Forumadvies ACME

Vergadering:	Forum Standaardisatie 25 juni 2025
Agendapunt:	04A
Documentnummer:	04A
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	6 juni 2025
Versie:	1.0
Bijlagen:	Intakadvies ACME Expertadvies ACME Verslag reacties openbare consultatie ACME
Rechten	CC0 publieke domein verklaring

1 Advies

Het Forum Standaardisatie adviseert om de standaard Automatic Certificate Management Environment (ACME) te verplichten aan de overheid (‘Pas toe of leg uit’) door deze met een nieuwe plaatsing toe te voegen aan 'Pas toe of leg uit'-lijst van het Forum Standaardisatie voor het automatisch verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten. Voor niet-publiek vertrouwde TLS-certificaten adviseert het Forum Standaardisatie om ACME niet te verplichten, maar aan te bevelen.

Daarnaast adviseert het Forum Standaardisatie om ACME niet te verplichten voor domeinvalidatie. Hoewel dat wel mogelijk is met ACME, zijn er alternatieven en goedwerkende andere methoden voor domeinvalidatie beschikbaar. Domeinvalidatie kan buiten het ACME-proces om plaatsvinden. ACME biedt middels External Account Binding (EAB) de mogelijkheid een ACME-account te koppelen aan een account bij de Certificate Authority (CA). Dit account kan al via andere methoden gevalideerde domeinen hebben. Kortom: ACME wel verplichten voor de certificaattransacties en niet voor validatie.

Op dit moment is er geen nationale organisatie die de regierol op zich neemt ter bevordering van de adoptie van de internationale standaard ACME in Nederland. Ook is er geen

vertegenwoordiging van de Nederlandse belangen bij de doorontwikkeling van ACME. Dit zijn aandachtspunten. Het Forum Standaardisatie kan overwegen het predicaat 'Erkende Nederlandse Intermediair' aan een Nederlandse intermediaire organisatie voor ACME toe te kennen.

Het voorgestelde functioneel toepassingsgebied voor ACME is:

> ACME moet worden toegepast voor het automatiseren van de interactie tussen certificaatautoriteiten en certificaatgebruikers, met als doel het proces van het verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten wendbaarder en betrouwbaarder te maken.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam en de experts die daarbij betrokken waren. Hoofdstuk 4 beschrijft de resultaten van de toetsing van de standaard tegen de criteria voor opname op de lijst. Tenslotte geeft hoofdstuk 5 aanvullende adviezen om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

Het Automatic Certificate Management Environment (ACME) is een protocol voor het geautomatiseerd verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten die onder andere kunnen worden ingezet om het gegevensverkeer tussen de browser van de eindgebruiker en de server waar de site gehost is te versleutelen. Een op die manier beveiligde website is te herkennen aan het slotje in de adresbalk. Ook mailverkeer kan met deze certificaten worden beveiligd.

Deze TLS-certificaten (Public Key Infrastructure (PKI)-certificaten) zijn unieke sleutels waarmee digitale systemen zich identificeren bij het online verbinden met een ander systeem. Ze hebben echter een afgebakende geldigheidsduur en het beheer van deze certificaten brengt het nodige handwerk met zich mee. Zo leidt het niet tijdig verlengen of het maken van fouten bij verlengen van certificaten met enige regelmaat tot het niet beschikbaar zijn van (overheids)websites of -systemen. De toepassing van ACME maakt het beheer van deze certificaten efficiënter en aanmerkelijk minder foutgevoelig. Ook maakt gebruik van ACME het overstappen naar een andere certificaatleverancier eenvoudiger.

ACME heeft brede bekendheid en populariteit verworven dankzij de gratis certificaten van Let's Encrypt, een non-profit organisatie en de grootste certificaatautoriteit ter wereld die door meer dan 570 miljoen websites wordt gebruikt. Hoewel Let's Encrypt een belangrijke rol heeft gespeeld in de ontwikkeling en promotie van ACME, is het belangrijk te benadrukken dat ACME niet exclusief aan Let's Encrypt is gebonden. Het protocol wordt inmiddels breed ondersteund door alle grote Certificate Authorities (CA's), zoals DigiCert, Sectigo, GoDaddy, GlobalSign, Let's Encrypt, ZeroSSL en Buypass.

2.2 Waarom is deze standaard belangrijk?

Het automatiseren van certificaatbeheer door de overheid op basis van ACME zorgt voor het efficiënter en betrouwbaarder verkrijgen, vernieuwen en intrekken van TLS-certificaten. Dit maakt de digitale overheid betrouwbaarder, wendbaarder en minder leveranciersafhankelijk.

Het gebruik van ACME draagt bij aan de bereikbaarheid en betrouwbaarheid van de digitale overheid, onder andere in de vorm van een hoge en doorlopende beschikbaarheid van overheidswebsites en overheidssystemen via het web. Als de geldigheidsduur van TLS-certificaten voor de beveiliging van websites en systemen verloopt omdat deze certificaten niet tijdig en/of niet goed worden vernieuwd, zijn deze gecertificeerde websites en systemen niet meer goed bereikbaar en betrouwbaar. Burgers en bedrijven hebben hierdoor geen betrouwbare toegang meer tot (informatie van) overheidsorganisaties en kunnen geen gegevens meer met hen uitwisselen. Daarom is het voor de overheid van belang om het levenscyclusbeheer van de gebruikte TLS-certificaten op orde te hebben.

