organisaties aangesloten. Daarnaast zijn er in het consumenten-domein oplossingen als iDIN die relatief betrouwbaar zijn en een hoge dekkingsgraad kennen.



❶ DUO geeft een eigen ODOC-certificaat aan af aan geregistreerde onderwijsinstellingen die daarmee kunnen inloggen in de DUO omgeving (b.v. BRON-systeem).

❷ Met de UZI-pas of servercertificaat kunnen zorgverleners inloggen op SBV-Z (overheidsdomein) of LSP. De pas wordt uitgegeven door CIBG en bevat een PKIo certificaat.

❸ De taxi-pas wordt uitgegeven aan geregistreerde taxichauffeurs voor rijtijdenadministratie op de boordcomputer. Politie, ILT en Garages kunnen toegang krijgen tot de boordcomputer met een eigen Taxi-pas. De Taxi-pas bevat een PKIo certificaat en wordt uitgegeven door KIWA.

❹ Voor digitale dienstverlening van de overheid is inloggen met DigiD of Idensys (personen) of eHerkenning (bedrijven) gebruikelijk. Alleen eHerkenning niveau 4 bevat een PKIo certificaat.

❺ Toegang tot gebouwen en kantoor-IT regelt Defensie met een PKIo-Defensie pas die door henzelf wordt verstrekt. De Rijkspas geeft toegang tot gebouwen en bevat geen PKIo maar een PKI onder de vlag van Min. EZ. De Rijkspas wordt uitgegeven via HR.

Figuur 9 Gebruik van persoonlijke en beroepscertificaten voor authenticatie.

Samenvattend: Er is geen duidelijk beleid m.b.t. toegang tot overheidsdiensten, er is een grote variëteit aan authenticatiemiddelen. Algemene digitale overheidsdienstverlening maakt gebruik van DigiD en eHerkenning voor het authentiseren van respectievelijk burgers en bedrijven. Er is in het overheidsdomein gepilot met Idensys en iDIN. Steeds meer maken organisaties daarbij gebruik van betrouwbaarheidsniveaus zoals gedefinieerd door eIDAS en de handreiking hiervoor van het Forum Standaardisatie. eHerkenning op het hoogste betrouwbaarheidsniveau is vaak gebaseerd op PKIo-certificaten, maar dit niveau kent slechts een beperkt aandeel in alle uitgegeven eHerkenningsmiddelen. Domein-specifieke diensten, bijvoorbeeld RDW, zorgdomein, Defensie, Rijkspas of Taxipas, verstrekken eigen middelen waar PKIo een element kan zijn. Ook hier geeft de BIR aanleiding om een breder gebruik van PKIo te verwachten. Wanneer authenticatie nodig is, gaat het daarna om specifieke dienstverlening waar de gebruiker rechten aan kan ontlenen. De BIR zegt dat voor dergelijke toepassingen PKIo verplicht is.

3.4 WET- EN REGELGEVING

Hieronder volgt een beknopt overzicht (niet uitputtend) van wet- en regelgeving relevant voor gebruik en toepassingen van PKIoverheid:

- In het **Encryptiebeleid gemeenten** (VNG Realisatie, 2014) staat dat gemeenten PKIoverheid-certificaten (paragraaf 2.2.) zouden moeten toepassen. Er wordt gesteld dat encryptie moet plaatsvinden conform de PKIoverheid standaard, dat gebruik moet worden gemaakt van de PKIoverheid-certificaten voor teken en/of encryptie van digitale documenten van de gemeente waar

burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van de PKIoverheid-certificaten voor tekenen en/of encryptie.

- Europese **eIDAS verordening** over elektronische identiten en vertrouwensdiensten. eIDAS is de algemene benaming voor de EU-verordening (EU) nr 910/2014 die nieuwe regels voor elektronische identificatie en vertrouwensdiensten vaststelt voor elektronische transacties binnen de Europese Unie. eIDAS vervangt de vorige Richtlijn 1999/93/EG, die meer specifiek gericht was op elektronische handtekeningen. Door de certificering van aanbieders van vertrouwensdiensten (Trust Service Providers, TSPs), streeft de eIDAS regulatie naar het verhogen van de interoperabiliteit en rechtszekerheid in grensoverschrijdende online transacties en het bevorderen van een "digitale interne markt" binnen de EU. Binnen eIDAS gekwalificeerde TSPs en hun diensten hebben in alle lidstaten dezelfde status en middelen worden door alle lidstaten erkend wanneer het notificatieproces is doorlopen. Sommige gekwalificeerde TSPs geven ook PKIo certificaten uit.
- De concept **Wet Digitale Overheid** gaat vooral over de toegang van burgers en bedrijven tot online dienstverlening bij de (semi)overheid. PKIoverheid valt hier buiten scope, maar desgewenst is het mogelijk om in deze wet een haakje richting beveiliging van communicatie voor dienstverlening te slaan.
- De **BIR 2017** betreft veiligheidseisen. De BIR stelt dat gebruik moet worden gemaakt van PKIoverheid certificaten bij web- en mailverkeer van gevoelige gegevens, zoals digitale documenten waar rechten aan kunnen worden ontleend, om zekerheid te bieden over de integriteit. De BIR gaat over gegevens op niveau 'departementaal vertrouwelijk'. Voor hogere vertrouwelijkheidsniveaus (d.w.z. confidentieel & (zeer) geheim) moet voor elke casus een afweging worden gemaakt of PKIo wenselijk is.
- **Webrichtlijnen 2018 / DigiToegankelijk** regelt dat websites in het (semi-)overheidsdomein voor iedereen toegankelijk zijn en moeten verplicht worden toegepast. De regels gaan in op techniek en vormgevingselementen die ervoor zorgen dat gebruikers de inhoud kunnen begrijpen en toepassen.
- **Handreiking betrouwbaarheidsniveaus** van Forum Standaardisatie. De handreiking adviseert in betrouwbaarheidsniveaus voor machtigingen, communicatie tussen applicaties, retourstromen, eenmalig inloggen en ondertekenen. De handreiking promoot toepassing van algemeen inzetbare oplossingen waaronder PKIoverheid voor authenticatie door personen. Voor applicatie-applicatieverkeer gaat het vooral over betrouwbaarheid en is PKIoverheid de verplichte standaard, waarbij wordt verwezen naar de BIR.
- **Europese Netwerk en Informatiebeveiliging** (NIB) richtlijn (2016/1148) en de hiervan afgeleide nationale Wet beveiliging netwerken informatiesystemen (Wbni) om de weerbaarheid van netwerk- en informatiesystemen te vergroten.
- In de **Wet Markt en Overheid** wordt geregeld dat dienstverlening door de overheid niet de markt mag verstoren. Relevantie van deze wet voor PKIo betreft de uitgifte van middelen door TSPs. In de huidige situatie zijn er zowel publieke als private TSPs. Als een overheidsTSP een meer prominente positie zou krijgen in het uitgifte proces, dan kan dat invloed hebben op de markt.

3.5 SCOPE

Hoewel de toepassing van PKIo het overheidsdomein betreft, is het verbreden van deze scope geen vreemde gedachte. Bijvoorbeeld naar de vitale sectoren alwaar informatiebeveiliging een steeds belangrijkere rol speelt zo blijkt wel uit de onlangs in werking getreden Wet beveiliging netwerk- en informatiesystemen[10]. Wbni is de vertaling van de Europese Netwerk- en Informatiebeveiliging Richtlijn, de NIB-Richtlijn.

Het feit dat PKIo-certificaten voor de vitale sectoren niet verplicht zijn, brengt het risico met zich mee dat elektronische communicatie binnen deze sectoren niet de beveiliging krijgt die vanuit het maatschappelijk belang wenselijk is. De overheid kan bovendien niet gemakkelijk ingrijpen om de maatschappelijke impact te beperken.

Het breder inzetten van PKIo biedt niet alleen extra veiligheidsgaranties maar zal ook zorgen voor een verlaging van de kosten van de certificaten door schaalgroottevoordelen.

[10] Zie bijvoorbeeld https://www.agentschaptelecom.nl/documenten/publicaties/2018/09/26/brochure-algemene-informatie-wet-beveiliging-netwerken-informatiesystemen-wbni.

3.6 CONCLUSIE

Ondanks dat de BIR en het Encryptiebeleid gemeenten in veel situaties PKIo certificaten verplicht stellen in de communicatie, wordt PKIoverheid nog niet in de volle breedte toegepast. Voor website beveiliging is toepassing van PKIoverheid afhankelijk van het beleid van de overheidsorganisatie en/of van de leverancier. Websites onder beheer van het Ministerie van Algemene Zaken hebben standaard PKIo. Ongeveer 40% van de overheidsdomeinen past een PKIo certificaat toe. Een specifiek probleem hier is de nieuwe generatie PKIoverheid certificaten (EV) mismatcht met oudere browserversies.

Toepassing van PKIoverheid voor server-to-server communicatie hangt af van de eisen die de dienstverlener aan de gebruikende partij stelt. Logius diensten verplichten vaak PKIo servercertificaten, andere diensten niet per se. Grootgebruikers van diensten, zoals gemeenten, hebben meerdere PKIo-certificaten nodig en gebruiken daarnaast ook andere PKI-certificaten.

Persoonlijke certificaten (en beroepscertificaten) worden toegepast voor waarmerken en authenticatie. Ook hier zien we verschillende manieren van toepassen. Bij Defensie wordt de Defensiepas toegepast voor authenticatie en waarmerken met daarop een PKIo certificaat. Als het gaat om het waarmerken van documenten lijken overheidsorganisatie over het algemeen te kiezen voor PKIo-certificaten of zien ze hier volledig van af. Ministerie van J&V kiest ervoor om een eigen waarmerk te gebruiken voor interne communicatie en bij externe communicatie voor een waarmerk met PKIo. Bij authenticatie voor dienstverlening geldt dat voor breed toegankelijke algemene dienstverlening voor bedrijven en personen meestal DigiD of eHerkenning wordt toegepast. Voor domeinspecifieke dienstverlening (bijv. RDW, DUO, Taxi, Zorg) wordt een eigen authenticatie middel uitgegeven. Sommige van deze middelen bevatten PKIo, anderen niet.

