Expertadvies ACME

Aan:	Forum Standaardisatie
Van:	InnoValor Advies
Datum:	woensdag 19 februari 2025
Versie:	1.1
Bijlagen:	geen

1 Advies

De experts die betrokken waren bij het expertonderzoek adviseren om de standaard Automatic Certificate Management Environment (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. Er zijn echter 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 ACME in Nederland. Ook is er geen vertegenwoordiging van de Nederlandse belangen bij de doorontwikkeling van ACME. Dit zijn aandachtspunten.

Het voorgestelde functioneel toepassingsgebied voor ACME is:

> *Het ACME-protocol moet worden toegepast voor het automatiseren van de interactie tussen certificaatautoriteiten en certificaatgebruikers, waardoor het proces van het verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten wendbaarder en betrouwbaarder wordt.*

Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies is extra aandacht besteed aan de volgende punten:

- aandacht of ACME geschikt is om te verplichten of aan te bevelen aan de overheid;
- aandacht voor draagvlak en adoptie voor de standaard door overheidspartijen;
- aandacht voor 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.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het nut en de werking van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 geeft de samenstelling van de expertgroep weer. Hoofdstuk 5 documenteert hoe de experts de standaard beoordelen tegen de criteria voor opname op de lijst.

Tot slot geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) 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) betreft een protocol voor het geautomatiseerd verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten die onder andere kan 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 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 gebonden is. Het protocol wordt inmiddels breed ondersteund door alle grote Certificate Authorities (CA’s) (zie paragraaf 5.3.2.1).

Uitgangspunt voor de beoogde toetsingsprocedure is om ACME te verplichten voor het automatiseren van het verkrijgen, vernieuwen en intrekken, oftewel het certificaatbeheer mogelijk te maken. Domeinvalidatie voor web zoals websites, webapplicaties, intranetsites en zogenaamde machine-to-machine koppelingen van systemen, mag plaatsvinden buiten het ACME protocol. Hoewel domeinvalidatie wel mogelijk is met ACME, zijn er alternatieven en goedwerkende andere methoden voor domeinvalidatie beschikbaar.

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 TLS-certificaten verlopen omdat deze niet tijdig of niet goed worden vernieuwd, zijn websites of systemen die op basis van deze TLS-certificaten worden beveiligd niet goed meer beschikbaar. Burgers en bedrijven hebben hierdoor geen toegang meer tot informatie en/of organisaties kunnen geen gegevens meer uitwisselen. Daarom is het van belang om het levenscyclusbeheer van TLS-certificaten op orde te hebben.

Daarnaast vermindert het gebruik van ACME de beheerlast voor het beheer van TLS-certificaten. Met de toename van het aantal websites en de ontwikkeling naar een kortere geldigheidsduur van TLS-certificaten – zoals de huidige negentig dagen voorgesteld door Chrome en de verwachte verdere reductie naar 47-48 dagen in 2028 volgens de ballot in het CA/Browser Forum – wordt het steeds minder haalbaar om TLS-certificaten handmatig tijdig te vernieuwen. Het gebruik van ACME maakt het mogelijk om dit proces te automatiseren, waardoor de schaalbaarheid en betrouwbaarheid van certificaatbeheer aanzienlijk worden verbeterd.

Ook helpt ACME 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 het eenvoudiger om interoperabiliteit te behouden tussen verschillende systemen en providers. Dit biedt gebruikers flexibiliteit en voorkomt *vendor lock-in*.

Tot slot is ACME ook cruciaal voor crypto-agility. Door het automatiseren van certificaatbeheer kunnen organisaties snel 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 snelle reactie op beveiligingsincidenten en een toekomstbestendig cryptografisch beleid.

3 Betrokkenen en proces

Op 23 oktober 2023 heeft Rijkswaterstaat ACME v2 aangemeld om te toetsen of de standaard geschikt is aan te bevelen aan de overheid via plaatsing op de lijst aanbevolen standaarden.

Op 26 februari 2024 heeft een intakegesprek plaatsgevonden met de indieners, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. Bij het online intakegesprek waren de volgende personen aanwezig:

- John van Agthoven (Rijkswaterstaat, indiener)
- Vleer Doing (Rijkswaterstaat)
- Dennis Hoogervorst (Rijkswaterstaat)
- Gaston Lamaitre (Rijkswaterstaat)
- Hans Laagland (Bureau Forum Standaardisatie, als toehoorder)
- Benjamin Broersma (Bureau Forum Standaardisatie, als toehoorder)
- Ruud Kosman (InnoValor Advies)

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 aanmelding in procedure te nemen.

Hierop volgend heeft de procedurebegeleider in overleg met de indiener en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld.

