Expertadvies DNS Certification Authority Authorization Resource Record (CAA)

Datum:	15 februari 2019
Versienummer:	1.0
Opdrachtgever:	Forum Standaardisatie Postbus 96810 2509 JE Den Haag 070-8887776 info@forumstandaardisatie.nl
Procedurebegeleiding:	Lost Lemon
Voorzitter expertgroep:	Diana Koppenol
Auteurs:	Arjen Brienen, Remo van Rest

Inhoud

1 Samenvatting en advies

Op basis van het expertonderzoek wordt geadviseerd om de internet veiligheidstandaard RFC 6844: DNS Certification Authority Authorization Resource Record (kort: "CAA") op te nemen op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie.

Als functioneel toepassingsgebied wordt geadviseerd:

CAA moet worden toegepast ten behoeve van het aanvraagproces van server certificaten door overheden bij CA's (certificate authorities) ter autorisatie van één of meer CA's.

Als organisatorisch werkingsgebied wordt geadviseerd:

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

Paragraaf 5.5 van dit document beschrijft aanbevelingen van de expertgroep aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) ten aanzien van de stimulering van adoptie van de standaard.

2 Doelstelling expertadvies

2.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een pas-toe-of-leg-uit verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

2.2 Doelstelling expertadvies

Dit document is een expertadvies voor CAA gericht aan het OBDO en Forum Standaardisatie. CAA is aangemeld voor opname op de lijst met open standaarden door Jochem van den Berge van Logius.

Doel van dit document is om het OBDO te adviseren of CAA in aanmerking komt voor opname op de pas-toe-of-leg-uit lijst, al dan niet onder voorwaarden.

2.3 Doorlopen proces

Voor het opstellen van dit proces is de volgende procedure doorlopen:

1. De procesbegeleider heeft op 9 november 2018 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. Op basis van de intake heeft het Forum Standaardisatie op 9 november besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
4. De expertgroep is op 24 januari 2019 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. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde.

2.4 Vervolg

Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 25 februari 2019 tot 25 maart 2019. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het OBDO op. Het OBDO besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

2.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Diana Koppenol, Directeur bij Lost Lemon.

Arjen Brienen, adviseur bij Lost Lemon, heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:

- Maarten Aertsen (NCSC)
- Jochem van den Berge (Logius)
- Jan van Boheemen (Dienst Publiek en Communicatie (DPC))
- Marco Davids (SIDN)
- Theo van Diepen (Logius)
- Joost van Dijk (SURFnet)
- Berry van Halderen (NLnet Labs)
- Rene van de Hesseweg (KPN)
- John van Huijgevoort (VNG Realisatie)
- Loek Kasting (Dienst Publiek en Communicatie (DPC))
- Pieter Lexis (PowerDNS)
- Marit van Piggelen (NCSC)
- Hans Sinnige (Stichting Rinis)
- Martin van Son (Infoblox)
- Tony van der Togt (Min BZK)
- Paddy Verberne (Gemeente 's-Hertogenbosch)
- Jeroen van de Weerd (Inlichtingenbureau)

Redouan Ahaloui en Han Zuidweg van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

2.6 Leeswijzer

Hoofdstuk 3 geeft een korte toelichting op de standaard, met name het nut en de werking ervan.

Hoofdstuk 4 beschrijft het voorgestelde functioneel toepassingsgebied (situaties waarin de standaard functioneel gebruikt moet worden) en organisatorisch werkingsgebied (organisaties die de standaard moeten toepassen).

Hoofdstuk 5 beschrijft de resultaten van de toetsing van de standaard aan de hand van de criteria voor opname op de lijst open standaarden.

3 Toelichting standaard CAA

In afgelopen jaren zijn er wereldwijd diverse incidenten geweest waarbij een aanvaller PKI- certificaten kon aanvragen (en krijgen) voor andermans domeinen. Het ging hier met name om fouten in het uitgifteproces. Toepassing van de standaard CAA verkleint de kans dat iemand onterecht een certificaat kan verkrijgen voor domeinen van bijvoorbeeld overheidsinstellingen of banken. Hiermee kunnen met name man-in-the-middle (MitM) aanvallen worden voorkomen.