4. SWOT

In de periode december 2018 – januari 2019 zijn er interviews gehouden met afnemers van PKIo, niet-afnemers, leveranciers en domeinexperts. Voor een overzicht van geïnterviewde organisaties zie bijlage 1. Tijdens de interviews vroegen we naar specifieke toepassingen van PKIo binnen de organisatie, welke voordelen werden ervaren, eventuele nadelen en belemmeringen, mening ten aanzien van verbreding van toepassing van PKIo, verplichting als maatregel om gebruik van PKIo te vergroten, mogelijkheden voor verplichting en consequenties die verplichting met zich mee zou brengen. Een aantal inzichten zijn verwerkt in de hoofdstukken 2 en 3.

In dit hoofdstuk gaan we in op het gebruik van PKIo, deze presenteren in de vorm van een SWOT waarin we voor PKIo in het algemeen en toepassing voor de vier toepassingsdomeinen een overzicht geven van sterke en zwakke punten, kansen en bedreigingen zoals die in de interviews naar voren kwamen. De onderwerpen die uit de SWOT analyse naar voren komen zijn besproken in een expertconsultatie. Aan de expertconsultatie namen 15 personen deel vanuit 10 organisaties (zie bijlage 2).

De SWOT analyse biedt aanknopingspunten om het onderwerp van de analyse te versterken, bijvoorbeeld door:

- Te zorgen dat sterke punten behouden blijven of worden versterkt;
- Te bekijken hoe de zwakke punten kunnen verminderen;
- Maatregelen die kansen benutten;
- Maatregelen die risico's van bedreigingen verminderen.

In paragraaf 4.1 gaan we in op het PKIo stelsel in het algemeen en bespreken we de balans tussen voor- en nadelen. In de paragrafen daarna gaan we in op de specifieke toepassingen van PKIo, waar aanvullende aandachtspunten uit volgen.

4.1 PKIo ALGEMEEN

De eerste SWOT analyse betreft het gehele PKIo stelsel. Het gaat in op de voor- en nadelen die de geïnterviewde stakeholders ervaren voor het stelsel als geheel en de kansen en bedreigingen voor toekomstig gebruik. In het algemeen is men gecharmeerd van PKIo. De staat der Nederlanden staat erachter en het zorgt voor betrouwbare dienstverlening en communicatie. Het straalt vertrouwen uit, zeker in de communicatie met overheidsorganisaties in het buitenland. Er is zeker draagvlak om PKIo gebruik te willen vergroten PKIo wordt in het algemeen gezien als de impliciete of zelfs verplichte standaard.

Veel geïnterviewden geven aan dat het opmerkelijk is dat er veel publieke middelen in PKIo worden gestoken (in stand houding van het stelsel) en dat het vreemd is dat de overheid het niet zelf altijd gebruikt. Toch zijn er ook andere geluiden. Als tegenhanger wordt ook gesteld dat toepassing van PKIoverheid wordt belemmerd door bijvoorbeeld onbekendheid, hoge kosten, beperkte scope en onduidelijke beveiligingsmeerwaarde. Het stelsel wordt beschouwd als complex, waarbij soms de pragmatische/praktische invulling van eisen wat uit het oog wordt verloren. Een andere beperking is de focus op de Nederlandse context die internationale harmonisatie zoals beoogd door eIDAS en communicatie over de grens in de kan weg zitten. De geclaimde onderscheidende eigenschappen van PKIoverheid zoals beschreven in sectie 2.3 worden niet door iedereen als voordelen ervaren.

De onderstaande tabel vat alle in de interviews genoemde en uit bureau-onderzoek gevonden sterke en zwakke punten en kansen en bedreigen samen.

SWOT PKIo stelsel

Sterke punten	Zwakke punten
• Keurmerk Staat der Nederlanden – biedt gevoelsmatige zekerheid en vertrouwen. • Volledige controle over kwaliteit van het stelsel en de processen voor uitgifte en intrekken van hoogwaardige en betrouwbare certificaten. • Overheid in control bij incidenten. • Overheid Identificatie Nummer maakt herleiden van identiteit mogelijk. • Beschikbaarheid van private en publieke roots. • Past bij de één overheid gedachte.	• Complexiteit, waardoor er soms sprake is van oneigenlijk gebruik van certificaten en het moeilijk is om goed toezicht te houden. • Hoge kosten van de certificaten en het beheer ervan bij afnemers. • Mee moeten gaan met alle verplichtingen CAB-forum voor publieke certificaten. • Beperkte scope (NL) waardoor weinig invloed bij CAB-forum. • Waarom geen eIDAS maar keuze PKIo voor NL - afscherming kan NL kwetsbaar maken. • Beveiligingsmeerwaarde t.o.v. andere gekwalificeerde certificaten is onduidelijk. • Afstand tussen normenkader en praktische toepassing. • Normenkader wordt verschillend geïnterpreteerd bij auditor(s), Policy Authority en toezichthouder. • Frictie van PKIo eisen met normenkader ETSI / eIDAS. • Eén normenkader voor alle certificaten is onlogisch. • Diginotar nog vers in het geheugen. • Geen overzicht afnemers, maakt stimuleren lastig. • Doorlooptijd uitgifte.
Kansen	**Bedreigingen**
• Er is voldoende draagvlak bij veel stakeholders om gebruik PKIo te vergroten. • Digitale zegels breder inzetten • Mogelijkheid om PKIo uit te breiden met nieuwe certificaten en het toevoegen van time stamping. • Veel partijen zien PKIo al als een verplichting. • PKIo is al voor veel gevallen in beleid/wet/richtlijnen verplicht gesteld of genoemd als best practise. • Mogelijkheid om verplichting te versterken. • Men staat redelijk neutraal t.o.v. type PKI certificaat, dus kan net zo goed PKIo zijn. Ofwel, de weerstand tegen PKIo is beperkt onder stakeholders. • Mogelijkheid om samenwerking tussen Policy Authority, afnemers en leveranciers te vergroten. • “Practise what you preach”.	• In de breedte is kennis/kunde over PKIo zeer beperkt • Afstand PKIo ecosysteem en de afnemers. Perceptie dat focus Policy Authority ligt bij commerciële TSPs en CAB-forum. TSPs ondersteunen afnemers, maar daar zit ook een commercieel belang. • PKIo wordt door afnemers ervaren als een melkkoe; de kosten zijn hoog. Testen is duur en de aanschaf van grote hoeveelheden (vaak persoonlijke) certificaten is onbetaalbaar. • Interferentie met eIDAS; weigeren van andere, niet-PKIo Trust Service Providers is niet mogelijk. • Focus op NL domein maakt internationale samenwerking lastig. • Risico op stopzetten dienstverlening bij niet volledig aan normenkader voldoen. • Weerstand tegen normenkader, ervaren frictie met uitgangspunten en doelen PKIo. • Interoperabiliteit kan door geslotenheid van het stelsel in het gedrang komen; teveel PKIo-specifieke eisen kunnen gaan knellen. • Ruimte om te innoveren met als doel PKIo middelen schaalbaar, gebruikersvriendelijk en laagdrempelig uit te rollen is beperkt.

PKIo heeft veel voordelen en wordt beschouwd als een sterk merk. Er is draagvlak voor verbreding van gebruik. Er worden echter ook zodanig veel vele zwakke punten en bedreigingen genoemd dat de voordelen van PKIo ernstig in gevaar worden gebracht. Wanneer het gewenst is om het gebruik te verbreden is het algemene advies van de geïnterviewden om naast verplichten ook te verleiden en PKIo aantrekkelijk(er) te maken. Dus bekijken hoe het normenkader (PvE) kan worden vereenvoudigd, zonder afbreuk te doen aan de kwaliteit, om de relatie met eIDAS middelen beter te duiden en afnemers beter te betrekken bij het stelsel. Dit zou de complexiteit sterk kunnen reduceren, waardoor toepassing eenduidiger en eenvoudiger wordt en de praktische mogelijkheden om PKIo voor specifieke situaties toepasbaar te maken sterk verbeteren. Daarnaast zou het helpen om normenkaders van PKIo toe te spitsen voor de specifieke toepassingen.

Verleiden kan ook op andere manieren. Denk hierbij aan het stimuleren en faciliteren van innovatieve oplossingen door deelnemers. Bijvoorbeeld door gebruikers, in plaats van fysiek, op afstand te identificeren tijdens het uitgifteproces van PKIo-certificaten en het gebruik ervan vriendelijker te maken.

Bestaansrecht

Tijdens de expertconsultatie werd het bestaansrecht van PKIo nogmaals onderschreven. Het is een sterk merk voor Nederland, het zit goed en degelijk in elkaar met je kunt erop vertrouwen. Men is van mening dat het "*uitvoering van de Nederlandse wet*" is. Het past goed om PKIo als merk voor de overheid neer te zetten. In andere landen zijn er vergelijkbare infrastructuren. Het past om zoiets ook in Nederland te hebben. Opgemerkt wordt dat de waarde van PKIo afhangt van de overheidsinstelling die het toepast. PKIo wordt extra belangrijk gevonden in domeinen zoals Defensie of Justitie, waar een grote nadruk ligt op vertrouwen, veiligheid en beveiliging. Het betreft hier dan vooral op het gebruik van PKIo-certificaten in een overheidscontext.

Schaalvoordelen

Het gebruik van PKIo certificaten is nog beperkt. Zie ook hoofdstuk gebruik. Verplichting is een manier om gebruik uit te breiden. De kosten van PKIo zijn relatief hoog. Dit ontstaat doordat de verplichtingen van de TSPs (audits, compliance) vanuit het PKIo stelsel die worden doorbelast in de prijs van de certificaten. Door groei van het gebruik ontstaan schaalvoordelen wat gunstig kan doorwerken in de prijs van een certificaat.

Kunnen we ook zonder PKIo?

Gezien de omvang van de zwaktes en bedreigingen, rijst de vraag of PKIo überhaupt wel nodig is. Het gaat immers om het gewenste betrouwbaarheidsniveau die ook door andere gekwalificeerde middelen kunnen worden geleverd. Met de komst van eIDAS, waarin de spelregels voor gekwalificeerde certificaten op Europees niveau geregeld wordt, lijkt de meerwaarde voor een Nederland-specifiek afsprakenstelsel beperkt en mogelijk zelfs risicovol.

Enige nuancering is hier ons inziens op zijn plaats. eIDAS is gebaseerd op onderling vertrouwen tussen de Europese lidstaten betreffende de kwaliteit en betrouwbaarheid van TSPs. De toekomst zal moeten uitwijzen of dit vertrouwen gegrond is, omdat nog onduidelijk is of er verschillen gaan ontstaan in de wijze waarop implementaties in de landen worden gerealiseerd. Daarmee zouden er verschillen kunnen ontstaan in de betrouwbaarheid van (toekomstige) TSPs. Met PKIo is veel zekerheid en controle over de uitgifte van certificaten.