Daarnaast vermindert het gebruik van ACME de beheerlast voor het beheer van TLS-certificaten door het beheer te automatiseren. De schaalbaarheid en betrouwbaarheid van certificaatbeheer wordt hiermee aanzienlijk verbeterd. Met de toename van het aantal websites en de ontwikkeling naar een kortere geldigheidsduur van TLS-certificaten wordt het steeds minder haalbaar om TLS-certificaten handmatig tijdig en correct te vernieuwen. Zo heeft het CA/Browser Forum – een gezaghebbend internationaal forum met als leden de grootste certificaatautoriteiten en browserontwikkelaars, waaronder Apple, Brave, Google, Microsoft, Mozilla en Opera – de stapsgewijze reductie aangekondigd van de geldigheid van TLS-certificaten naar uiteindelijk 47 dagen per 15 maart 2029.

Ook helpt ACME de leveranciersafhankelijkheid te verminderen. Omdat ACME een gestandaardiseerd protocol is, zijn TLS-certificaten en automatiseringsprocessen niet afhankelijk van de specifieke implementatie van een Certificate Authority (CA). Dit maakt de portabiliteit eenvoudiger tussen verschillende systemen en providers.

Tot slot is ACME ook cruciaal voor crypto-agility. Door het automatiseren van certificaatbeheer kunnen organisaties sneller schakelen tussen cryptografische standaarden. Dit maakt het eenvoudiger om kwetsbare algoritmen te vervangen en nieuwe technologieën, zoals post-quantum cryptografie, te integreren. Door de gestandaardiseerde en flexibele aanpak ondersteunt ACME een snellere reactie op beveiligingsincidenten en een toekomstbestendig cryptografisch beleid.

3 Betrokkenen en proces

3.1 Gevolgde procedure

Op 23 oktober 2023 heeft Rijkswaterstaat ACME (RFC8555) aangemeld om te toetsen of de standaard geschikt is om aan te bevelen aan de overheid via plaatsing op de lijst aanbevolen standaarden.

Op 26 februari 2024 heeft het intakegesprek plaatsgevonden met de indieners, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. In dit gesprek is onderzocht of ACME voldoet aan de criteria om in procedure genomen te worden. De resultaten van het onderzoek zijn vastgelegd in het intakeadvies.

Op basis van dit intakeadvies heeft het Forum Standaardisatie op 19 juni 2024 besloten de standaard in procedure te nemen. Vervolgens heeft de procedurebegeleider in overleg met Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld. Hoofdstuk 3.2 geeft de samenstelling van de expertgroep weer.

De expertgroep is op vrijdag 15 november 2024 online bijeengekomen in plaats van fysiek wegens een staking van het personeel van spoorwegbeheerder Prorail om de standaard te toetsen op basis van de inhoudelijke hoofdcriteria en om geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en het organisatorisch werkingsgebied vastgesteld. Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies is extra aandacht besteed aan de volgende punten:

- of ACME geschikt is om te verplichten of aan te bevelen aan de overheid;
- het draagvlak voor en de adoptie van de standaard door overheidspartijen;
- het beleggen van de regierol voor deze internationale standaard bij een geschikte nationale organisatie ter bevordering van de adoptie in Nederland en vertegenwoordiging van de Nederlandse belangen bij de doorontwikkeling van ACME.

De uitkomst van het expertonderzoek is vastgelegd in het expertadvies.

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie op internetconsultatie.nl van 19 februari 2025 tot 19 maart 2025. In de openbare consultatie zijn vier reacties, waarvan één niet-openbaar, ontvangen, te weten van Sig-I/O Automatisering, Solstice en twee anonieme reacties. Na sluiting van de consultatie zijn per mail de reacties ontvangen van de Ministeries van JenV en AenM en de G4. Bureau Forum Standaardisatie heeft geoordeeld dat deze reacties als reacties uit de openbare consultatie in het verslag worden opgenomen.

Dit Forumadvies is opgesteld op basis van het expertadvies, de reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie. Indien het Forum Standaardisatie instemt met dit advies, wordt het aan het OBDO ter besluitvorming voorgelegd.

3.2 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt.

Aan de expertbijeenkomst hebben deelgenomen:

- John van Agthoven (Rijkswaterstaat – Indiener)

- Jochem van den Berge (Logius)
- Rob Brand (Ministerie Economische Zaken)
- Paul van Brouwershaven (Entrust)
- Marco Davids (SIDN)
- Danny Emmerik (SSC-ICT)
- Joost Gadellaa (SURF)
- Koen Sandbrink (NCSC)
- Johan de Vroom (DICTU)
- Peter Wiggers (ICTU / Digilab)

Aan de experts is gevraagd of zij bezwaar hebben om met naam in het expertadvies te worden genoemd. De experts hebben verklaard daartegen geen bezwaar te hebben.

Als onafhankelijk voorzitter is opgetreden Claudia Vermeulen, Managing Partner bij InnoValor Advies. Ruud Kosman, Managing Partner van InnoValor Advies, heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Joram Verspaget, Bart Knubben en Benjamin Broersma van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

3.3 Resultaat van het expertonderzoek

De geconsulteerde experts adviseren om ACME te verplichten aan de overheid (‘Pas toe of leg uit’) via plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie voor het automatisch verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten. Voor niet-publiek vertrouwde TLS-certificaten adviseren de experts om ACME niet te verplichten, maar aan te bevelen.

Daarnaast adviseren de experts om ACME niet te verplichten voor domeinvalidatie. Hoewel dat wel mogelijk is met ACME, zijn er alternatieven en goedwerkende andere methoden voor domeinvalidatie beschikbaar. Domeinvalidatie kan buiten het ACME-proces om plaatsvinden.

