Intakeadvies ACME

Vergadering:	Forum Standaardisatie 19 juni 2024
Agendapunt:	3D
Documentnummer:	FS-20240619.3D-intakeadvies-acme
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	19 juni 2024
Versie:	1.0
Bijlagen:	geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om Automatic Certificate Management Environment (ACME) (automatiseren van uitgifte van certificaten) in procedure te nemen. Een uitgebreid expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst open standaarden. Onderdeel van dit expertonderzoek is om te onderzoeken om de standaard te verplichten aan de overheid (via 'Pas toe of leg uit'-verplichting) of aan te bevelen aan de overheid.

ACME bevat een protocol voor het geautomatiseerd uitgeven en vernieuwen van beveiligingscertificaten. Deze beveiligingscertificaten (Public Key Infrastructure (PKI) certificaten) zijn unieke sleutels waarmee digitale systemen zich identificeren bij het online verbinden met een ander systeem. Gebruik van het ACMEprotocol zorgt ervoor dat tijdrovende en foutgevoelige, handmatige stappen met betrekking tot de *lifecycle* van PKI certificaten kunnen worden geautomatiseerd. Uitgangspunt voor de beoogde toetsingsprocedure is het verplichten of aanbevelen van ACME voor domeinvalidatie voor web.

Tijdens het intakegesprek zijn de diverse criteria besproken. De standaard lijkt kansrijk om in aanmerking te komen voor plaatsing op de lijst open standaarden. Tijdens de

expertbijeenkomst en het tot stand komen van het expertadvies zal extra aandacht zijn voor de volgende punten:

- aandacht of ACMEprotocol 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 het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de standaard voldoet aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan.

Tenslotte wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke waarde van de standaard te communiceren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

Het Automatic Certificate Management Environment (ACME) betreft een protocol voor het geautomatiseerd uitgeven en vernieuwen van beveiligingscertificaten. Deze beveiligingscertificaten (*Public Key Infrastructure* (PKI) certificaten) zijn unieke sleutels waarmee digitale systemen zich identificeren bij het online verbinden met een ander systeem. Deze certificaten hebben een afgebakende geldigheidsduur. 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 het ACMEprotocol maakt het beheer van deze certificaten efficiënter en beduidend minder foutgevoelig. Ook maakt gebruik van ACME het overstappen naar een andere certificaatleverancier eenvoudiger.

Er zijn verschillende soorten certificaat validaties: *extended validation*, *organisation validation* en *domain validation*. Uitgangspunt voor de beoogde toetsingsprocedure is het verplichten of aanbevelen van ACME voor domeinvalidatie voor web zoals websites, webapplicaties, intranetsites en zogenaamde *machine-to-machine* koppelingen van systemen.

2.2 Waarom is deze standaard belangrijk?

Het gebruik van ACME draagt bij aan 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. Daarnaast zorgt het gebruik van ACME

voor minder beheerlast voor het gebruik van beveiligingscertificaten. Dit bevordert een veilige en betrouwbare informatieverstrekking en gegevensuitwisseling.

Als certificaten verlopen en niet tijdig of niet goed vernieuwd worden, zijn websites of systemen niet meer beschikbaar waardoor burgers en bedrijven geen toegang meer hebben tot informatie of organisaties geen gegevens meer kunnen uitwisselen. Zo leidt het niet tijdig vervangen van certificaten tot grote storingen in belangrijke digitale systemen. Daarom is het van belang om certificaten op orde te hebben.

Met de toename van het aantal websites en een ontwikkeling van kortere geldigheidsduur van certificaten, schaalt het slecht om de tijdige vernieuwing van certificaten handmatig te blijven doen. Het gebruik van ACMEprotocol zorgt ervoor dat het bovenstaande proces kan worden geautomatiseerd. Geautomatiseerde validatie zorgt voor betrouwbaardere validatie en daarmee voor een betrouwbare digitale overheid.

3 Betrokkenen en proces

Op 23 oktober 2023 heeft Rijkswaterstaat het Automatic Certificate Management Environment (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 intake gesprek 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. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van de informatie in het aanmeldformulier, deskresearch, en de aanvullende informatie uit het intakegesprek.

4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

ACME voldoet aan alle vier criteria om in behandeling genomen te worden voor plaatsing op de lijst aanbevolen standaarden of 'Pas toe of leg uit’-lijst. Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1 Valt de standaard binnen de scope van Forum Standaardisatie?

De standaard is toepasbaar voor elektronische gegevensuitwisseling tussen (semi-) overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling.