Het lijkt dus meer een vertrouwenskwestie en daarmee een gevoelskwestie of PKIo beter is dan andere gekwalificeerde oplossingen. Puur rationeel kan PKIo vervangen worden door andere oplossingen. Wat prevaleert – emotioneel of rationeel – hangt mogelijk af van de toepassing. Voor specifieke overheidstoepassingen is het wenselijk om de "Staat der Nederlanden" root te opereren: het straalt vertrouwen, zekerheid en herkenbaarheid uit. Voor andere toepassingen zijn deze twee kwaliteiten wellicht minder relevant en is zekerheid over een bepaald betrouwbaarheidsniveau voldoende. Er valt bijvoorbeeld iets voor te zeggen dat alle websites van de rijksoverheid met een PKIo EV certificaat zijn beveiligd. Immers deze websites vormen het *uithangbord* van de overheid richting burgers en bedrijven en dienen ook als zodanig *herkenbaar* te zijn. Maar technisch gezien is een koppeling op Digipoort met een gekwalificeerd eIDAS certificaat net zo veilig als met een PKIo certificaat.

Overheids-TSP vs commerciële TSPs

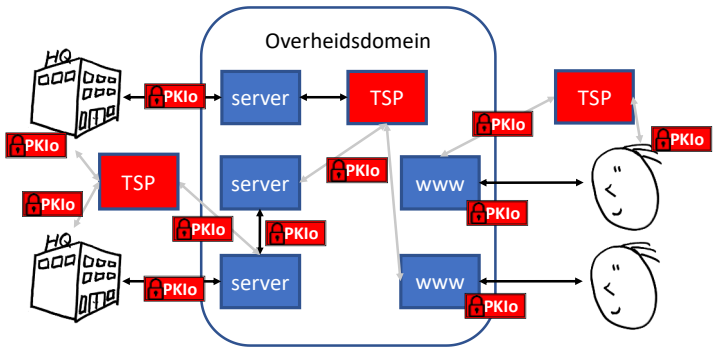
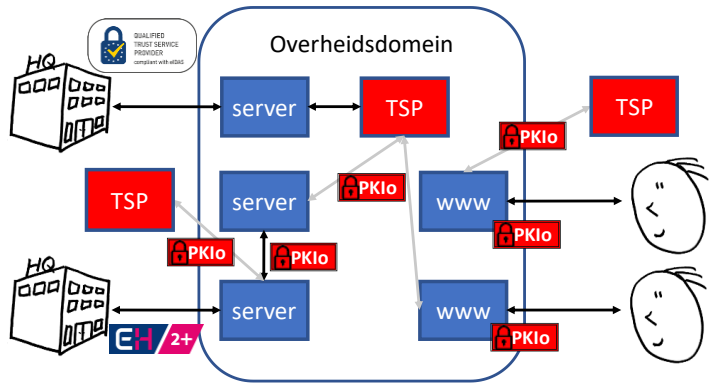
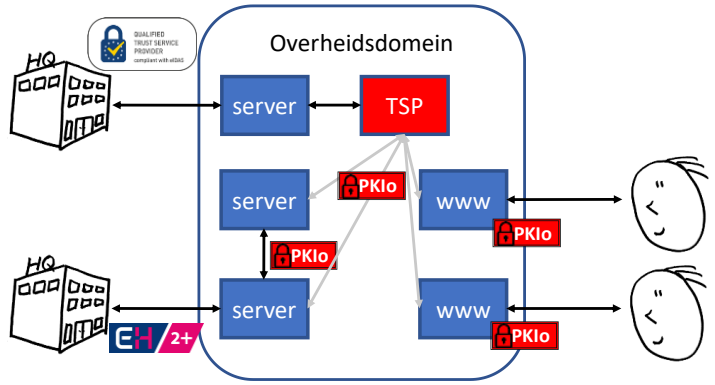
Als voor specifieke overheidstoepassingen PKIo de voorkeur geniet, dan is de volgende vraag of de overheid dan niet zelf hiervoor de enige TSP moet zijn. Waarom zijn hiervoor private TSPs nodig? Door het als overheid zelf te doen kunnen de kosten van certificaten voor intern gebruik door overheidsorganisaties omlaag en hoeven onderdelen als RDW, DUO en JustID zelf geen eigen PKI meer te onderhouden. De TSP van het Ministerie van Defensie zou hier invulling aan kunnen geven. Voor certificaat-gebaseerde toepassingen *buiten* het overheidsdomein volstaat het om aan te geven welk niveau van betrouwbaarheid voor bijvoorbeeld een authenticatie of digitale handtekening gewenst is. Zo zijn alle overheidswebsites en de onderlinge communicatiekanalen tussen overheidsorganisaties met PKIo beveiligd. Ook kunnen ambtenaren met een persoonsgebonden PKIo certificaat inloggen bij overheidsdiensten, de eigen kantoor infrastructuur of toegang krijgen tot fysieke locaties. Partijen buiten de overheid kunnen met eigen middelen met de overheid communiceren; deze middelen moeten wel voldoen aan door de overheid gestelde betrouwbaarheidsniveaus. Een kanttekening bij de overweging overheids-TSP is dat er in het algemeen een groter vertrouwen in stelsels waarin ook private partijen een rol hebben dan in stelsels waar alleen de overheid de bepalende factor is.

PKIoverheid scenario's

Samenvattend zijn de volgende scenario's denkbaar voor PKIoverheid van de toekomst:

1. PKIoverheid voor alle overheid gerelateerde diensten met zowel private als publieke TSPs
2. PKIoverheid alleen binnen het overheidsdomein met zowel private als publieke TSPs
3. PKIoverheid alleen binnen het overheidsdomein met een publieke TSP

De onderstaande figuren illustreren de hiervoor genoemde scenario's.

1. PKIo voor alle overheid gerelateerde diensten met zowel private als publieke TSPs Karakteristieken: • Dit is de huidige situatie. • Zorgsector inbegrepen (UZI pas etc) • PKIo-certificaten voor server-to-server communicatie intern overheid. • PKIo-certificaten voor externe koppelingen vanuit bedrijven met overheidsvoorzieningen. • Ook PKIo-certificaten voor burgers om mee in te loggen. • Alle overheidswebsites met PKIo-certificaten beveiligd.	
2. PKIo alleen binnen het overheidsdomein met zowel private als publieke TSPs Karakteristieken: • Als hierboven behalve externe koppelingen op basis van betrouwbaarheidsniveaus. • Defensie zou met de eigen huidige TSP invulling kunnen geven aan de overheidsbrede TSP functionaliteit.	
3. PKIo alleen binnen het overheidsdomein met een publieke TSP Karakteristieken: • Eigen overheids-TSP en root voor de verstrekking van PKIo-certificaten voor intern gebruik. • Externe toegang op basis van betrouwbaarheidsniveaus.	

De aanvullende aandachtspunten voor de verschillende toepassingsdomeinen worden uitgewerkt in de volgende paragrafen.

4.2 TOEPASSINGSDOMEIN WEBSITE BEVEILIGING

PKIo kent verschillende toepassingsdomeinen. Eén daarvan is website beveiliging met een (EV/QWAC) SSL website certificaat, waarmee de website betrouwbaar te herleiden is naar de desbetreffende overheidsorganisatie. Door het certificaat aan te klikken kan de gebruiker de echtheid en de beveiliging van de website controleren. Hij/zij zal dan zien dat dit middels een certificaat gebeurd dat onder de root van de Staat der Nederlanden is uitgegeven.

SWOT Toepassing PKIo (EV) SSL certificaten voor website beveiliging

Sterke punten	Zwakke punten
• Veel websites passen al PKIo toe. • Past bij uniforme implementatie van overheidswebsites. • Als je zo'n sterk middel hebt, waarom pas je het dan niet overal toe?	• Oudere browsers ondersteunen mogelijk niet een nieuwe generatie PKIo certificaten, waardoor beperking toegankelijkheid. • Afhankelijkheid CAB-forum / browserpartijen. • Gebruiker herkent niet dat de website authentiek is; certificaat zegt hem niks. • Het aanklikken van het certificaat is niet mogelijk in browsers op mobiele telefoons.
Kansen	**Bedreigingen**
• PKIo toepassen is een logische stap in digitale dienstverlening, passend bij verplicht gebruik DigiD en eHerkenning. • Stimulering toepassing PKIo vanuit Algemene Zaken. • Steeds meer mijn-omgevingen waarvoor website beveiliging essentieel is. • Toestaan van wildcard certificaten in PKIo.	• Onbekendheid met PKIo bij afnemers en leveranciers. • Frictie tussen visie dat gebruiker het zou moeten vertrouwen en browserpartijen die er tussen gaan zitten. • Certificaten voor testgebruik zijn kostbaar.

De meeste geïnterviewden vinden een PKIo website certificaat prima, vooral vanuit beveiligingsperspectief en herkenbaarheid als overheidsmedium. Men vindt het opmerkelijk dat er eisen worden gesteld aan de betrouwbaarheid van de authenticatie van de klant en dat daarvoor bepaalde middelen worden voorgeschreven en dat er daarnaast geen duidelijke betrouwbaarheids- en veiligheidseisen zijn voor website van bijvoorbeeld de mijn-omgeving die de diensten moet leveren. Voor de overheid is het dan logisch om herkenbaar te zijn met een PKIo certificaat. Vooral als het websites betreft die informatie verwerken die gevoelig van aard is of op basis waarvan rechten kunnen worden verleend, zo stelt ook de BIR.

De vraag rijst of íedere overheidswebsite beveiligd moet zijn en of een (goedkoper) certificaat dat door een commerciële partij is uitgegeven, zoals Let's Encrypt of Amazon, niet voldoende is. Het antwoord hierop is niet triviaal. Een belangrijk uitgangspunt van elke overheidswebsite is dat de integriteit van alle gegevens op de website is geborgd. Ook als de gegevens niet gevoelig zijn moet de bezoeker ervan uit kunnen gaan dat ze authentiek en van de Nederlandse overheid zijn. Een PKIo-certificaat biedt hierbij meerwaarde ten opzichte van andere certificaten. Bovendien past het beter bij een uniforme implementatie van alle overheidswebsites. Dit ongeacht het gegeven dat niet iedere bezoeker het certificaat zal controleren of zal begrijpen wat het betekent. Mogelijk kan het toestaan van wildcard certificaten binnen PKIo het gebruik van PKIo-certificaten voor website beveiliging stimuleren. Merk op dat Let's Encrypt of Amazon certificaten onder de US wet- en regelgeving vallen (Patriot Act) en niet voldoen aan NL of EU wetgeving. Dit compliceert het toepassen van deze certificaten.