3.4 Resultaat van de openbare consultatie

Hieronder volgt een samenvatting van de reacties uit de openbare consultatie en de reactie hierop van de indiener. De volledige reacties uit de openbare consultatie zijn in het consultatieverslag bijgevoegd.

3.4.1 Reactie van Anoniem

De naam van de reageerder en diens organisatie zijn bekend bij Bureau Forum Standaardisatie.

[Austerlitz, 20 februari 2025]

Volgens de reageerder kan het gebruik van ACME ook op officiële .gov.nl domeinnamen bijdragen aan phishing, omdat mensen het niet begrijpen of er niet op letten. Daarnaast

wordt gewaarschuwd dat de invoering van de European Digital Identity Wallet (EDIW/EUDIW) kan leiden tot een toename van identiteitsfraude.

3.4.2 Reactie van indiener Rijkswaterstaat op Anoniem

Rijkswaterstaat stelt dat het een goed idee is om extra te toetsen of het gebruik van ACME in combinatie met External Account Binding (EAB) geen risico's oplevert voor phishing en identiteitsfraude. De aanvraag richt zich op het beheer van certificaten, niet op de keuze voor een betrouwbare Certificate Authority (CA). Het door de reageerder aangehaalde bericht op security.nl gaat over het gebruik van certificaten, terwijl deze aanvraag specifiek het beheer betreft. In combinatie met de opmaat BIO 2.0 norm 5.14.3, waarin het gebruik van OV-certificaten is voorgeschreven, biedt ACME met EAB een open standaard voor geautomatiseerd handmatig beheer. Zodra een betere open standaard beschikbaar komt, kunnen organisaties die zelf aanmelden.

3.4.3 Reactie van Sig-I/O Automatisering

De naam van de reageerder is bekend bij Bureau Forum Standaardisatie.

Sig-I/O Automatisering beveelt aan om het gebruik van ACME binnen de overheid zoveel mogelijk te stimuleren. Het huidige proces van certificaataanvragen wordt als omslachtig, foutgevoelig, duur en met een lange doorlooptijd ervaren. De invoering en verplichting van ACME kan hierin helpen. Er wordt opgemerkt dat veel departementen en afdelingen nog steeds verplicht EV-certificaten afnemen, terwijl deze tegenwoordig geen toegevoegde waarde of herkenbaarheid voor de eindgebruiker hebben. Het advies hierbij is om waar mogelijk ACME te gebruiken, aangezien het de hoeveelheid handmatig werk en foutgevoeligheid flink beperkt. Wat betreft de verplichting van de standaard voor overheidsorganisaties geeft de reageerder vanuit persoonlijke ervaring aan dat er bij het ministerie waar reageerder werkzaam is een verplichting geldt om PKI-O certificaten af te nemen voor productieomgevingen. Deze PKI-O certificaten kunnen nog niet met behulp van ACME worden aangevraagd en de procedure hiervoor en de bijbehorende kosten zijn significant. Tot slot wordt aangegeven dat ACME al binnen het Ministerie van Volksgezondheid, Welzijn en Sport uitgebreid wordt gebruikt.

3.4.4 Reactie van indiener Rijkswaterstaat op Sig-I/O Automatisering

De indiener benadrukt dat de aanvraag niet gaat over het kiezen van een betrouwbare CA. In de opmaat BIO 2.0 norm 5.14.3 staat het volgende: *Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.* ACME met External Account Binding (EAB) maakt dit op een geautomatiseerde manier mogelijk.

3.4.5 Reactie van Anoniem

De naam van de reageerder en diens organisatie zijn bekend bij Bureau Forum Standaardisatie.

[Den Haag, 11 maart 2025]

De reageerder beveelt aan om het geautomatiseerd verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten te verplichten, bij voorkeur met ACME, maar met de mogelijkheid om ook andere geautomatiseerde oplossingen toe te staan. Dit houdt het geautomatiseerde certificatenbeheer open naar de toekomst. Zo wordt ruimte geboden om andere oplossingen te onderzoeken in omgevingen waar niet alleen publieke certificaten worden gebruikt, maar bijvoorbeeld ook private certificaten en *self signed* certificaten, als onderdeel van een geïntegreerde aanpak voor de gehele automatisering van [het beheer] van certificaten.

Wat betreft de kosten van implementatie merkt de reageerder op dat organisaties met veel teams die slechts een of een klein aantal websites beheren, centrale voorzieningen voor ACME moeten opzetten of ondersteunen. Hierdoor wordt voorkomen dat elk team zelf verantwoordelijk is voor de implementatie. Als organisaties dit niet centraal regelen of ondersteunen, is het de vraag of de kosten van implementatie acceptabel zijn.

3.4.6 Reactie van indiener Rijkswaterstaat op Anoniem

De indiener benadrukt dat deze aanvraag niet gaat om het kiezen van een betrouwbare CA. In de opmaat BIO 2.0 norm 5.14.3 staat het volgende: *Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.* ACME met External Account Binding (EAB) maakt dit op een geautomatiseerde manier mogelijk.

Het voordeel van het kiezen van één open standaard, in tegenstelling tot meerdere geautomatiseerde oplossingen, is dat organisaties makkelijker kunnen veranderen van CA-leverancier, zonder de automatisering grondig aan te moeten passen. Zodra een betere open standaard zich aandient, kan deze uiteraard worden aangemeld. Iedere organisatie kan een nieuwe standaard aanmelden.