De leden van de expertgroep hebben een concept expertadvies gekregen dat is samengesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit concept expertadvies doorgenomen en aandachtspunten geïdentificeerd.

De expertgroep is op 17 november 2024 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld. Dit expertadvies geeft de uitkomst van de expertgroep weer.

Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie op internetconsultatie.nl. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep. Indien nodig kan dit aanleiding geven tot een aanvullend expertonderzoek.

Het Forum Standaardisatie formuleert op basis van het expertadvies, reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Het OBDO besluit om het advies wel of niet over te nemen.

4 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)

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.

5 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst nodig om de adoptie te bevorderen?

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.

5.1 Toegevoegde waarde

Met dit criterium wordt bepaald of het toepassingsgebied van de standaard duidelijk is, of deze zich goed verhoudt tot andere standaarden die al dan niet op de lijst staan, of de standaard een duidelijke meerwaarde heeft en of deze opweegt tegen eventuele risico’s en nadelen.

5.1.1 Waardering van het criterium criteria 'Toegevoegde waarde'

De experts komen tot de conclusie dat ACME voldoet aan het criterium 'toegevoegde waarde'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.1.2 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.2.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Het voorgestelde functioneel toepassingsgebied voor ACME op de 'Pas toe of leg uit'-lijst is:

> *ACME moet worden toegepast voor het automatiseren van de interactie tussen certificaatautoriteiten en certificaatgebruikers, waardoor het proces van het verkrijgen, vernieuwen en intrekken van publiek vertrouwde TLS-certificaten wendbaarder en betrouwbaarder wordt.*

De experts oordelen dat dit functioneel toepassingsgebied voldoende duidelijk is en het verplichte gebruik van de standaard of lijst aanbevolen standaarden, eenduidig beschrijft.

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het voorgestelde organisatorisch werkingsgebied voor ACME op de 'Pas toe of leg uit'-lijst, is:

> *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.*

Dit is het gangbare organisatorisch werkingsgebied voor standaarden op de 'Pas toe of leg uit'-lijst of lijst aanbevolen standaarden van het Forum Standaardisatie.

5.1.2.3 Is de standaard generiek toepasbaar?

Ja, ACME kan over de grenzen van organisaties en sectoren gebruikt worden en is niet alleen bedoeld voor gegevensuitwisseling binnen één organisatie of sector.

5.1.3 Verhoudt de standaard zich goed tot andere standaarden?

5.1.3.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast?

Ja, ACME sluit goed aan op TLS. Ook werkt ACME in combinatie met de standard Certification Authority Authorization (CAA). Voorwaarde is dat de Certificate Authority 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. Experts geven aan dat een handleiding en toelichting hierbij gewenst is voor gebruikers om de configuratie op de juiste manier in te richten.

ACME kan in standalone mode worden gebruikt waarbij het systeem onafhankelijk van externe systemen of integraties functioneert. Dit biedt voordelen zoals eenvoud in beheer en minder risico op storingen door externe factoren. 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, zien experts dit als een gewenste aanvulling om de wendbaarheid van het systeem te vergroten.

5.1.3.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?

Ja. ACME automatiseert het verkrijgen, vernieuwen en intrekken van TLS-certificaten en ondersteunt daarbij het totstandbrengen van een beveiligde verbinding op basis van TLS.

5.1.3.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

Ja, RFC 8894 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.

5.1.3.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

Ja, ACME is een internationale standaard in beheer bij Internet Engineering Task Force (IETF) en wordt beschreven in RFC 8555.

5.1.4 Wegen de voordelen van de standaard op tegen de nadelen?

5.1.4.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja, het proces van certificaatbeheer wordt versimpeld en geautomatiseerd, waar eerder handmatige stappen nodig waren. ACME zorgt niet voor een besparing op de kosten van TLS-certificaten, maar bespaart op kosten van beheer en capaciteit. Daarnaast vermindert het risico op verstoringen, die vaak financiële gevolgen hebben en extra inzet van medewerkers vergen, bijvoorbeeld bij onderzoek waarom een bepaalde dienst niet functioneert.

5.1.4.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

Ja, de implementatie van ACME kan een initiële investering met zich meebrengen. De kosten hiervoor kunnen onder andere de aanschaf van de software, training van medewerkers en eventuele aanpassingen aan bestaande systemen omvatten.

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. Dit resulteert in een efficiënter en nauwkeuriger certificaatbeheerproces, wat op zijn beurt kostenbesparingen met zich meebrengt.

Daarnaast biedt ACME ook voordelen op het gebied van leveranciersonafhankelijkheid. Door gebruik te maken van ACME kunnen organisaties gemakkelijker switchen tussen certificaatautoriteiten, zonder dat dit hoge kosten met zich meebrengt. Dit vermindert de afhankelijkheid van specifieke leveranciers en geeft organisaties meer flexibiliteit en controle over hun certificaatbeheer.