Regelmatig wordt de afhankelijkheid van het CAB-forum genoemd om geaccepteerd te worden in de browsers. Deze afhankelijkheid geldt natuurlijk voor elk type PKI, behalve dat de scope van PKIo tot Nederland beperkt is en de urgentie van een Nederlands middel daarmee beperkt is voor het CAB.
Er is enige frictie tussen de eisen van CAB, die ingevuld moeten zijn, en eIDAS/ETSI eisen. Het CAB-forum heeft een sterke oriëntatie op de Verenigde Staten, waarbij eIDAS nog behoorlijk onbekend is en afwijkt van de VS-norm. Een vervelend probleem is dat een website voor oudere browserversies wellicht niet toegankelijk is omdat deze browsers niet met een recente PKIo om kunnen gaan. Wanneer verplichting aan de orde is, zal dit probleem opgelost moeten worden.

4.3 VEILIGE COMMUNICATIE

Het gebruik van servercertificaten is op dit moment de belangrijkste toepassing van PKIo.

SWOT Toepassing PKIo servercertificaten voor veilige communicatie

Sterke punten	Zwakke punten
• PKIo is afdwingbaar door de dienstverlener, middels standaarden en in afsprakenstelsels. • OIN is handig. • Private en Publieke variant.	• Certificaten zijn server en domeinnaam afhankelijk, hoge kosten omdat meerdere certificaten nodig zijn. • Gebruik voor testen is duur. • Omgaan met grote variatie aan systemen en versies. • Niet alle diensten verplichten gebruik PKIo aan afnemers. • Meerwaarde t.o.v. andere gekwalificeerde certificaten is onduidelijk. • OIN beperkt operabiliteit.
Kansen	**Bedreigingen**
• Verdere verplichting vanuit dienstverlening lijkt logisch. • Past bij uniforme werkwijze voor communicatie tussen en met overheid.	• Door beperkt gebruik kan je niet leren van PKIo ervaringen in het verleden. • Kennis / kunde m.b.t. PKIo bij afnemers beperkt; vernieuwen van certificaten gaat wel eens fout. • Onduidelijk welk type certificaat in te zetten.

Uitwisseling van gegevens tussen servers is beveiligd met PKIo certificaten wanneer dat wordt geëist door de dienstverlener, zoals Logius of VWS, bepaalde standaarden voor gegevensuitwisseling (b.v. Digikoppeling) of afsprakenstelsels, zoals eHerkenning en MedMij. Zie ook hoofdstuk 3. Desalniettemin zijn er nog veel diensten die werken met eigen certificaten, bijvoorbeeld bij de RDW en DUO systemen richting respectievelijk de garagebedrijven en scholen.

OIN – het Organisatie Identificatie Nummer

Specifiek is het gebruik van OIN (Organisatie Identificatie Nummer) binnen PKIo. Het OIN is een uniek identificerend nummer dat gebruikt wordt door organisaties met een publieke taak zoals overheidsorganisaties in de digitale communicatie met andere publieke of private partijen. Een OIN is verplicht binnen PKIo en wordt toegekend door Logius. Ook bedrijven en privaatrechtelijke instellingen zonder publieke taak of bevoegdheid moeten door overheden geïdentificeerd kunnen worden. Daar wordt het Handelsregisternummer (HRN) voor gebruikt. Het direct meenemen van dit nummer in de dienstverlening is zowel een sterkte als een zwakte. Een voordeel is dat het OIN/HRN een partij uniek identificeert en het gebruikt kan worden om meer informatie te achterhalen. Het OIN of HRN wordt in bepaalde gevallen ook gebruikt als identificatienummer voor het adresseren of routeren van berichten in het elektronisch verkeer tussen met andere overheden en burgers en/of bedrijven. Een nadeel is dat het PKIo-specifiek is; in andere gekwalificeerde certificaten zal een OIN/HRN typisch ontbreken. Dit maakt dat het PKIo-ecosysteem relatief gesloten en beperkt interoperabel is met andere PKI-ecosystemen. De eIDAS verordening stelt dat lidstaten geen technische drempels mogen opwerpen die de interoperabiliteit ten behoeve de interne markt belemmeren. Op dit moment is er binnen de EU geen uniform bedrijvennummer beschikbaar. Er is wel een initiatief vanuit de G20 om wereldwijd een zogenaamd Legal Entity Identifier (LEI)[11] voor te schrijven.

De vraag is of het voor server-communicatie belangrijk is dat de certificaten onder de root van de Staat der Nederlanden vallen. De menselijke interactie is immers veel minder waardoor het gevoelsmatige aspect minder meespeelt. Echter, het gebruik van servercertificaten onder een andere root is niet triviaal. Voor communicatie conform Digikoppeling is bijvoorbeeld de opname van een OIN noodzakelijk. Dit is bijvoorbeeld het geval bij communicatie met Diginetwerk, Digipoort, SBR, OLO, LV WOZ, WSNP, GBA-V, BAG, WKPB e.a. Er is voor gekozen om het OIN te integreren in de dienstenarchitectuur in plaats van het afzonderlijk behandelen van certificaat en herleidbaar nummer. Daarmee wordt PKIo op een min-of-meer oneigenlijke manier afgedwongen. De vraag rijst of dat een wenselijke situatie is. Alternatieven voor OIN zijn er wel (bijvoorbeeld Legal Entity Identifier of een Europees handelsregister nummer) echter herleidbaarheid is dan beperkt omdat

[11] GLEIF – Global Legal Entity Identifier Foundation, https://www.gleif.org/en/

het achterliggende register niet geraadpleegd kan worden. Het zou vanuit dit oogpunt wenselijk zijn om dit EU-breed op te pakken en te migreren naar een identificatie nummer passend bij eIDAS.

4.4 DIGITAAL WAARMERKEN

De focus hier is op het waarmerken documenten met persoonlijke certificaten, niet het waarmerken van berichten met server certificaten in een server-to-server setting.

SWOT Toepassing PKIo persoons- of beroepscertificaten voor digitaal waarmerken

Sterke punten	Zwakke punten
• Uitgifte onder NL overheid root past bij overheidsmedewerkers. • Mogelijkheid om voor alle interne en externe communicatie toe te passen.	• Signing certificaten uitgeven aan alle medewerkers is erg kostbaar. • Uitgifte onder NL overheid root is niet per sé logisch voor niet-overheid personen. • Persoon is niet accountable, dat is de organisatie. Frictie met het normenkader. • Waarmerken op organisatieniveau is mogelijk, maar nog zeer onbekend (eSeal)
Kansen	**Bedreigingen**
• Past bij een uniforme manier van werken binnen de overheid voor digitaal waarmerken. • Ondersteuning van wederzijds vertrouwen. • Logisch gebruik als algemeen geaccepteerd en officieel overheidswaarmerk buiten overheidsdomein (bijv. richting burgers). • Snel groeiende markt.	• Escape naar eigen oplossing door hoge kosten/investeringen. • Niet meegaan met nieuwe (technologische) ontwikkelen, bijv. online identificeren, cloud storage. • Kosten / slechte business case / benodigde investeringen

Het digitaal kunnen waarmerken van gegevens begint een steeds grotere vlucht te nemen. Accountants gebruiken een persoonsgebonden beroepscertificaat voor het rechtsgeldig ondertekenen van de accountantsverklaring en voor het waarmerken van de jaarrekening die ze vervolgens via Digikoppeling communiceren. KvK waarmerkt uittreksels uit het handelsregister met een PKIo certificaat. In het certificaat staat welke functionaris van KvK ondertekend heeft.

Het gebruik van digitale of elektronische zegels door overheidsorganisaties is mogelijk binnen PKIo, maar gebruikers zijn hier niet mee bekend. Sinds medio 2017 bestaat de mogelijkheid van een eSeal (uitgegeven onder deel 3b van PKIoverheid). Met een dergelijk zegel weet de ontvanger van het document dat het inderdaad afkomstig is van de betreffende overheidsorganisatie. Dit is vaak relevanter dan de betreffende naam van de functionaris op wiens naam het certificaat staat.

Het algemeen beeld uit de interviews is dat, als de overheid gegevens digitaal waarmerkt, PKIo van meerwaarde is. Het straalt duidelijkheid, herkenbaarheid en betrouwbaarheid uit en is daarmee gevoelsmatig te vergelijken met het beveiligen van de overheidswebsites.

Waarmerken met PKIo is niet altijd wenselijk of niet nodig. Een ander gekwalificeerd certificaat kan voldoende of net zo betrouwbaar zijn. Maar ook met niet-gekwalificeerde certificaten is waarmerken mogelijk. Deze waarmerken hebben dan een andere juridische status. In plaats van de focus op wel of niet PKIo zou de focus moeten liggen op het geëiste betrouwbaarheidsniveau van een waarmerk.

Ook zijn er scenario's denkbaar waarbij waarmerken middels een PKIo certificaat minder wenselijk is. Bijvoorbeeld, bij het ondertekenen van een indiening voor een overheidsaanbesteding door een internationale groep van bedrijven. In een internationale context zou je willen toestaan dat de partij met een gekwalificeerd PKI-certificaat ondertekent (niet zijnde PKIo), bijvoorbeeld uit het eigen land.

4.5 TOEPASSINGSDOMEIN AUTHENTICATIE

SWOT Toepassing PKIo persoons- of beroepscertificaten voor authenticatie

Sterke punten	Zwakke punten
• Uitgifte onder NL overheid root past bij overheidsmedewerkers.	• Certificaten uitgeven aan alle medewerkers is erg kostbaar. • Uitgifte onder NL overheid root is niet per se logisch voor niet-overheid personen. • Niet meegaan met nieuwe (technologische) ontwikkelen, bijv. online identificeren, cloud storage.
Kansen	**Bedreigingen**
• Iedere burger een PKIo certificaat	• Frictie met andere erkende en/of gekwalificeerde authenticatie middelen (DigiD, eHerkenning, eIDAS). • Kosten / slechte business case / benodigde investeringen

Authenticatie is het vaststellen van de (elektronische) identiteit van de communicatiepartner. Een toepassing die met behulp van PKIo-certificaten heel goed kan worden ingevuld. Voorbeelden hiervan zijn de persoonlijke certificaten op de defensie- en UZI-pas waarmee medewerkers toegang krijgen tot diensten.