CAA is een DNS[1]-record dat domeineigenaren extra controle geeft over SSL-certificaten die worden uitgegeven voor diens domeinen. Met een CAA-record geeft een domeineigenaar aan welke certificate authority (CA) certificaten uit mag geven voor diens domeinen. Een domein eigenaar kan dit zelf regelen zonder dat hier medewerking vanuit de CA voor nodig is. Zo kan de eigenaar van een domein zelf bepalen welke CA's certificaten mogen uitgeven voor zijn of haar domeinen en kan dit ook weer (laten) wijzigen.

De CAA-standaard biedt verder de mogelijkheid aan CA's om melding te maken van foutief aangevraagde certificaten. Hierdoor krijgen domeineigenaren meer inzicht in eventuele foutieve of frauduleuze aanvragen voor het domein.

De CAA-specificatie wordt beheerd door de IETF. Het DNS CAA-Record is beschreven in RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record[2]. De versie van CAA aangemeld voor de pas-toe-of-leg-uit lijst betreft versie 1.0 uit januari 2013. Op het moment van schrijven wordt een erratum 5065 besproken, deze verandert de manier waarop CA's DNS padvalidatie moeten doen bij CAA-records. PKIoverheid TSP's dienen de wijziging zoals beschreven in RFC 6844bis[3] al te volgen (conform de Baseline Requirements van het CABforum), genoemde wijziging heeft geen impact op implementatie door overheidspartijen op hun servers en zal RFC 6844 vervangen. De publicatiedatum voor het erratum is nog niet bekend.

Met een CAA-record kunnen drie soorten tags worden meegegeven:

1. ‘issue’, hiermee machtigt de houder van de domeinnaam of een partij die handelt onder de uitdrukkelijke toestemming van de houder van die domeinnaam om certificaten af te geven voor het domein waarin het eigendom wordt gepubliceerd;
2. ‘issuewild’, hiermee machtigt de houder van de domeinnaam of een partij die handelt onder de uitdrukkelijke toestemming van de houder van die domeinnaam om 'wildcards' uit te geven voor het domein waarin de eigenschap is gepubliceerd;
3. ‘iodef’, beschrijft een URL (email en/of webservice) waarnaar een uitgevende instantie mogelijk certificaat uitgifteaanvragen

---

[1] *Het Domain Name System (DNS) is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd.*

DNS wordt ook gebruikt in het SMTP-protocol om de mailservers voor een domein op te zoeken, via zogenaamde MX-Records. Ook is er een protocol, het Sender Policy Framework (SPF), waarmee men vastlegt welke computer het recht heeft om namens een bepaald domein mail te versturen. Dit laatste als anti-spammaatregel.

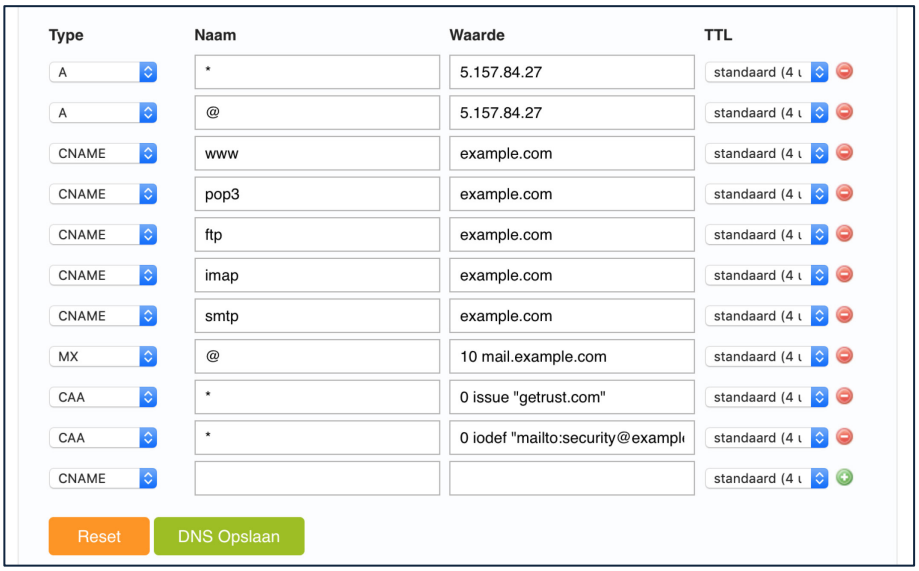
[2] *https://datatracker.ietf.org/doc/rfc6844/*

[3] *https://datatracker.ietf.org/doc/draft-ietf-lamps-rfc6844bis/*

> rapporteert die niet consistent zijn met de Certificate Practice of het Certificate Policy van de uitgever, of die een Certificate Evalator kan gebruiken om observatie van een mogelijke beleidsschending te rapporteren.