Wat betreft de kosten van implementatie wijst de reageerder erop dat organisaties met veel teams die slechts een of een klein aantal websites beheren, binnen de organisatie centrale voorzieningen voor ACME moeten opzetten of ondersteunen. Rijkswaterstaat erkent dit en stelt dat het een goede overweging is om op te nemen in een implementatiehandreiking, zodat elke organisatie een goede basis heeft om een gedegen besluit te nemen.

3.4.7 Reactie van Luc Nieland (Solstice)

Luc Nieland (Solstice) vindt het een goed advies van de experts om ACME verplicht te stellen aan de overheid. Deze werkwijze is efficiënt, goed reproduceerbaar en kwaliteitsverhogend.

Bovendien zou dit ook leiden tot kostenverlaging. Behalve de invoering van deze nieuwe werkwijze ziet Nieland geen nadelen.

3.4.8 Reactie van indiener Rijkswaterstaat op Luc Nieland (Solstice)

De indiener heeft geen opmerkingen op de reactie van Luc Nieland.

3.4.9 Reactie van de Ministeries van JenV en AenM

De naam van de reageerder is bekend bij Bureau Forum Standaardisatie.

Volgens de reageerder kiest de indiener de naam wat ongelukkig. ACME is immers ook de naam van de fictieve fabriek uit de Road Runner-tekenfilmserie waar Wile E. Coyote zijn bestrijdingsmiddelen voor de Roadrunner kocht. Veel gemeenten maken gebruik van Let's Encrypt, wat een positieve ontwikkeling is. De keuze voor betrouwbare (Europese) CA's is echter buiten beeld gebleven. Dit aspect mag niet terugkomen in het (expert)advies. CA's moeten naast ACME ook op de trusted list van de EU staan, zeker gezien de geopolitieke spanningen, die de beschikbaarheid van een CA van buiten de EU negatief kunnen beïnvloeden. Het voorstel en het advies besteden onvoldoende aandacht aan de implementatie van ACME. Er moet een geautomatiseerde koppeling zijn tussen de server waarop de dienst wordt gehost, de CA die het nieuwe certificaat uitgeeft en de oude intrekken door het te plaatsen op de CLR. Het toepassen van ACME vereist meer dan alleen een instelling op een server of applicatie. Daarnaast ontbreken in het advies en de expertanalyse een impactweging. Het zou problematisch zijn als het onderhoud van certificaten van buitenaf beïnvloed kan worden.

3.4.10 Reactie van indiener Rijkswaterstaat op de Ministeries van JenV en AenM

Warner Bros gebruikt de naam ACME voor de fabriek in meerdere van hun titels. De naam is vermoedelijk afgeleid van het Griekse ἀκμή, wat 'piek' of 'hoogste punt' betekent. Rijkswaterstaat koos de afkorting niet zelf, maar wijst erop dat de makers van de standaard duidelijk een knipoog beoogden. Om humor te vermijden en de zoekresultaten te verbeteren, stelt de indiener voor om RFC 8555 (of ACME Protocol) als roepnaam te gebruiken.

Volgens de Ministeries van Justitie en Veiligheid en Asiel en Migratie moeten CA's naast ACME ook op de trusted list van de Europese Unie (EU) staan, zeker gezien de geopolitieke spanningen, die de beschikbaarheid van een CA van buiten de EU negatief kunnen beïnvloeden. De indiener stemt in met de insteek en het sentiment van het voorstel, maar geeft aan dat de relevantie voor dit voorstel onduidelijk is. Het kiezen van een betrouwbare (Europese) CA is nu al belangrijk en het voorstel heeft daar geen negatieve invloed op. Bij het selecteren van een CA wordt verder gekeken dan alleen naar het wel of niet ondersteunen van ACME. Een betrouwbare CA is slechts één aspect van betrouwbaar certificaatbeheer. Het voorstel draait niet om Lets's Encrypt als CA, maar om het technische protocol. Omdat Let's Encrypt alleen maar ACME ondersteunt, wordt de groei van Let's Encrypt gezien als een teken van draagvlak voor ACME en een afname van de voorkeur voor

huidige werkwijze (en kosten) van CA's. Als zoveel mogelijk CA's standaardiseren op ACME, maakt dit voor een organisatie gemakkelijker om te migreren van Let's Encrypt, mocht de noodzaak zich voordoen.

Het gebruik van een standaardprotocol maakt organisaties wendbaarder in het kiezen van een nieuwe CA. Ze kunnen zelf een back-up CA in huis hebben en in korte tijd naar deze CA migreren door het gebruik van hetzelfde protocol. Dit stelt kleinere CA's in staat zich te richten op één standaard en daar wijzigingen op aan te dragen in plaats van zelf alles te ontwikkelen. De betrouwbaarheid van ACME als protocol is te correleren aan de betrouwbaarheid van de Internet Engineering Task Force (IETF), die de standaard beheert. Het kan geen kwaad om als overheid hier extra onderzoek naar te (laten) doen, aangezien het al breed wordt ingezet met Let's Encrypt als CA.

Volgens de Ministeries van Justitie en Veiligheid en Asiel en Migratie besteedt het voorstel en het advies onvoldoende aandacht aan de implementatie van ACME. Volgens de indiener verschilt de impact per organisatie, aangezien de infrastructuur en applicaties variëren. Het is duidelijk dat de impact van de status 'Pas toe of leg uit' groter is dan de status aanbevolen. De werking van de koppeling met de CA is beschreven in de RFC.