5.1.4.3 Is de meerwaarde van de standaard goed inzichtelijk te maken?

Ja, omdat bij uitgifte van TLS-certificaten en identiteitsverificatie zonder gebruik te maken van ACME bij bestaande Web PKI CA's doorgaans handmatige stappen betrokken zijn. ACME versimpelt de automatisering op het gebied van certificaatuitgifte en -vernieuwing en het intrekken van TLS-certificaten.

5.1.4.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, omdat handmatige stappen en eventueel versturen van gevoelige data via e-mail of andere onveilige methodes voor het certificatenbeheer dankzij de automatisering middels ACME worden vermeden.

Tijdens de expertsessie werden verschillende beveiligingsrisico's voor ACME geïdentificeerd. 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. Dit creëert een grote afhankelijkheid van organisaties zoals Let's Encrypt. Een zorgpunt is dat wanneer Let's Encrypt alle TLS-certificaten intrekt, gecompromitteerd raakt of door andere problemen, zoals financieringstekorten, ophoudt te bestaan, dit grote gevolgen kan hebben voor de beschikbaarheid van diensten. Tot slot is het cruciaal om geen enkele EAB te gebruiken over meerdere platformen, om het risico van grootschalig compromitteren te minimaliseren.

5.1.4.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, omdat door gebruik van deze standaard sprake is van machine-machine communicatie, in plaats van mens-mens of mens-machine, waardoor alleen informatie die nodig is voor het vernieuwen van de TLS-certificaten gecommuniceerd hoeft te worden. Daardoor is geen uitwisseling van extra communicatiegegevens nodig, wat in het geval van handmatige uitgifte wel potentieel noodzakelijk is.

5.2 Open standaardisatieproces

Met dit criterium wordt bepaald of het beheer en de (door)ontwikkeling van de standaard op een open, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

5.2.1 Waardering van het criterium criteria 'open standaardisatieproces'

De experts komen tot de conclusie dat ACME voldoet aan het criterium 'open standaardisatieproces. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.2.2 Is de documentatie voor een ieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, de specificatie van de standaard en algemene documentatie is voor iedereen direct en vrij toegankelijk.

5.2.2.2 Is de documentatie over het ontwikkel- en beheerproces beschikbaar zonder dat er sprake is van belemmeringen?

Ja, de standaard wordt door IETF beheerd en de specificaties van de standaarden en algemene documentatie over het ontwikkel- en beheerproces is voor iedereen direct en vrij toegankelijk.

5.2.3 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.3.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, IETF stelt de standaard onherroepelijk royalty-free voor eenieder beschikbaar.

5.2.3.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja, IETF garandeert dat bijdragen van partijen aan de ontwikkeling van de standaard royalty-free beschikbaar worden gesteld.

5.2.4 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.4.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?

Ja, IETF kent een open besluitvormingsproces.

5.2.4.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Ja, IETF kent een open besluitvormingsproces. Deze wordt beschreven in hun *Internet standards process*. Op hun website beschrijft IETF: Ruwe consensus en draaiende code - We maken standaarden op basis van het gecombineerde technische oordeel van onze deelnemers en onze praktijkervaring bij het implementeren en inzetten van onze specificaties.

5.2.4.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, bijvoorbeeld via de 'Report errata' knop op de webpagina van ACME. Algemene informatie over formeel bezwaar is daarnaast te vinden via de *policies and procedures* en via de *process* pagina.

5.2.4.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja, 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.

5.2.4.5 Organiseert de standaardisatieorganisatie een openbare consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Ja, IETF organiseert een openbare consultatie voordat een nieuwe versie van ACME wordt vastgesteld.

5.2.5 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.5.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, IETF is een onafhankelijke non-profit organisatie.

5.2.5.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Nee, 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, waarvan diverse multinationals.

5.2.6 Is het (versie) beheer van de standaard goed geregeld?

5.2.6.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard?

Ja, IETF heeft algemeen beleid met betrekking tot versiebeheer.

5.2.6.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, een beheerdocumentatie is beschikbaar via IETF Datatracker.

5.2.6.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

Nee, 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.

5.2.6.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

De IETF hanteert een open participatiemodel zonder formeel lidmaatschap, waarbij iedereen kan bijdragen door deel te nemen aan werkgroep-mailinglijsten of door IETF-bijeenkomsten bij te wonen. Deelnemers komen uit verschillende delen van de internetindustrie en uit de hele wereld. Dit open karakter bevordert een brede vertegenwoordiging van belanghebbenden in het beheer van standaarden zoals ACME, ook voor Nederlandse overheden en instellingen uit de (semi-)publieke sector.