Mede door de strikte eisen die door PKIo worden gesteld aan het uitgifteproces van certificaten (fysieke identificatie aan de balie) en robuustheid van de beveiliging ervan (tamper resistant hardware) resulteert een authenticatie tot een hoge identiteitszekerheid. De betrouwbaarheidsniveaus van authenticatie zijn in de eIDAS wetgeving gedefinieerd: Laag, Substantieel en Hoog. In principe komt een authenticatie met een PKIo-certificaat overeen met eIDAS Hoog.

Er zijn in Nederland nog diverse andere authenticatievoorzieningen die door de burger of ondernemer kunnen worden gebruikt om in te loggen bij publieke of private diensten:

- DigiD: voor burgers om in te loggen bij diensten die het BSN mogen verwerken, ofwel dienstaanbieders in de overheid-, zorg- en pensioensector. DigiD is momenteel in te zetten op de betrouwbaarheidsniveaus Laag en Substantieel. DigiD Hoog maakt gebruik van de chip (e-functionaliteit) op de Nederlandse identiteitsdocumenten en bevindt zich nog in de pilot-fase.
- eHerkenning: een afsprakenstelsel dat het voor bedrijven mogelijk maakt om in te loggen bij private of overheidsdiensten. eHerkenning voorziet in authenticatiemiddelen op alle niveaus. Deze middelen kunnen worden aangeschaft bij private middelenuitgevers als KPN, Digidentity, Creaim Reconi, Connectis, Unified Post en QuoVadis. Merk op dat een deel van deze uitgevers ook PKIo TSPs zijn. De meeste aanbieders van eHerkenning niveau 4 middelen (ofwel eIDAS Hoog) maken hiervoor gebruik van PKIo-certificaten. Eén aanbieder biedt hiervoor ook een eigen gekwalificeerd certificaat aan.
- Idensys: een afsprakenstelsel dat het voor burgers mogelijk maakt om in te loggen bij private of overheidsdiensten. Idensys is sterk gebaseerd op eHerkenning en kent veel overlap in deelnemers. In Idensys is het mogelijk om een persoonlijk PKIo-certificaat te laten registreren als Idensys Hoog middel. De pilots met Idensys zijn onlangs gestopt; onduidelijk is of en hoe het verder gaat met Idensys.
- iDIN: een afsprakenstelsel dat het voor burgers mogelijk maakt om met bankauthenticatie in te loggen bij private diensten. Het gebruik van iDIN voor publieke diensten is op dit moment niet toegestaan.
- Private middelen: de overheid is voornemens om een aantal private middelen aan te besteden waarmee burgers kunnen inloggen bij publieke diensten. Dit om te voorkomen dat DigiD teveel een single-point-of-failure wordt.
- eIDAS middelen: Nederlandse burgers kunnen elders in Europa een eIDAS-erkent authenticatiemiddel aanvragen waarmee ze (ook) kunnen inloggen bij Nederlandse publieke diensten. Een voorbeeld hiervan is het Estse eResidency middel op niveau Hoog.

In de context van dit uiteenlopende authenticatie-landschap, is een eventuele verplichtstelling van PKIo-certificaten voor authenticatiedoeleinden voor de overheid niet evident. In de context van eHerkenning en Idensys zijn PKIo-certificaten voor Hoog al min of meer gemeengoed en zal verplichting haalbaar zijn door

aanpassing van het afsprakenstelsel. Echter verplichtstelling van PKIo via eHerkenning staat haaks op het doel van het eHerkenningsstelsel, namelijk dat verschillende middelen van hetzelfde betrouwbaarheidsniveau naast elkaar bestaan en toegang geven. Let wel, beide stelsels richten zich op dit moment volledig op overheidsdienstverleners. Bij een toekomstige verbreding naar private dienstverleners kan er meer behoefte ontstaan naar het gebruik van andere, commerciële en mogelijk goedkopere gekwalificeerde certificaten. Onwenselijk is om zakelijke gebruikers te verplichten om twee middelen te gebruiken: één voor overheidsdienstverleners (op basis van PKIo) en één voor private dienstverleners (op basis van andere gekwalificeerde certificaten).

De keuze voor PKIo-certificaten als verplicht authenticatiemiddel op niveau Hoog kan een grote impact hebben op de huidige voorziene DigiD Hoog oplossing dat gebruik maakt van een authenticatie-applet op de chip van wettelijke identiteitsdocumenten. Het voorzien van dergelijke documenten met een PKIo-certificaat zal grote technische en organisatorische aanpassingen vereisen. Het is onduidelijk of de ICAO-standaard zo'n chip überhaupt toestaat.

Overigens is voor toegang tot de meeste publieke diensten geen niveau Hoog authenticatie nodig. Een iets minder betrouwbare, twee-factor oplossing, volstaat hier. Die zijn ook goedkoper en gebruikersvriendelijker. Eventuele verplichtstelling kan alleen maar voor die diensten die authenticatieniveau Hoog vereisen, zoals bijvoorbeeld in de zorgsector voor het werken met medische gegevens.

Ook hier ligt het voor de hand om te abstraheren van de manier waarop iemand wordt geauthentiseerd en te focussen op het betrouwbaarheidsniveau dat nodig is voor toegang tot diensten. Ofwel de eIDAS-aanpak te volgen, waarbij de dienstverlener erop kan vertrouwen dat de gebruiker op het juiste, door hem aangegeven betrouwbaarheidsniveau wordt geauthentiseerd. Dan maakt het niet meer uit of dat met een PKIo-certificaat of anderszins is gedaan. Tenminste als het om toegang van burgers of bedrijven gaat tot overheidsdienstverlening. Voor de eigen overheidsmedewerkers geldt een ander verhaal. Niets staat de overheid in de weg om de eigen medewerkers een authenticatiemiddel te verstrekken dat gebaseerd is op PKIo-certificaten. De defensiepas van het ministerie van Defensie is hiervan een goed voorbeeld.

4.6 ANALYSE

Uit de diverse SWOT-analyses volgt een wisselend beeld van het nut en de noodzaak van PKIo. De kernvraag is of door PKIo te verplichten de zwaktes worden weggenomen zodat de sterke punten worden versterkt. Per toepassingsgebied is het antwoord op deze vraag als volgt:

1. Website beveiliging: Niet alle (rijks)overheidswebsites zijn beveiligd met PKIo (EV/QWAC) certificaten. Dit wordt wel als wenselijk gezien: PKIo draagt bij aan een betrouwbare en veilige uitstraling de websites. Ook zouden websites van lagere overheden gebruik moeten maken van PKIo certificaten. Verplichting van dergelijke certificaten kan bijdragen tot uniforme beveiliging en uitstraling van alle overheidswebsites.
2. Veilige communicatie (tussen servers): De meerwaarde van PKIo ten opzichte van andere certificaten is beperkt voor deze toepassing. Verplichten neemt deze zwakte niet weg. De vraag is ook of Nederland met het toenemende Europese berichtenverkeer (single European digital market) dit kan afdwingen naar servers in andere lidstaten. Verstandiger is om in dit geval in te steken op betrouwbaarheidsniveaus: geef aan welke niveau vereist is om te koppelen met overheidsvoorzieningen als Digikoppeling. Het toepassen van OIN in dienstverlening is een knelpunt om deze visie te realiseren.
   Voor veilige intra-overheidscommunicatie zou PKIo wel verplicht kunnen worden. In dat geval is het wellicht verstandiger om als overheid zelf TSP te worden. Deze TSP voorziet alle overheidsorganisaties van PKIo certificaten waarmee de kosten kunnen worden gedrukt. Een dergelijke aanpak heeft een grote impact op het huidige PKIo stelsel: private partijen die PKIo certificaten uitgeven zijn dan niet meer nodig. Deze partijen kunnen wel een rol spelen bij het aanleveren van voorzieningen voor het inrichten van de overheids-eigen PKI. Hier knelt het met de Wet Markt en Overheid.
3. Digitaal waarmerken: Hier geldt hetzelfde als bij website beveiliging: PKIo biedt meerwaarde in termen van uitstraling. Het is niet betrouwbaarder dan andere onder eIDAS gekwalificeerde certificaten. Vooral als er vanuit de overheid naar buiten toe wordt gecommuniceerd. Gezien de groeipotentie van deze toepassing kan verplichting van PKIo bijdragen aan harmonisatie van oplossingen. De kosten van PKIo zijn een potentiele showstopper. Verplichting kan helpen om schaalvoordelen te bereiken die doorwerken in de

kosten. Om de kosten te verlagen valt ook te overwegen om digitale zegels in te zetten en om goed te beoordelen of in alle gevallen een gekwalificeerde digitale handtekening nodig is.

4. Authenticatie van personen, beroepen of bedrijven: Het verplichten van PKIo is niet haalbaar. Er zijn teveel andere publieke en private oplossingen die last krijgen van een eventuele verplichting van PKIo. Bovendien is het te kostbaar om bijvoorbeeld iedere Nederlander een persoonscertficaat te geven. De overheid moet hier focussen op het vaststellen van betrouwbaarheidsniveaus van authenticatie voor toegang tot diensten. Het is dan aan de gebruiker om hiervoor een bijpassend authenticatiemiddel te selecteren (DigiD, iDIN, eHerkenning, eIDAS, PKIo). Ook voor ambtenaren is een persoonsgebonden PKIo certificaat duur, tenzij in combinatie met certificaten voor waarmerken en kosten door schaalvoordelen verlaagd worden.

Verplichting vereist dat weerstanden en knelpunten zoveel mogelijk worden weggenomen. Het wordt aanbevolen om het normenkader eens goed tegen het licht te houden en te bekijken wat elke eis toevoegt aan de kwaliteit en betrouwbaarheid van het stelsel. Waar nodig te vereenvoudigen, vooral voor de afnemer. Het is belangrijk dat de voordelen van PKIo goed voor het licht komen, nu overwegen vaak de nadelen. Er is een sterke wens vanuit de TSPs om te innoveren zodat kosten voor PKIo certificaten beperkt kunnen worden en gebruiksgemak voor afnemers vergroot.