CAA is niet alleen effectief als het DNS waarin het CAA-record geadministreerd wordt, niet is beschermd met DNSSEC. Maar zonder DNSSEC bescherming kan een aanvaller het DNS verkeer omleiden, waardoor het CAA-record niet meer effectief is. De CAA specificatie (RFC 6844) adviseert dan ook ten sterkste het gebruik van CAA in combinatie met DNSSEC.

Figuur 1 laat een voorbeeld zien van een CAA-record voor het domein example.com dat aangeeft dat alleen geotrust.com certificaten voor dit domein mag uitgeven. Ook is met een CAA-iodef- record aangegeven bij welke emailadres onregelmatigheden gemeld moeten worden.



Figuur 1: Voorbeeld CAA-Record

Per september 2017 moeten CA's (wereldwijd) verplicht[4] het CAA-record van een domeinnaam controleren als onderdeel van het uitgifteproces van een certificaat. Binnen PKIoverheid dienen CA's in hun "certificate practice statement" (CPS) te vermelden welke CAA identifier zij hanteren. Het is voor domeineigenaren niet verplicht het record te vullen.

[4] https://cabforum.org/2017/03/08/ballot-187-make-caa-checking-mandatory/

4 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten* verplicht overheidsorganisaties om relevante standaarden op de pas-toe-of-leg-uit lijst uit te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de pas-toe-of-leg-uit lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

Secties 4.1 en 4.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepassingsgebied van CAA.

4.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor CAA:

CAA moet worden toegepast ten behoeve van het aanvraagproces van servercertificaten door overheden bij CA's (certificate authorities) ter autorisatie van één of meer CA's.

4.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop de 'pas toe of leg uit' verplichting van toepassing is, te weten:

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

5 Toetsing van standaard aan 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?[5]

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *'Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts',* te vinden op de website van het Forum Standaardisatie https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving van elk criterium opgenomen.

5.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

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

5.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Ja, zie paragraaf 4.1

5.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Ja, zie paragraaf 4.2

5.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)

Ja, zie paragraaf 4.1

5.1.2 Verhoudt de standaard zich goed tot andere standaarden?

5.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

Ja, het dient zelfs de aanbeveling om CAA naast bestaande standaarden toe te passen die op de pas-toe-leg-uit lijst staan.

5.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

[5] *Dit criterium is voornamelijk van toepassing op standaarden op de 'pas toe of leg uit' lijst, niet voor aanbevolen standaarden.*

Ja, CAA verkleint het risico op onbedoelde foutieve uitgave van PKI certificaten.

5.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Er zijn geen conflicterende standaarden geïdentificeerd op de lijst van open standaarden.
Bij partijen kan DANE ten onrechte als conflicterend worden gezien. DANE als afzonderlijke standaard is aanvullend op CAA en beschrijft een mechanisme om te voorkomen dat wordt vertrouwd op verkeerd uitgegeven certificaten, waar CAA beschrijft hoe het risico op foutieve afgifte van (server) certificaten te verminderen.

5.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)

CAA is een internationale standaard. CAA wordt beheerd door de IETF.

5.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

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

Naar verwachting zijn de technische implementatiekosten van CAA relatief laag wanneer binnen de gebruikte DNS-server software CAA resource records in DNS-zones opgenomen kunnen worden. De winst in veiligheid weegt op tegen de kosten, de risico's en nadelen van de adoptie van CAA. Het opnemen van CAA-records is een zeer beperkte inspanning door beheerders van de domeinen. CA's moeten CAA records verplicht checken bij uitgifte van een certificaat, waardoor de standaard zeer effectief is. Bovendien kan de CA aan de eigenaar van een domein informatie verstrekken over pogingen om ten onrechte certificaten voor het domein te registreren. Dit geeft een beter zicht op fraudepogingen. CA's zijn op dit moment al verplicht het CAA-record te controleren. Organisatorisch kunnen kosten hoog zijn vanwege organisatorische complexiteit.

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

5.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?

Ja, zie 5.1.2.2

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

Ja.