Rijkswaterstaat:

1. De eigen (solution) architecten en techneuten moeten kennis hebben.
   A. Er moet een handreiking komen (geleverd door NBV, onder regie van de CTO Rijk) voor de implementatie, zodat het organisaties gemakkelijker wordt gemaakt.
      i. Deze handreiking moet ook de meer technische details bevatten.
   B. Elke organisatie kan de technische impact zelf bepalen, en de handreiking kan daarbij helpen.
   C. Kennis, documentatie en cursussen zijn op veel plekken beschikbaar.
   D. De account key waarmee bij de CA wordt geauthentiseerd, moet goed beschermd worden.
2. CA moet ACME ondersteunen
   A. Als de huidige CA ACME niet ondersteunt:
      i. Vernieuw de verlopende certificaten op de huidige manier en plan vooruit.
      ii. Neem bij de volgende aanbesteding de eis op dat ACME ondersteund moet worden.
      iii. Bij 'Pas toe of leg uit': neem de afwijking organisatiebreed op als explain en borg de oplossing/migratieplan.
3. Gebruikte applicaties moeten ACME ondersteunen.
   A. Als de applicatie ACME niet ondersteunt:
      i. Vernieuw de verlopende certificaten op de huidige manier en plan vooruit.
      ii. Neem bij eventuele aanbesteding mee dat ACME ondersteund moet worden.
      iii. Bij 'Pas toe of leg uit' en de eerstvolgende toets: neem de afwijking op als explain en borg de oplossing/migratieplan.

Impact bij CA:

1. Bij 'Pas toe of leg uit' sluit een aanbesteding een CA uit als deze geen ondersteuning biedt voor ACME (must-have).
2. Bij aanbevolen krijgt een CA met ACME-ondersteuning extra punten (should-have).
3. Dit moedigt CA's aan die ACME nog niet ondersteunen, om mee te doen met de standaard.

Impact bij applicatieleveranciers:

1. Dit geldt hetzelfde als voor de CA's.
2. Uiteindelijk verlaagt dit de kans op verlopen certificaten, wat de beschikbaarheid verhoogt.
3. Bij applicatieleveranciers die nu al gebruikmaken van Let's Encrypt, komen er meer opties beschikbaar in de vorm van andere CA's die ook ACME ondersteunen, evenals OV/EV met EAB.

De Ministeries van Justitie en Veiligheid en Asiel en Migratie stellen de vraag hoe extern vastgesteld kan worden dat aan de standaard is voldaan, terwijl het tegelijkertijd problematisch zou zijn als het onderhoud van buitenaf kan worden bekeken. Van buitenaf kan niet gezien worden hoe certificaten worden geplaatst of vervangen. Een audit bij de applicatiebeheerders of de CA kan dit echter wel vaststellen per URL.

Certificaten met korte geldigheid impliceren dat ze automatisch worden vervangen, terwijl een lange geldigheidsduur een handmatig proces impliceert. Dit biedt indirecte controle. In de huidige situatie is het een gegeven dat Let's Encrypt als CA ACME gebruikt. Let's Encrypt wordt echter als "minder betrouwbaar" beschouwd, waardoor het handig is om ook andere CA's te gebruiken die ACME ondersteunen. Zo kunnen de huidige Let's Encrypt-certificaten waar nodig worden vervangen, zonder verlies van automatisering. De migratiekosten blijven beperkt tot het veranderen van de verwijzing naar het account van de nieuwe CA en de kosten van de certificaten zelf. Aan OV- en EV-certificaten zijn extra kosten verbonden, maar OV is volgens informatie verplicht. ACME in combinatie met EAB biedt hier een mooie oplossing voor. De handmatige methode voor het onderhoud van certificaten is vatbaarder voor externe beïnvloeding (bijvoorbeeld door phishing) dan de geautomatiseerde methode.

3.4.11 Reactie van G4 (Peter den Held)

ACME automatiseert de uitgifte en het beheer van digitale certificaten, wat voordelen biedt op het gebied van beveiliging, efficiëntie en het verminderen van menselijke fouten. Het protocol automatiseert de uitgifte en verlenging van certificaten, waardoor het risico op verlopen certificaten wordt verminderd en de beveiliging wordt verbeterd. Ook maakt ACME het eenvoudiger om best practices voor certificaatbeheer te implementeren.

De implementatie van ACME heeft echter enkele nadelen. Niet alle leveranciers ondersteunen het protocol native, wat kan leiden tot extra kosten en beheerlasten bij het aanpassen aan het protocol.

Een betere benadering zou zijn om ACME op de lijst van aanbevolen standaarden te plaatsen, waardoor de adoptie van het protocol gestimuleerd wordt zonder de afdwingende

verplichtingen van de 'Pas toe of leg uit'-lijst. Dit biedt de mogelijkheid om het protocol breder te implementeren wanneer de ondersteuning bij leveranciers verbetert.

3.4.12 Reactie van indiener Rijkswaterstaat op G4

Volgens de G4 neemt de adoptie van ACME toe, maar ondersteunen niet alle leveranciers het protocol volledig. Volgens Rijkswaterstaat creëert dit een kip-ei situatie, waarbij de vraag is of “aanbevolen” voldoende is voor leveranciers om naar een uniforme standaard toe te werken. Wordt iets pas verplicht als alle leveranciers iets ondersteunen? Er moet ergens een kantelpunt tussen ‘aanbevolen’ en 'Pas toe of leg uit' worden gedefinieerd. Het is uiteindelijk niet aan de indiener om de juiste timing te bepalen.