De standaard omvat een uitbreidbaar framework voor het automatiseren van de uitgifte en domeinvalidatieprocedure van certificaten (PKI). Met de toename van het aantal (overheids)websites en een kortere *lifecycle* van certificaten, wordt deze standaard belangrijk voor de overheid. Daarnaast ligt het in de lijn van de verwachting dat het aantal koppelingen tussen overheidssystemen alleen maar zal toenemen, en daarmee ook het aantal gebruikte certificaten. De toepassing van het ACME-protocol zorgt ervoor dat de toename niet leidt tot een verzwaring van de beheerlast.

4.2 Heeft de standaard een toepassing die een enkele organisatie of sector overstijgt?

Het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied overstijgen een enkele organisatie of sector omdat de overheid breed gebruik maakt van PKI-certificaten (RFC 5280). Het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard is daarom voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid.

ACMEprotocol borgt een doorlopende gegevensuitwisseling en informatievoorziening binnen en tussen organisaties doordat dankzij het gebruik van het ACMEprotocol certificaten via een geautomatiseerd proces worden vernieuwd.

4.3 Is de standaard al wettelijk verplicht?

Het is zinvol ACME op te nemen. ACME is niet wettelijk verplicht voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied en draagt bij aan de beschikbaarheid van (semi-)overheidswebsites en -systemen. De standaard draagt bij aan hogere bereikbaarheid en betrouwbaarheid van informatieverstrekking en gegevensuitwisseling en aan lagere beheerlast. De verwachting is dat het opnemen van de standaard op de lijst open standaarden de adoptie van deze standaard zal versnellen.

4.4 Draagt de standaard bij tot de oplossing van een bestaand probleem?

Het ligt in de lijn van de verwachting dat het aantal koppelingen tussen overheidssystemen alleen maar zal toenemen (denk aan ontwikkelingen rond Federatief Datastelsel), en daarmee ook het aantal gebruikte certificaten. De toepassing van het ACMEprotocol zorgt ervoor dat de toename niet leidt tot een verzwaring van de beheerlast. Het gebruik van ACMEprotocol is

één van de projecten in Digilab. Digilab is Innovatiewerkplaats voor het Federatief Datastelsel en onderdeel van het programma 'Data bij de bron'.

Het gebruik van ACME betreft het standaardiseren van het proces voor beheren van certificaten, en maakt het hierdoor ook 'gemakkelijker' om over te stappen naar andere leveranciers. ACME wordt ondersteund door meerdere certificaatautoriteiten (CA's) waaronder ook Europese. Doordat meerdere CA's gebruik maken van ACME wordt overstappen tussen leveranciers eenvoudiger. Leveranciersafhankelijkheid wordt daarmee voorkomen.

Gebruik van dit protocol zorgt ervoor dat tijdrovende en foutgevoelige, handmatige stappen met betrekking tot de *lifecycle* van PKI-certificaten kunnen worden geautomatiseerd. Dit biedt een aantal voordelen ten opzichte van het huidige (handmatige) proces: beheerlast wordt verkleind, kans op fouten wordt verlaagd, kosten kunnen beperkt worden gehouden door minder menselijke tussenkomst, beschikbaarheid van websites wordt vergroot.

5 Is er zicht op een positief expertadvies?

Als het Forum Standaardisatie de standaard in procedure neemt, gaat een groep experts de standaard toetsen op de vier inhoudelijke criteria voor opname op de lijst open standaarden. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief expertadvies kan rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria.

Het intakeonderzoek heeft geen inhoudelijke criteria gevonden die een positief expertadvies voor plaatsing van ACME op de lijst aanbevolen standaarden of op de 'Pas toe of leg uit'-lijst in de weg zou kunnen staan. Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

De ACME standaard heeft meerwaarde ten opzichte van andere standaarden met een (deels) overlappend functioneel toepassingsgebied.

Een voorstel voor het functioneel toepassingsgebied is als volgt gedefinieerd (afhankelijk van respectievelijk aanbevelen of verplichten van de standaard aan de overheid):

> *Het ACME-protocol kan worden toegepast/ moet worden toegepast voor het automatiseren van de interactie tussen certificaatautoriteiten en gebruikers voor web, waardoor het proces van het verkrijgen, vernieuwen en herroepen van SSL/TLS-certificaten efficiënter wordt.*

ACME automatiseert de handmatige stappen bij gebruik van PKIcertificaten voor, het wettelijk verplichte en onderliggende, HTTP over TLS. TLS (Transport Layer Security), is een standaard op de 'Pas toe of leg uit'-lijst die moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief *machine-to-machine* communicatie. ACME heeft bovendien een verbeterd protocol t.o.v. het Simple Certificate Enrolment Protocol (SCEP), een eerdere poging op een geautomatiseerd certificaatuitgifte protocol. Daarnaast is er raakvlak met CAA (standaard voor controle over uitgifte van digitale certificaten) van lijst aanbevolen

standaarden van Forum Standaardisatie. Om betrouwbaarheid van certificatenuitgifte te vergroten wordt met de standaard CAA aangegeven welke organisaties certificaten uit mogen geven voor een specifieke organisatie.