In de SWOTs is een voor een aantal toepassing gesteld dat gekeken moet worden naar betrouwbaarheids-niveaus en de focus niet moet liggen op wel of niet PKIo. Dat kunnen we iets breder trekken door onszelf de vraag de stellen wat PKIo toevoegd aan het beveiligingskader van overheidsdienstverlening. Hier verschillen de meningen. Sommige vinden dat PKIo wel wezenlijk beter presteert dan een ander gekwalificeerd middel. Anderen vinden dat andere gekwalificeerde middelen net zo goed zijn en dat je je dus kunt afvragen of PKIo wel nodig is en de investeringen daarin gerechtvaardigd. Deze mening wordt gesteund door het feit dat het aantal genoemde zwaktes en bedreigingen van het PKIo stelsel te voordelen en kansen overtroeven, wat de ervaren meerwaarde sterk beperkt.

Als het gaat om verplichting, dan zijn er drie toepassingsgebieden waar dit relevant is: websites, digitaal waarmerken/ondertekenen en voor veilige communicatie tussen servers van overheidsorganisaties onderling. In het volgende hoofdstuk gaan we nader in op welke manier dit het beste zou kunnen.

5. Verplicht stellen

Verplicht stellen genereert een groter gebruik van PKIo. Verplichten is geen doel op zich, maar een middel dat tot doel met hebben om web- en mailverkeer betrouwbaarder en veiliger te maken. Een belangrijke consequentie van verplicht stellen is dat kosten voor afnemers sterk kunnen stijgen i.v.m. aanschaf van (meer) PKIo certificaten, met daarbij een grotere certificatenbeheerslast en noodzaak tot opbouwen van expertise. De verwachting is wel dat er schaalvoordelen ontstaan door vergroting van gebruik die de prijzen kunnen laten dalen. Verplicht stellen vereist dat gebruik van PKIo wordt gemonitord en dat er zicht is op waar en door wie PKIo certificaten worden toegepast.

Zoals in het vorige hoofdstuk geconcludeerd is verplicht stellen relevant voor de toepassing voor website beveiliging, waarmerken en veilige communicatie tussen servers van overheidsorganisaties. Voor andere toepassingen is PKIo één van de mogelijke oplossingen naast andere certificaten. Verplichten kan op verschillende manieren:

- Verankering in wetgeving;
- Opnemen in baselines, handreikingen of richtlijnen;
- Opnemen in de Pas-toe-of-leg-uit lijst van verplichte standaarden;

In de volgende paragraaf bespreken we de voor- en nadelen van de verschillende opties. Daarnaast is er de optie om PKIo-certificaten in eigen beheer uit te gaan geven. Dit wordt besproken in paragraaf 5.2.

5.1 MOGELIJKHEDEN VOOR VERPLICHTSTELLING

De drie mogelijkheden voor verplichtstelling van PKIo certificaten was een van de onderwerpen in de interviews. De voor-, nadelen en consequenties worden hier besproken.

Verankering in de wet

Er is op dit moment geen wettelijke verplichting om PKIoverheid te gebruiken. Een mogelijkheid voor concrete duiding van het gebruik van PKIo-certificaten is de voorgestelde wet Digitale Overheid (DO) of de hieruit voortvloeiende onderliggende regelgeving. De eerste tranche van deze wet betreft vooral kaders voor het beveiligen van elektronisch verkeer in het publieke domein en voor de generieke digitale infrastructuur en sluit dus goed aan bij de doelen van PKIo. Het wetsvoorstel adresseert o.a. standaarden (wat PKIo zou kunnen zijn/worden), betrouwbaarheidsniveaus (PKIo zit op het hoogste niveau) en beveiliging en verantwoordelijkheden hieromtrent (waarin PKIo zou kunnen voorzien). De wet DO wordt door de meeste geïnterviewden / experts genoemd als de weg die we moeten gaan.

Op het eerste gezicht vormt de wet DO of onderliggende regelgeving dus een goede plek om het verplicht gebruik van PKIo te verankeren, vooral nu een aantal specifieke toepassingsgebieden duidelijk zijn. De vraag is echter of het nog mogelijk is om PKIo op te nemen in de wet en of dit niet ten koste gaat van de gewenste technologie-neutraalheid. Vooral in situaties waarbij PKIo niet goed werkt kan het wettelijk verplichtende karakter nadelig zijn. Zoals bijvoorbeeld het geval was voor verouderde browsers op mobiele telefoons die niet overweg konden met de nieuwste PKIo certificaten. Een consequentie van wettelijke verplichting is dat er moet worden toegezien op naleving. Er moet een toezichthouder komen die een mandaat heeft om in te grijpen als partijen zich niet aan de wet houden. De impact van het ‘niet aan de wet houden’ is zeer groot omdat dit betekent dat de dienstverlening offline gaat als de PKIo certificaten worden ingetrokken. Al met al lijkt het verplichten van PKIo middels een wettelijke verankering dus iets teveel van het goede en voorlopig niet haalbaar. Zeker gezien de lange doorlooptijd voor het vastleggen in wetten.

De wet DO is grotendeels gebaseerd op de eIDAS verordening en rept over erkende middelen die moeten worden toegestaan. Afbakenen van een Nederland-specifieke PKI druist in tegen het uitgangspunt van eIDAS, dat streeft naar een unieke digitale Europese markt. De Nederlandse overheid zal ook andere erkende certificaten die onder eIDAS gekwalificeerde TSPs worden uitgegeven moeten accepteren. Vanuit wettelijk oogpunt is verplichtstelling van PKIo-certificaten dus niet haalbaar. Beter is om het gebruik van certificaten verplicht te stellen die voldoen aan de eisen, i.e. uitgegeven door erkende TSPs. De handreiking betrouwbaarheidsniveaus biedt overheidsorganisaties voldoende handvatten om het betrouwbaarheidsniveau

van een bepaalde dienst of voorziening te bepalen. Daarnaast is het onwenselijk dat (nieuwe) gekwalificeerde middelen uit de markt worden gedrukt door verplichtstelling van PKIo. Dat is in strijd met de wens om een breed en gevarieerd aanbod van vertrouwensdiensten te realiseren.

Opname in de wet is een langdurig traject. Door te wachten tot de verplichting een feit is, zal het gebruik van PKIo kunnen stagneren en/of nieuwe werkwijzen ontstaan. Vooruitlopend op eventuele verplichting kan daarom worden gekeken naar andere manieren, zoals opname in richtlijnen of Pas-toe-of-leg-uit lijst.

Opnemen in baselines, handreikingen of richtlijnen

Informatie beveiligingsrichtlijnen werken de uitvoering van de wet uit voor een specifiek domein eventueel aangevuld met aanvullend beleid, bijvoorbeeld Rijksoverheid of gemeenten. De BIR (Baseline Informatiebeveiliging Rijksoverheid) is er zo een. Hierin staat als dat PKIo verplicht is voor web- en mailverkeer van gevoelige informatie. In het Encryptiebeleid voor gemeenten wordt PKIo ook hiervoor genoemd. De verplichtstelling in deze richtlijnen wordt meer gezien als een advies en niet van toepassing voor alle rijksoverheiddienstverlening, ondanks besluitvorming hierover in de Ministerraad. Het is zeker aan te bevelen om verplichting van PKIo nader te specificeren in de richtlijnen en de richtlijnen op beleidsniveau wederom onder de aandacht te brengen bij de verschillende interdepartementale overleggen, zoals Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) en het CIO beraad. Visie op gebruik van PKIo kan worden voorbereid door de Subcommissie Informatie Beveiliging (SIB). Opgemerkt moet worden dat in het SIB verschillende departementen zijn vertegenwoordigd en daarnaast het Nationaal Cyber Security Centrum (NCSC), het Nationaal Bureau Verbindingsbeveiliging (NBV), het Integraal Beveiligingsberaad rijksoverheid (IBR) en het Centrum voor Informatiebeveiliging en Privacy (CIP). Voor dit onderzoek is met een aantal van deze partijen gesproken en kan geconcludeerd worden dat er geen consensus is over de meerwaarde van PKIo en gewenst gebruik ervan. Dit is een gevaar voor de besluitvorming.

Een combinatie van opnemen in richtlijnen en opname op de Pas-toe-of-leg-uit lijst zet het gebruik van PKIo nog beter op de kaart en zal het gebruik ervan versterken.

Opnemen in de Pas-Toe-of-Leg-Uit lijst

Een minder verplichtend alternatief voor verplichtstelling is de pas-toe-of-leg-uit-lijst (PTOLU) van het Forum Standaardisatie. Deze comply or explain lijst biedt ruimte voor alternatieven als PKIo toch niet passend is. Er is al eerder geprobeerd op PKIo op deze lijst te krijgen (Forum Standaardisatie, 2010. Expertadvies PvE PKIoverheid). Dit is niet gelukt omdat het toepassingsgebied van PKIo niet voldoende scherp kon worden gedefinieerd. Met een scoping naar website certificaten, waarmerken en/of veilige communicatie tussen overheidsservers zou dit wellicht beter kunnen waardoor er meer kans van slagen is op opname op de PTOLU-lijst.

Plaatsing van PKIo op de PTOLU lijst alleen is onvoldoende om gebruik van PKIo te stimuleren. De adoptie van standaarden op de lijst is niet altijd even succesvol. Extra drijfveren voor het gebruik van PKIo zijn nodig. Baselines voor informatiebeveiliging zijn hiervoor uitermate geschikt. In de BIR bijvoorbeeld staan tal van aanknopingspunten om PKIo te verankeren.

Verplichten gaat samen met verleiden

Naast verplichten is het ook wenselijk te zorgen voor verleiding door PKIo beter in de markt te zetten en zo te zorgen dat men niet om PKIo heen. Communicatie speelt daarbij een essentiële rol. Die is vaak nog moeizaam vanwege de complexiteit van het stelsel en de verschillende soorten certificaten. Te overwegen valt om het stelsel te vereenvoudigen en praktischer te maken. De focus moet liggen op het probleem dat PKIo moet oplossen en welk normenkader daarvoor nodig is. PKIo is geen doel op zich, maar een middel om veilige samenwerking met een willekeurig partij te realiseren. In de interviews werden de volgende vereenvoudigingen genoemd:

- De arbeidsovereenkomst (voor overheidsmedewerkers) onderdeel maken van het uitgifte proces.
- Inloggen met certificaten is ouderwets en omslachtig; er zijn andere manieren om in te loggen.
- Het encryptiecertificaat dat onderdeel uitmaakt van een persoonsgebonden PKIo-oplossing wordt nauwelijks gebruikt en zou weggelaten kunnen worden om kosten te drukken en risico's door kwijtraken te beperken.
- Onderzoek manieren om de kosten (tijd en geld) voor de afnemer te beperken.