Volgens de G4 zou de uitvraag van ACME kunnen leiden tot veel uitleg en lastige gesprekken met leveranciers die het protocol nog niet kunnen implementeren en mogelijk extra kosten bij noodzakelijke aanpassingen. Volgens Rijkswaterstaat kan het uitblijven van reacties van leveranciers op de consultatie betekenen dat zij er geen hinder van ondervinden of de opname in de lijst niet relevant vinden. Rijkswaterstaat denkt echter dat de betere leveranciers dit met weinig moeite kunnen implementeren en het als voordeel zien.

Volgens de G4 zou het implementeren van ACME betekenen dat aanvullende software van derden nodig is, wat extra beheerlast met zich meebrengt. Rijkswaterstaat stelt de vraag: Als handmatig beheer van certificaten tot een hogere beheerlast leidt dan automatisch beheer, waarom wordt ACME (met Let’s Encrypt) dan zoveel toegepast? De algemene mening onder beheerders is dat automatisering de beheerlast vermindert. Het betreft inderdaad een vergelijking tussen kapitaaluitgaven (de investering) en operationele uitgaven (het onderhoud). Er is een initiële investering nodig om de kosten op termijn terug te verdienen. Ook hier gaat het om de vraag: ‘Wanneer komt dit uit?’

Volgens de G4 is het beter om afwijkingen van standaarden te beperken, en alleen toe te staan als een dienst of product ondermaats functioneert, onvoldoende veilig is, of als er andere zwaarwegende redenen zijn. Rijkswaterstaat is het hier helemaal mee eens. Gewetensvraag: Is een product veilig genoeg zonder de verbeterde beveiliging die hierboven is gemeld?

De G4 geeft aan dat een betere manier om de adoptie van ACME door overheidspartijen te stimuleren is door het op de lijst van aanbevolen standaarden te plaatsen. Volgens Rijkswaterstaat gaat het uiteindelijk om de vraag wat Forum Standaardisatie en de overheid willen bereiken met de opname van de standaard op de 'Pas toe of leg uit'-lijst in plaats van op de lijst aanbevolen standaarden, aangezien de 'Pas toe of leg uit'-lijst een hogere urgentie aangeeft. Vragen zijn: hoe hoog is de urgentie om het beheer van certificaten te standaardiseren en automatiseren en wegen de voordelen op tegen de nadelen?

4 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor verplichten (‘Pas toe of leg uit’) of aanbevelen aan de overheid:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Bevordert opname van de standaard op de 'Pas toe of leg uit'-lijst de adoptie?

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan op de website van het Forum Standaardisatie. Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing op basis van het expertadvies, de reacties uit de openbare consultatie en de inzichten van de leden van het Forum Standaardisatie.

4.1 Toegevoegde waarde

De toetsingsprocedure wijst uit dat ACME voldoet aan het criterium 'Toegevoegde waarde'.

Het voorgestelde functioneel toepassingsgebied voor ACME is:

> ACME moet worden toegepast voor het automatiseren van de interactie tussen certificaatautoriteiten en certificaatgebruikers, met als doel het proces van het verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten wendbaarder en betrouwbaarder te maken.

ACME sluit goed aan op TLS en werkt samen met de standaard Certification Authority Authorization (CAA). Voorwaarde is dat de CA die via ACME wordt gebruikt is opgenomen in de CAA-records van het domein. Dit versterkt de beveiliging zonder in te boeten op de voordelen van geautomatiseerd certificaatbeheer. Daarnaast kan ACME worden gebruikt in combinatie met HTTPS. In feite is ACME ontworpen om het verkrijgen en beheren van TLS-certificaten (die HTTPS mogelijk maken) te automatiseren en te vereenvoudigen. Hoewel ACME het beheer van TLS-certificaten sterk vereenvoudigt, brengt het extra complexiteit en risico's op fouten met zich mee voor toepassingen zoals STARTTLS en DANE.

De korte levensduur van TLS-certificaten kan leiden tot mismatches tussen het vernieuwde TLS-certificaat en de bijbehorende DNS TLSA-records. Zorgvuldige configuratie kan deze risico's beperken. Een handleiding en toelichting is hierbij gewenst voor gebruikers om de configuratie op de juiste manier in te richten. *Provisioning* daarentegen is het proces waarbij middelen en configuraties automatisch worden toegewezen en beheerd, zodat systemen snel en flexibel kunnen inspelen op veranderingen. Hoewel *provisioning* geen inherent onderdeel is van ACME, is dit wel een gewenste aanvulling om de wendbaarheid van het systeem te vergroten.

ACME automatiseert het verkrijgen, vernieuwen en intrekken van TLS-certificaten en ondersteunt daarbij het tot stand brengen van een beveiligde verbinding op basis van TLS. Het Simple Certificate Enrolment Protocol (SCEP) was een eerdere poging op een geautomatiseerd TLS-certificaat uitgifte protocol. Voor ACME ligt de focus op publieke TLS-certificaten, wat bij SCEP niet het geval is.

De implementatie van ACME kan een initiële investering met zich meebrengen. Echter, door de implementatie van ACME kunnen organisaties aanzienlijke besparingen realiseren op het

gebied van certificaatbeheer. Met ACME kunnen TLS-certificaten automatisch worden uitgegeven, vernieuwd en ingetrokken, waardoor handmatige handelingen en menselijke fouten worden geminimaliseerd. Daarnaast biedt ACME ook voordelen op het gebied van leveranciersonafhankelijkheid.