De baten van het adopteren van ACME wegen op tegen de kosten, risico's en nadelen. Bij Web PKI CA's die zonder ACME werken, zijn er doorgaans handmatige stappen nodig bij uitgifte van certificaten. ACME versimpelt de automatisering op het gebied van certificaatuitgifte en domeinvalidatieprocedure en neemt handmatige stappen weg. Daarnaast zorgt de standaard voor verbeterde beveiliging, doordat handmatige stappen en eventueel versturen van data via e-mail of andere onveilige methodes aan CA's bij het verlengen van de certificaten worden verminderd. Bij overheidsbrede adoptie worden ook privacy risico's verminderd, omdat door gebruik van deze standaard sprake is van *machine-to-machine* communicatie in plaats van mens-mens of mens-machine bij het beheren en verlengen van certificaten. Hierdoor wordt alleen informatie gecommuniceerd die nodig is voor het vernieuwen van de certificaten. Daardoor is geen uitwisseling van extra communicatiegegevens nodig, wat in het geval van handmatige uitgifte wel noodzakelijk is.

Door automatisering is andere expertise van mensen nodig. Potentieel risico hierbij is dat ook kennis en kunde verdwijnt over het handmatige proces, in geval dat er fouten in systemen optreden. Daarnaast vergroot automatisering de impact bij fouten, doordat fouten ongezien versneld en op grotere schaal doorgevoerd kunnen worden ten opzichte van handmatige handelingen. De toename van certificaten en de kortere levensduur van certificaten vraagt echter om automatisering. Het is van belang om nu al daarmee aan de slag te gaan.

5.2 Open standaardisatieproces

Internet Engineering Task Force (IETF) beheert ACMEprotocol. IETF is een internationale organisatie die vrijwillig te adopteren open internetstandaarden ontwikkelt.

Documentatie is vrij beschikbaar. Er is een uitgebreid document met de specificaties van de standaard, evenals informatie over het ontwikkel- en beheerproces, notulen en informatie over de besluitvormingsprocedure. IETF heeft als kernwaarden dat het tot stand komen van een standaard een open proces is. Het beheerproces is transparant en benaderbaar, iedere belanghebbende kan participeren in het ontwikkel en beheerproces als onderdeel van een van de werkgroepen. Er is een bezwaarprocedure, onder meer door gebruik van de *report errata*

Het besluitvormingsproces vindt plaats op basis van consensus waarin *engineering* overwegingen en ervaring van participanten een belangrijk onderdeel vormen van de afweging. Onduidelijk is of de belangen van de Nederlandse overheid worden meegenomen bij de ontwikkeling van ACME. Dit is een aandachtspunt voor het expertonderzoek. Wel is er dus altijd de mogelijkheid voor de Nederlandse overheid om in IETF te participeren.

IETF stelt het intellectueel eigendomsrecht op de standaard onherroepelijk *royalty-free* voor eenieder beschikbaar en garandeert beschikbaarheid van intellectueel eigendom van partijen die bijdragen aan de ontwikkeling van de standaard onder dezelfde condities.

De IETF bestaat sinds 1986. De IETF geeft inzicht in de eigen financiële situatie. Er is geen reden om aan te nemen dat IETF binnen drie jaar niet meer in staat is de standaard te beheren en door te ontwikkelen. Bovendien wordt de verdere ontwikkeling vormgegeven door een levendige community van vrijwilligers die zich inzetten de standaard verder te verbeteren.

Op de website van IETF kan alle informatie gevonden worden die nodig is om de standaard te gebruiken. Let's Encrypt (zeer grote CA) ondersteunt ACME en heeft documentatie gepubliceerd. Er zijn meerdere, andere CA's dan Let's Encrypt, die ACMEprotocol ondersteunen. Er zijn CA's die certificaten via ACME gratis beschikbaar aanbieden. CA's kunnen extra kosten rekenen voor het implementeren van het ACME protocol.

Er is op dit moment geen duidelijke nationale regie partij (of intermediair) die belangen van Nederlandse overheid behartigd bij IETF voor deze standaard. Het gaat hier om de vertegenwoordiging van de Nederlandse belangen bij de doorontwikkeling van ACME. In het expertonderzoek wordt verder verkend welke partij deze rol op zich kan en wil nemen.