- Bekijk welke eisen afgezwakt kunnen worden zonder de kwaliteit van het stelsel te verminderen.
- Is een one-size-fits-all manier van werken nodig? Of kan er ook enige ruimte komen voor het tunen voor specifieke toepassingen.
- Zorg voor een eenduidig normenkader en overeenstemming daarover tussen toezichthouder, PA en auditor.
- Biedt een betaalbare en laagdrempelige oplossing voor testcertificaten.
- Onderzoek de haalbaarheid van 'wildcard' PKIo.
- Overweeg uitgifte in 'eigen beheer' i.p.v. afnemen via commerciële TSPs.
- Differentiëren normenkaders tussen toepassingen.
- Verleng de doorlooptijd van (server) certificaten.
- Ondersteun afnemers met kennis en kunde.
- Sluit meer aan bij eIDAS.

Het creëren van ruimte voor innovaties kan ook helpen, zoals het op afstand identificeren van gebruikers in plaats van fysieke verschijning aan de balie.

Verbreding van de inzet van PKIo-certificaten is tot slot nog een andere manier om het gebruik ervan te stimuleren. Gedacht kan worden aan het verplicht gebruik van PKIo-certificaten in kritische of vitale infrastructuren, bijvoorbeeld op basis van de Wbni. Dit zal kostenverlagend en bewustzijnsverhogend werken.

Deze gecombineerde aanpak moet ertoe leiden dat PKIo binnen de overheid vanzelfsprekend wordt.

5.2 HERIJKEN PKIo

In diverse interviews en tijdens de expertconsultatiesessie kwam naar voren dat herijking van het PKIo stelsel nodig is. Destijds is de overheid gestart met PKIo op basis van een aantal uitgangsprincipes en doelstellingen. De focus lag primair op het verstrekken van persoonsgebonden certificaten en het bedienen van deze markt samen met private TSPs op basis van een grotendeels zelf uitgewerkt afsprakenkader. In de loop der jaren zijn er zaken veranderd: meer focus op server certificaten, een publieke en private root, veel aandacht voor het CAB-forum, en de komst van de Europese eIDAS verordening.

Ook voor het eventueel verplichten van PKIo toepassingen is een herijking wenselijk. Na een herijking zal het eenvoudiger zijn om bepaalde onderdelen van PKIo te verplichten.

Herijking is meer dan alleen 'de stofkam' door het stelsel halen om het 'lean and mean' te maken. Eén van de overwegingen die uit de interviews kwam was om uitgifte van PKIo certificaten te centraliseren onder eigen (overheids)beheer. Dit zou de kosten sterk kunnen drukken en de uitvoering van het stelsel vereenvoudigen. De eigen overheidsbrede TSP zou bijvoorbeeld door de huidige TSP van Defensie kunnen worden ingevuld of door een meer neutrale partij als Logius of DICTU. Daarmee wordt de rol van commerciële TSPs voor het overheidsdomein beperkt tot het leveren van infrastructuur componenten of kan zelfs wegvallen. De vraag is of dat laatste wenselijk is en zelfs toegestaan is.

Over de wenselijkheid van private TSPs kan het volgende worden gezegd. Het betrekken van private partijen bij PKIo komt voort uit marktwerking: concurrentie tussen TSPs verlaagt de prijs van certificaten, creëert betere dienstverlening en stimuleert innovaties. Echter, de prijs is hoog en de afgelopen jaren staan niet te boek als de meest innovatieve. De dienstverlening is wel verbeterd; er is veel gedaan om het gebruik van PKIo zo vriendelijk mogelijk te maken. Een situatie die enigszins te vergelijken is met het afsprakenstelsel voor elektronische toegangsdiensten waaronder eHerkenning valt.

Is het toegestaan? De overheid gaat geen PKIo aanbieden op de markt; het gebruik van PKIo-certificaten is vooral voor en door overheidsorganisaties en -diensten. Echter een publiek-privaat afsprakenstelsel kan niet zomaar worden beëindigd. Private partijen hebben geïnvesteerd om te voldoen aan PKIo en zullen ruimschoots de tijd moeten krijgen om zich voor te bereiden op de beëindiging en om te kunnen overstappen op een andere root CA. Vervolgens duurt het ongeveer drie jaar voordat alle certificaten zijn uitgefaseerd. Nog belangijker is de Wet Markt en Overheid, die de rechten van commerciële partijen regelt voor het PKIo domein. Of er ruimte is voor een publiek stelsel moet nader worden uitgezocht, maar de experts geven aan dat deze mogelijkheden beperkt zijn.

Als het gaat om uitgifte door slechts overheids-TSPs, dan is een complicerende factor is dat de overheid op dit moment ook PKIo-certificaten verstrekt aan private partijen zoals taxichauffeurs (I&W via KIWA) en zorgverleners en -organisaties (VWS via CIBG). Weliswaar op basis van wetgeving, maar bij een PKIo voor en door de overheid past dit minder goed. Wenselijk is dat private TSPs onder een andere root CA deze markten gaan bedienen om onterechte mededinging door de overheid te voorkomen.

Een omgekeerd scenario is ook denkbaar. Overheid-TSPs geven nu alleen certificaten uit t.b.v. de eigen overheidsorganisatie. Dat valt onder de noemer 'zelfvoorziening' en is uitgesloten als economische activiteit in de zin van de Wet Markt en Overheid. Als een overheids-TSP ook PKIo certificaten aan andere overheden kan leveren (als generieke overheidsdienst) noemt de Wet Markt en Overheid dit een economische activiteit omdat het breder gaat dan de eigen overheidsorganisatie. Er zijn in dat geval, vanuit deze wet, vier gedragsregels waar de overheid-TSP zich aan moet houden. De Nederlandse Mededingingsautoriteit (NMa) ziet toe op de naleving van deze regels. Dit zijn de regels:

- **Integrale kostendoorberekening: overheden moeten ten minste de integrale kosten van hun goederen of diensten in hun tarieven doorberekenen.** In het geval van PKIo moeten alle (vaste) kosten van de TSP organisatie en (variabele) kosten per certificaat uitgifte worden doorbelast. Een overheid-TSP kan wellicht efficiënter het uitgifte proces organiseren, bijvoorbeeld door decentraal beleggen van identiteitsverificatie en integratie met personeelsadministraties. De verwachting is dat de kostprijs die de overheid-TSP doorbelast lager is dan de tarieven van de commerciële TSP.
- **Bevoordelingverbod: overheden mogen hun eigen overheidsbedrijven niet bevoordelen ten opzichte van concurrerende bedrijven**. Zoals genoemd bij het vorige punt, zou een overheid-TSP voordelen kunnen hebben in het uitgifteproces doordat het gemakkelijker kan integreren/samenwerken met andere overheidspartijen. Dit voordeel hebben de commerciële partijen in beginsel niet. Wanneer ook niet-overheidafnemers bij de overheid-TSP terecht zouden moeten kunnen, kan dit voordeel niet worden ingezet. Het is niet aannemelijk dat een overheid-TSP goed is toegerust om certificaten uit te geven aan een niet-overheid afnemer.
- **Gegevensgebruik: overheden mogen de gegevens die ze vanuit hun publieke taak verkrijgen niet gebruiken voor economische activiteiten die niet dienen ter uitvoering van de publieke taak.** Deze lijkt voor uitgifte van PKIo certificaten niet van toepassing, tenzij de overheid-TSP een actief afnemersbestand tot haar beschikking heeft en deze inzet voor marketing en sales doeleinden.
- **Functiescheiding: als een overheid op een bepaald terrein een bestuurlijke (bijvoorbeeld toetsende) rol heeft voor bepaalde economische activiteiten en ook zelf die economische activiteiten uitvoert, mogen niet dezelfde personen betrokken zijn bij de uitoefening van de bestuurlijke bevoegdheid en bij het verrichten van de economische activiteiten van de overheidsorganisatie**. Agentschap Telecom (onderdeel van EZK) is toezichthouder onder eIDAS voor TSPs die o.a. PKIo certificaten uitgeven, Logius als onderdeel van BZK beheert het PKIo stelsel. Het voor de hand dat een overheid-TSP wordt uitgevoerd door Logius omdat daar nu al veel kennis en kunde is over PKIo en het inrichten van centrale voorzieningen. Een kanttekening is dat de TSP rol niet vermengd wordt met de PA rol.

Opgemerkt moet worden dat de technische infrastructuur kan worden ingekocht via aanbesteding van een van de commerciële aanbieders. Echter, hiervan kan slechts één partij of een klein consortium van partijen profiteren.

Kortom, een herijking van PKIo is niet triviaal en raakt diverse aspecten die van grote invloed kunnen zijn op een toekomstige andere inrichting ervan. De verwachting is dat vanuit de Wet Markt en Overheid er zeer beperkt ruimte is om invulling te geven aan een volledig publiek systeem. Nader onderzoek is nodig naar de mogelijkheden van verschillende inrichtingen van PKIo en de beleidsmatige impact die hiermee gepaard gaat. De eigenaar zal moeten kiezen voor een bepaalde inrichting van PKIo en hier naar moeten gaan handelen. Wenselijk is dit wel om beter duiding te kunnen geven aan verplichtende onderdelen van PKIo op langere termijn.

5.3 RISICO'S

Het verplichten van PKIoverheid gaat ook gepaard met potentiele risico's. Indien heel de overheid van rijksoverheid tot lagere overheden zouden overstappen op PKIoverheid dan ontstaat er een zwak punt: het wordt een interessant doelwit voor kwaadwillende actoren. Als het stelsel succesvol wordt aangevallen kan de gehele PKIo dienstverlening plat komen te liggen. Heel veel alternatieven zijn niet beschikbaar (alleen QuoVadis biedt iets anders aan).

De BIR schrijft in de rijksmaatregel 10.1.2.2. verplicht voor dat "Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn." In het PvE wordt hier geen rekening mee gehouden. Is het wenselijk om in Nederland slechts één alternatieve geregistreerde leverancier te hebben en aan welke eisen dienen alternatieve leveranciers te voldoen in het geval PKIoverheid gecompromitteerd raakt? Bij de herijking van PKIo is het dus ook noodzakelijk om aan risico analyse te maken en uitspraken te doen over alternatieve certificaten en leveranciers hiervan.