5.2.6.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

Het standaardisatieproces van de 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. Het standaardisatieproces van de IETF begint met een Internet-Draft, die wordt besproken en herzien binnen werkgroepen om consensus te bereiken. Na goedkeuring wordt het document als een *Request for Comments* (RFC) gepubliceerd. Vervolgens wordt de standaard geïmplementeerd en getest door verschillende partijen. Bij succesvolle toepassing en evaluatie kan de standaard officieel als Internetstandaard worden vastgesteld. Dit proces zorgt voor technische betrouwbaarheid, brede acceptatie en interoperabiliteit.

IETF is echter geen Nederlandse beheerorganisatie. Daarmee kan het Forum Standaardisatie niet aan IETF het predicaat ‘Uitstekend beheer’ toekennen voor ACME. Wel kan het Forum

Standaardisatie aan een Nederlandse intermediaire organisatie het predicaat 'Erkende Nederlandse Intermediair' voor een standaard met een internationale beheerorganisatie toekennen (dit is mogelijk sinds het akkoord van het Forum Standaardisatie op 12 februari 2025 hierop). Op dit moment kent ACME geen Nederlandse intermediaire organisatie.

5.2.7 Is er adoptieondersteuning voor de standaard?

5.2.7.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?

Ja, zowel de auteurs van de standaard als de beheerorganisatie IETF zijn direct te benaderen.

5.2.7.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, meerdere Certificate Authorities (CA's) ondersteunen ACME. Afhankelijk van de gekozen CA kunnen verschillende niveaus van ondersteuning bij de desbetreffende CA voor hun implementatie van de standaard worden geleverd.

5.3 Draagvlak

Met dit criterium wordt bepaald of de opname van de standaard op de 'Pas toe of leg uit'-lijst op voldoende draagvlak kan rekenen over de breedte van de overheid. Een voorwaarde hiervoor is ook dat er voldoende marktondersteuning voor de standaard bestaat, en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

5.3.1 Waardering van het criterium criteria 'draagvlak'

De experts komen tot de conclusie dat het onbekend is of ACME voldoet aan het criterium 'draagvlak'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.3.2 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.2.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja, meerdere leveranciers ondersteunen ACME en dit aantal groeit voortdurend. Dankzij de open standaard van ACME kunnen diverse Certificate Authorities (CA's) en leveranciers het protocol 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.

5.3.2.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Ja, via de support procedures van de gekozen Certificate Authority kan assistentie gevraagd worden met betrekking tot de implementatie. Testen van een implementatie kan ook gratis via Let's Encrypt.

5.3.2.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Nee, omdat het moeilijk blijkt om te valideren of een complex verzoek van een client voldoet aan welke eisen een Certificate Authority zich moet houden. Over het aanpakken hiervan is een actieve en online inzichtelijke discussie gaande.

5.3.2.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja, 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.

5.3.3 Kan de standaard rekenen op voldoende draagvlak?

5.3.3.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

Vooralsnog onbekend. De kans is groot dat de standaard al breder wordt ingezet vanwege de voordelen die de standaard biedt en adoptie door de grootste Certificate Authorities.

5.3.3.2 Staan de overheidsorganisaties die worden geraakt door een verplichting van de standaard achter het verplichte gebruik van de standaard?

Zie 5.3.3.1

5.3.3.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, onder andere door Rijkswaterstaat. Verder is dit vooralsnog onbekend.

NCSC adviseert het gebruik van ACME.

5.3.3.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Onbekend, experts hebben geen zicht op 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 het ACME-protocol 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 echter niet meer ondersteunen is de waarschijnlijkheid dat deze verouderde versie nog wordt gebruikt laag.

5.3.3.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Nee, ACME v1 wordt niet meer ondersteund.

5.3.3.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Vooralsnog onbekend, experts staan positief tegenover het gebruik van ACME, maar hebben geen zicht op signalen van andere (semi-)overheidsorganisaties.

Adoptie in bedrijfsleven is groot en ondersteunde client implementaties zijn aanwezig voor gangbare talen en platforms. Onder andere door Sectigo, Globalsign, SecureW2, Venafi en Digicert.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie 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 wordt met betrekking tot automatisering van een kritisch proces voor beveiliging van webapplicaties, namelijk verkrijgen, vernieuwen en intrekken van webPKI-certificaten.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie en OBDO de volgende adviezen bij van ACME op de 'Pas toe of leg uit'-lijst/lijst aanbevolen standaarden:

- 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 ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) te herzien en de impact van ACME hierin mee te nemen. Hierin onder andere de volgende punten in mee te nemen:
    - Een handreiking met geleerde lessen voor het implementeren van ACME, met 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 ACME te ontwikkelen hoe ACME in combinatie met STARTTLS & DANE kan worden toegepast.
    - In te zetten 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.