5.3 Draagvlak

Gebruik van ACME wordt door verschillende partijen ondersteund, waaronder DigiCert, Sectigo, GoDaddy, GlobalSign Google Trust Services en Let's Encrypt. Bij Let's Encrypt en Google Trust Services kan énkel ACME worden gebruikt.

VNG heeft speciaal voor dit Intakeadvies een korte inventarisatie gemaakt nagezocht via Basisbeveiliging. Uit de inventarisatie kwam naar voren dat bij gemeenten meer dan 20% van alle certificaten op bekende domeinen van Let's Encrypt afkomstig zijn, met ondersteuning van ACME. Dit percentage ligt mogelijk hoger, aangezien ook andere certificaatleveranciers ACME ondersteunen. Uit diezelfde eerste inventarisatie van VNG komt naar voren dat provincies en waterschappen voor meer dan 10% van alle certificaten gebruik maken van Let's Encrypt met ondersteuning van ACMEprotocol. De aanname is dat de standaard al breder wordt ingezet vanwege de voordelen die deze biedt en door de brede adoptie onder CA's.

Ook het NCSC (het Nationaal Cyber Security Centrum), dat de opdracht heeft om in Nederland een open en stabiele informatiesamenleving te creëren, raadt het gebruik van ACME aan.

Daarnaast zijn er voldoende positieve signalen over toekomstig gebruik van de standaard. Zo is Let's Encrypt, waaruit de standaard is ontstaan, inmiddels een top vijf wereldwijde CA. De standaard wordt door steeds meer CA's ondersteund en de adoptie in het bedrijfsleven is groot. Daarnaast zijn ondersteunde client implementaties aanwezig in alle gangbare talen en voor alle gangbare platforms.

De bij het Forum Standaardisatie aangemelde versie van ACMEprotocol (ACME v.2) is niet *backward compatible* met eerdere versies van de standaard. Voor zover inzichtelijk is ACME v.2 breed in gebruik; versie 1 wordt ook niet langer ondersteund.

Er zijn geen aanvullende profielen nodig om de standaard te kunnen toepassen. Wel kan in het expertonderzoek worden verkend in hoeverre een handreiking bijdraagt aan het vereenvoudigen van het toepassen van de standaard. Deze kennis is nu niet formeel vastgelegd. Het ACMEprotocol kent vele client 'referentie implementaties'

5.4 Opname op de lijst bevordert adoptie

Het is de verwachting dat het verplichten of aanbevelen aan de overheid van ACMEprotocol ervoor gaat zorgen dat een algehele kwaliteitsslag gemaakt kan worden met de automatisering van uitgifte en beheer van certificaten.

Indiener Rijkswaterstaat wil een actieve rol spelen in het vinden van een geschikte regie partij voor deze internationale standaard en actief bijdragen aan de activiteiten rond adoptie die een regie partij initieert. Er zijn vanuit Rijkswaterstaat momenteel geen specifieke plannen om adoptie van de standaard overheidsbreed te bevorderen.

6 Praktijkvoorbeeld

Onderstaande *use cases* beschrijven de toepassing van ACME in de praktijk.

6.1 Use case: overstap van interne certificaten naar publieke certificaten

Rijkswaterstaat is overgestapt van interne PKI-certificaten naar publieke certificaten voor test en acceptatieomgevingen, zodat deze niet meer afwijken van productiesystemen, die publieke certificaten gebruiken. Dit bracht een hogere beheerlast met zich mee, vanwege de vele certificaatwisselingen voor de test en acceptatiesystemen.

DevOps werkwijze en Continuous Integration/Continuous Delivery CI/CD pipelines zorgen voor een versnelling in het ontwikkelproces, waardoor het aanvraagproces voor certificaten een bottleneck vormen en extra monitoring vergen. De inzet van ACME protocol lost dit probleem op.

6.2 Use case: inzet ACMEprotocol bij online samenwerkingsplatform

Het Infra Domein ”Cloud hosting” van Rijkswaterstaat ontsluit een online samenwerkingsplatform voor interne *public cloud* afnemers. Via een application gateway is het *domain* ontsloten en voorzien van een certificaat.

Wekelijks checkt een *automation pipeline* of het certificaat minimaal dertig dagen geldig is. Zo niet, dan wordt deze middels ACME ververst. De *automation pipeline* maakt gebruik van een Terraform ACME provider die geheel automatisch het certificaat aanmaakt en vernieuwt. De inzet van ACME zorgt ervoor dat certificaten altijd correct geïnstalleerd, geldig en vertrouwd zijn.