6. Conclusies en aanbevelingen

PKIoverheid (of PKIo) is een sterk merk voor Nederland, het straalt vertrouwen uit. PKIo wordt gezien als 'uitvoering van de Nederlandse wet' en het past goed om PKIoverheid als merk voor de overheid neer te zetten. In andere landen zijn er vergelijkbare stelsels. Echter, meestal zijn deze stelsels volledig door de overheid gecontroleerd; zelden zijn het publiek-private stelsels zoals bij PKIoverheid het geval is. Deze voordelen wegen op tegen het risico dat de sturing op stelsels als PKIoverheid door het mondiale karakter van het internet en de macht van het CAB-forum wordt beperkt. Of de PKIo-certificaten worden geaccepteerd door de webbrowsers van de Nederlandse burger of ondernemer, wordt in de praktijk bepaald door de internationale browserleveranciers. In het PKIoverheid stelsel hebben zij geen formele rol, maar hun besluiten kunnen wel vergaande implicaties hebben. Er is echter voldoende afstemming om dit risico te beperken.

Het gebruik van PKIo-certificaten is significant: meer dan 650.000 waren er in gebruik in 2017. Dit komt mede door het feit dat op diverse manieren de inzet van PKIo-certificaten verplicht wordt gesteld. Er zijn standaarden die het afdwingen (bijv. Digikoppeling), of voorzieningen zoals de BSN-diensten van de SBV-Z) en stelsels die het afgesproken hebben (bijv. eHerkenning en MedMij). Ook in vigerende beveiligingsbaselines zoals de BIR wordt het gebruik van PKIo voor veilige communicatie verplicht gesteld.

Het potentieel van PKIo is echter nog niet ten volle benut voor eigenlijk alle toepassingsmogelijkheden van certificaten (website beveiliging, server-to-server communicatie, digitaal waarmerken en authenticatie). Het gebruik van PKIo-certificaten voor de beveiliging van overheidswebsites wordt geschat op minder dan 50%. Redenen hiervoor zijn kosten, het ontbreken van de noodzaak om de website te beveiligen, en de beperkte beveiligingsmeerwaarde van PKIo-certificaten ten opzichte van andere (goedkopere) certificaten. Voor veilige communicatie tussen servers kiezen diverse overheidsorganisaties voor een eigen PKI. Dit doen ze vooral vanuit kostenoogpunt en om zelf controle te hebben over de uitgegeven certificaten. Binnen bepaalde domeinen geldt dit ook voor het gebruik van persoonsgebonden certificaten als authenticatiemiddel. Bij veel afnemers lopen de kosten enorm op als het PKIo-certificaten betreft. Daarnaast zijn er tal van andere authenticatie-oplossingen die een veel grotere dekkingsgraad genieten dan PKIoverheid op dit moment. Denk daarbij aan DigiD en de eHerkenningsmiddelen op niveau Substantieel. De concurrentie is groot binnen dit toepassingsgebied. Het sterk in opkomst zijnde toepassingsgebied van digitaal waarmerken biedt mogelijkheden voor PKIoverheid. Diverse overheidsorganisaties maken al gebruik van PKIo-certificaten om te waarmerken. Vooral als het communicatie betreft naar organisaties of personen buiten het overheidsdomein biedt een digitaal waarmerk met een PKIo-certificaat meerwaarde. Een soortgelijke redenering als bij de websites is hier van toepassing: vertrouwen en betrouwbaarheid.

De ervaringen en visies met PKIo die zijn opgehaald in het onderzoek zijn gestructureerd door middel van een SWOT-analyse. Er ontstaat een wisselend beeld over nut en noodzaak van PKIo, met veel sterke punten en kansen en ook veel zwaktes en bedreigingen. Verplicht stellen wordt gezien als de manier om het gebruik van PKIo te vergroten. De vraag is dan of door PKIoverheid verplicht te stellen de sterke punten worden versterkt. Bij website beveiliging, veilige communicatie tussen servers van overheidsorganisaties en waarmerken lijkt dit het geval. Voor de toepassingsgebieden van authenticatie en veilige communicatie met servers buiten het overheidsdomein is hiervan minder sprake. Het is verstandiger om voor deze toepassingen betrouwbaarheidsniveaus en alle erkende oplossingen die hier aan voldoen centraal te stellen. Dit past bij de Europese eIDAS verordening die de geldigheid van elk gekwalificeerd certificaat op het hele grondgebied, ongeacht het land van herkomst, garandeert met als doel de grenzen voor elektronische transacties in de EU op te heffen.

PKIoverheid heeft, in tegenstelling tot het stelsel gekwalificeerde certificaten van eIDAS, geen wettelijke grondslag. Wel is PKIoverheid compliant met eIDAS. In het wetsvoorstel Digitale Overheid zitten voldoende aspecten om toekomstig gebruik van PKIo-certificaten te stimuleren. Het wetsvoorstel bevat onderdelen zoals de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid, het stellen van regels over informatieveiligheid en de digitale toegang tot publieke dienstverlening voor burgers en bedrijven op basis van erkende middelen. Opgepast dient te worden dat teveel afbakenen van een Nederland-specifieke PKI mogelijk kan indruisen tegen het uitgangspunt van de eIDAS verordening, dat streeft naar een unieke digitale Europese markt. De Nederlandse overheid zal ook andere erkende certificaten die door eIDAS

gekwalificeerde TSPs worden uitgegeven moeten accepteren. Het is raadzaam om te inventariseren welke risico's dat met zich meebrengt en of mitigerende maatregelen nodig zijn. Vanuit wettelijk oogpunt is verplichtstelling van alleen PKIo-certificaten dus niet haalbaar. Vooral niet richting partijen buiten het overheidsdomein die met overheidsvoorzieningen moeten communiceren.

Daarnaast zijn er nog een tweetal andere mogelijkheden om het gebruik van PKIo-certificaten af te dwingen: opnemen in vigerende baselines voor beveiliging en plaatsing op de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie. In de BIR is al sprake van verplichting van PKIo. Met de scoping voor het gebruik van PKIoverheid voor bepaalde toepassingen lijkt plaatsing op de PTOLU-lijst dit keer wel haalbaar.

Een middel dat de andere middelen voor verplichting kan ondersteunen is het toepassen van verleidingstactieken. Door PKIo-certificaten gebruikersvriendelijker, vriendelijker geprijst of breder inzetbaar te maken zullen partijen sneller bereid zijn ermee aan de slag te gaan. Dit kan door bijvoorbeeld innovatieve toepassingen toe te staan voor TSPs bij de verstrekking van certificaten of door de mogelijkheden van het gebruik van PKIo-certificaten in bijvoorbeeld vitale of kritische sectoren en vanuit maatschappelijk belang te verkennen. De Wbni biedt voor dit laatste wellicht enig soelaas. Dergelijke tactieken dienen te worden ondersteund door een goede begeleidende communicatie vanuit PKIoverheid, want voor veel afnemers is PKIo zeer complexe materie.

De complexiteit van PKIo is een belangrijk aandachtspunt. Te overwegen valt om PKIoverheid te herijken: gelden de uitgangspunten van destijds nog steeds en geven de huidige afspraken en implementaties hieraan de juiste invulling? Een dergelijke herijking is meer dan alleen de 'stofkam' door het stelsel te halen zodat het weer een paar jaar verder kan. Wenselijk is ook dat er gekeken wordt naar de opzet van het stelsel als geheel en of deze past bij de eventueel nieuwe herijkte uitgangspunten. Past een publieke-private samenwerking hierbij of moet de overheid zelf in control zijn over de uitgifte van certificaten? Of moeten juist de private partijen het verstrekken van certificaten voor hun rekening nemen met daarbij de overheid slechts in de rol van eigenaar, zoals bij eHerkenning bijvoorbeeld het geval is. Dergelijke structurele aanpassingen van PKIoverheid zijn niet triviaal en raken al snel de Wet markt en overheid. Nader onderzoek is nodig naar de mogelijkheden van verschillende inrichtingen van PKIo en de beleidsmatige impact die hiermee gepaard gaat. De eigenaar zal moeten kiezen voor een bepaalde inrichting van PKIo en hier naar moeten gaan handelen. Wenselijk is dit wel om beter duiding te kunnen geven aan verplichtende onderdelen van PKIo op langere termijn.

Samenvattend:

- Verplichting PKIo voor beveiliging van overheidswebsites, digitaal waarmerken en server-to-server communicatie binnen overheid.
- De mogelijkheid om PKIo toe te passen voor andere toepassingen is niet verplicht maar wel mogelijk.
- Verplichting vooralsnog via handreikingen en richtlijnen (bijv. BIR) en opname in Pas-toe-of-leg-uit lijst.
- Verplichting laten samengaan met een communicatiecampagne, o.a. richting afnemers in het algemeen over de voordelen van PKIo, en specifiek ook richting beleid.
- Herijking PKIo afsprakenstelsel om complexiteit te reduceren en ruimte te creëren voor vernieuwing (zoals bijv. in het uitgifte proces).
- Bij herijking hoort ook een keuze maken rond de scope van verplichting van PKIo: PKIo voor alle overheidsdiensten in een publiek-privaat stelsel, PKIo alleen binnen het overheidsdomein met publieke en private TSPs of PKI alleen binnen het overheidsdomein met een publieke TSP.
- Keuze om toepassing van PKIo buiten het overheidsdomein te laten groeien, typisch voor kritische of vitale infrastructuren (zoals nu voor zorgsector of taxibranche).

Bijlage 1 Interviews

Overzicht geïnterviewde organisaties:

- Agentschap Telecom
- Ministerie van Algemene Zaken
- Cleverbase
- DICTU
- Gemeente Den Haag
- Gemeente Twenterand
- Ministerie van Justitie en Veiligheid
- KPN
- Logius
- Ministerie van Defensie
- Provincie Drenthe
- QuoVadis
- RDW
- Rijkspas
- Ministerie van Volkgezondheid, Welzijn en Sport
- VNG Realisatie

Bijlage 2 Expertconsultatie

Overzicht organisaties met afvaardiging in de expertsessie van 14 februari 2019:

- Ministerie van Algemene Zaken
- Cleverbase
- Digidentity
- Forum Standaardisatie
- Gemeente Den Haag
- Ministerie van Justitie en Veiligheid
- Logius
- Ministerie van BZK
- Ministerie van Defensie
- QuoVadis