De beveiligingsrisico's en privacyrisico's voor overheidsbrede adoptie van ACME zijn acceptabel. Handmatige stappen en eventueel versturen van gevoelige data via e-mail of andere onveilige methodes voor het certificatenbeheer worden dankzij automatisering middels ACME vermeden. Wel bestaan er verschillende beveiligingsrisico's voor ACME. Een belangrijk risico is de aanwezigheid van een Single Point of Failure (SPoF), hoewel dit relatief eenvoudig te mitigeren is door redundantie in te bouwen. Bij het gebruik van ACME met External Account Binding (EAB) kan authenticatie buiten het reguliere proces plaatsvinden ("*out of band*"), wat extra beveiliging biedt, maar ook specifieke risico's introduceert als EAB verkeerd wordt toegepast. Bij DNS-validatie zijn er kwetsbaarheden, zoals het risico dat een aanvaller controle krijgt over DNS-records. De grote certificaatpartijen zoals Let's Encrypt en Google PKI domineren de markt met meer dan 75% van alle uitgifte van TLS-certificaten. Een zorgpunt is dat Let's Encrypt alle TLS-certificaten kan intrekken, zelf gecompromitteerd kan raken of door andere problemen, zoals financieringstekorten, kan ophouden te bestaan. Tot slot is het cruciaal om geen enkele EAB te gebruiken over meerdere platformen om het risico van grootschalig compromitteren te minimaliseren.

Uit de openbare consultatie komen de volgende aandachtspunten naar voren met betrekking tot de toegevoegde waarde.

Volgens een anonieme reageerder kan het gebruik van officiële .gov.nl domeinnamen bijdragen aan phishing, omdat mensen het niet begrijpen of er niet op letten. Daarnaast wordt gewaarschuwd dat de invoering van de European Digital Identity Wallet (EDIW/EUDIW) kan leiden tot een toename van identiteitsfraude. Rijkswaterstaat stelt dat het een goed is om extra te toetsen of het gebruik van het ACME-protocol in combinatie met External Account Binding (EAB) geen risico's oplevert voor phishing en identiteitsfraude. De aanvraag richt zich op het beheer van certificaten, niet op de keuze voor een betrouwbare Certificate Authority. Het aangehaalde bericht op security.nl gaat over het gebruik van certificaten, terwijl deze aanvraag specifiek het beheer betreft. In combinatie met de opmaat BIO 2.0 norm 5.14.3, waarin het gebruik van OV-certificaten is voorgeschreven, biedt ACME met EAB een open standaard voor geautomatiseerd handmatig beheer. Zodra een betere open standaard beschikbaar komt, kunnen organisaties die zelf aanmelden.

Door een andere anonieme reageerder wordt over de kosten van implementatie opgemerkt dat organisaties met veel teams die slechts een of een klein aantal websites beheren centrale voorzieningen voor ACME centraal binnen de organisatie moeten worden opgezet of ondersteund. Hierdoor wordt voorkomen dat elk team zelf verantwoordelijk is voor de implementatie. Als organisaties dit niet centraal regelen of ondersteunen, is het de vraag of de kosten van implementatie acceptabel zijn. Rijkswaterstaat erkent dit en stelt dat het een goede overweging is om op te nemen in een implementatiehandreiking, zodat elke organisatie een goede basis heeft om een gedegen besluit te nemen.

Volgens Luc Nieland van Solstice is het een goed advies van de experts om ACME verplicht te stellen aan de overheid. Hij ziet de werkwijze als efficiënt, goed reproduceerbaar en kwaliteitsverhogend. Bovendien zou dit ook leiden tot kostenverlaging. Behalve de invoering van deze nieuwe werkwijze ziet de reageerder geen nadelen.

4.2 Open standaardisatieproces

De toetsingsprocedure wijst uit dat ACME voldoet aan het criterium 'Open standaardisatieproces'.

De ontwikkeling en het beheer van ACME is belegd bij IETF, een onafhankelijke non-profit organisatie die algemeen beleid heeft met betrekking tot versiebeheer. De beheerdocumentatie is voor iedereen direct en vrij toegankelijk.

IETF kent een open besluitvormingsproces. Deze wordt beschreven in hun Internet Standards Process en op hun website. IETF organiseert verschillende bijeenkomsten met belanghebbenden in diverse werkgroepen. Hoewel het meeste werk van de IETF-werkgroepen online plaatsvindt, worden er ook diverse bijeenkomsten en andere evenementen georganiseerd. Ook organiseren zij een openbare consultatie voordat een nieuwe versie van ACME wordt vastgesteld.

De financiering van het beheer van ACME is niet gegarandeerd voor ten minste drie jaar, maar wordt wel actief ondersteund door een groot aantal organisaties, waaronder diverse multinationals.

Het standaardisatieproces van IETF is open en goed gedocumenteerd. Iedereen kan deelnemen door zich aan te melden voor een werkgroep-mailinglijst of door een IETF bijeenkomst bij te wonen. De Nederlandse overheid is op dit moment niet betrokken bij de ontwikkeling en het beheer van de standaard. Er wordt op dit moment verkend welke organisatie de regierol in Nederland op zich kan en wil nemen ter bevordering van de adoptie in Nederland en de vertegenwoordiging van de Nederlandse belangen bij de doorontwikkeling van ACME kan borgen door deel te nemen aan de IETF-werkgroep.

Uit de openbare consultatie zijn geen aandachtspunten naar voren gekomen met betrekking tot het open standaardisatieproces.

4.3 Draagvlak

De toetsingsprocedure wijst uit dat ACME deels voldoet aan het criterium 'Draagvlak'.

Meerdere leveranciers ondersteunen ACME en dit aantal groeit voortdurend. Dankzij het open karakter van ACME kunnen diverse CA's en leveranciers het protocol makkelijker implementeren, wat gebruikers meer keuze en flexibiliteit biedt. Ondersteuning van ACME wordt onder andere aangeboden door: DigiCert, Sectigo, GoDaddy, GlobalSign, Let's Encrypt, ZeroSSL, Buypass. Via de support procedures van de gekozen CA kan assistentie worden gevraagd met betrekking tot de implementatie. Testen van een implementatie kan ook gratis via Let's Encrypt. ACME draagt onvoldoende bij aan interoperabiliteit zonder aanvullende

standaardisatieafspraken, zoals lokale profielen. Het blijkt moeilijk om te valideren of een complex verzoek van een client voldoet aan welke eisen een CA zich moet houden. Over het aanpakken hiervan is een actieve en online inzichtelijke discussie gaande.

Er zijn diverse implementaties van ACME beschikbaar, waaronder Certbot, acme.sh, lego, Caddy en Dehydrated. Deze implementaties zijn open source of vrij te gebruiken. Dit betekent dat organisaties deze kunnen downloaden, aanpassen en implementeren in hun eigen omgeving. Op de website van Let's Encrypt wordt een overzicht gegeven van ACME client implementaties.

Het is vooralsnog onbekend in hoeverre de belangrijkste stakeholders vanuit de overheid achter de adoptie van ACME staan. De kans lijkt hierop groot vanwege de voordelen die de standaard biedt en adoptie door de grootste CA's. Binnen het organisatorische werkgingsgebied maken meerdere Nederlandse overheidsorganisaties gebruik van de standaard, waaronder Rijkswaterstaat. Het Nationaal Cyber Security Centrum (NCSC) adviseert het gebruik van ACME.

Onbekend is of Nederlandse overheidsorganisaties ACME v1 nog gebruiken. Dat is lastig te achterhalen aangezien ACME v1 ook intern kan worden gebruikt. Het CA/Browser Forum heeft geen specifieke vereisten met betrekking tot de versie van ACME die moet worden gebruikt. Echter, Let's Encrypt, lid van het CA/Browser Forum, heeft het gebruik van ACME v1 uitgefaseerd. Doordat leveranciers deze versie niet meer ondersteunen is de waarschijnlijkheid dat deze verouderde versie nog breed wordt gebruikt laag. Adoptie in bedrijfsleven is groot en ondersteunde clientimplementaties zijn aanwezig voor gangbare talen en platforms. Onder andere Sectigo, Globalsign, SecureW2, Venafi en Digicert verzorgen dit.

Uit de openbare consultatie komen de volgende aandachtspunten naar voren met betrekking tot het draagvlak.

Sig-I/O Automatisering geeft aan dat er, wat betreft de verplichting van de standaard voor overheidsorganisaties, bij een ministerie (redactie: niet gemeld welke) een verplichting geldt om PKI-O certificaten af te nemen voor productieomgevingen. Deze PKI-O certificaten kunnen nog niet met behulp van ACME worden aangevraagd. De procedure hiervoor en de bijbehorende kosten zijn significant. Tot slot geeft de reageerder aan dat ACME al binnen het Ministerie van Volksgezondheid, Welzijn en Sport uitgebreid wordt gebruikt. Rijkswaterstaat benadrukt dat de aanvraag niet gaat over het kiezen van een betrouwbare Certificate Authority. In de opmaat BIO 2.0 norm 5.14.3 staat het volgende: *Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.* ACME met External Account Binding (EAB) maakt dit op een geautomatiseerde manier mogelijk.

4.4 Opname op de lijst bevordert adoptie

De toetsingsprocedure wijst uit dat ACME voldoet aan het criterium ‘Opname op de lijst bevordert adoptie’.

De opname op de ‘Pas toe of leg uit’-lijst bevordert de adoptie van de standaard. Door het verplichten van ACME kan een algehele kwaliteitsslag gemaakt worden met betrekking tot automatisering van een kritisch proces voor beveiliging van webapplicaties, namelijk verkrijgen, vernieuwen en intrekken van webPKI-certificaten.

Uit de openbare consultatie zijn er geen aandachtspunten naar voren gekomen met betrekking tot dit criterium.

5 Adviezen bij opname van de standaard

Het Forum Standaardisatie geeft de volgende adviezen bij plaatsing van ACME op de ‘Pas toe of leg uit’-lijst:

- Aan Logius om niet-publiek vertrouwde TLS-certificaten aan te bevelen en op termijn te verkennen om ook ACME hiervoor te verplichten. Daarnaast ook om duidelijk te maken dat het gaat om de certificaattransacties, niet over de (domein)validatie.
- Aan indiener om te verkennen wie de regierol voor ACME in Nederland kan oppakken, bijvoorbeeld CIO Rijk of NCSC.
- Aan NCSC om de Factsheet Veilig beheer van digitale certificaten van het NCSC te herzien en de impact van implementatie van ACME en de volgende punten hierin mee te nemen:
    - Een handreiking met geleerde lessen over het implementeren van ACME, tooling, prehooks en het delen van ervaringen.
    - Een handreiking voor het toepassingsgebied van het type certificaten voor Extended Validation (EV) en Organisation Validation (OV).
    - Een handreiking voor hoe ACME in combinatie met STARTTLS & DANE toe te passen.
    - Inzet op het vergroten van bewustwording over geautomatiseerd certificaatbeheer, de verschillen tussen certificaatautoriteiten (CA's) en de nuances tussen ACME en Let's Encrypt, door middel van gerichte lobbyactiviteiten en informatieve publicaties.