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

Ja

5.1.4 Conclusie criteria 'Toegevoegde waarde'

Ja. CAA is van toegevoegde waarde om foutieve afgifte van certificaten te verminderen en het gebruik van 'abuse-mail' geeft inzicht op mogelijke beveiligingsrisico's. Let wel op de technische en organisatorische kosten die bij de implementatie van CAA gemoeid zijn, de min-of-meer noodzakelijk gecombineerde implementatie van DNSSEC en op de privacy (AVG) bij het opnemen van persoonlijke gegevens in het iodef CAA-record.

5.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

5.2.1 Is de documentatie voor iedereen drempelvrij beschikbaar?

5.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

Ja, Het specificatiedocument is kosteloos verkrijgbaar via website van IETF. https://tools.ietf.org/pdf/rfc6844.pdf en https://tools.ietf.org/pdf/draft-ietf-lamps-rfc6844bis-04.pdf

5.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant.

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

5.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, De specificatie van CAA valt onder de Simplified BSD License, waarmee het vrij te gebruiken mits de copyright tekst wordt meegegeven bij hergebruik.

5.2.2.2 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?

Zie 5.2.2.1

5.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

Ja, het beheerproces en de besluitvorming omtrent CAA is open en transparant. Via o.a. de ACME Working Group[6] wordt met belanghebbenden overlegd over de doorontwikkeling en het beheer van CAA.

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

Ja, dat is mogelijk via The Internet Engineering Task Force (IETF)'[7].

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

Ja, de IETF kent de mogelijkheid bezwaar aan te tekenen als standaarden in concept zijn gepubliceerd.

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

Ja, Via de ACME Working Group wordt met belanghebbenden overlegd over de doorontwikkeling en het beheer van CAA.

5.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Ja

5.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

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

Ja, de standaard is in beheer bij 'The Internet Engineering Task Force (IETF)'[8].

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

Ja, die is gegarandeerd door de beheerorganisatie IETF. Sec gezien biedt het IETF geen harde garanties maar gezien de staat van dienst van de IETF heeft de expertgroep vertrouwen in het onderhoud.

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

5.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)

Ja, deze is te vinden op de website van IETF.

5.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, deze is te vinden op de website van de IETF.

---

6 *https://datatracker.ietf.org/wg/acme/charter/*
7 *http://ietf.org*
8 *http://ietf.org*

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

Het staat Nederlandse overheidspartijen vrij om deel te nemen aan de ontwikkeling en het beheer van de standaard. Het gaat om een internationale standaard die breder wordt toegepast dan alleen overheidsorganisaties. De expertgroep heeft vertrouwen in het feit dat Nederlandse belangen niet worden geschaad.

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

Ja, zie lijst deelnemers bij de IETF.

5.2.5.5 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?

Nee, aanvullende toetsing van nieuwe versies van CAA wordt aangeraden alvorens over te gaan tot opname op de pas-toe-leg-uit-lijst. Hiertoe vindt nu toetsing door onder meer de experts plaats.

5.2.6 Is er adoptieondersteuning voor de standaard?

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

Ja, bij IETF voor de standaard.

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

Nee, maar CA's doen en kunnen het al. Daarnaast is de implementatie door gebruikers zeer eenvoudig.

5.2.7 Conclusie criteria 'Open standaardisatieproces'

Ja, de standaard en het standaardisatieproces zijn voldoende open.

5.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

5.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja, courante DNS software CAA in voldoende mate te ondersteunen en CA/Browser Forum verplicht het opnemen van deze standaard.

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

Ja, dat is mogelijk.

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

Ja, implementatie van CAA staat de interoperabiliteit niet in de weg. Eenduidigheid binnen de keten met betrekking tot configuratie.

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

Ja, deze zijn aanwezig. (bijvoorbeeld https://sslmate.com/caa)

5.3.2 Kan de standaard rekenen op voldoende draagvlak?

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

Ja.

5.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?

Ja

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

Ja, de indruk is dat de standaard goed wordt gebruikt, maar het zou breder kunnen worden toegepast.

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

Niet van toepassing

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

Er is nog geen eerdere versie aangemeld.

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

Ja, zie ook 5.3.2.3. Daarnaast is het per september 2017 voor CA's (wereldwijd) verplicht het CAA-record van een domeinnaam te controleren, als onderdeel van de uitgifte van een servercertificaat. Volgens een recente (24-01-2019) telling door SIDN zijn er momenteel 14.208 unieke URL's met een CAA record. Een analyse door gemeente Den Bosch heeft opgeleverd dat 43 van de 355 gemeenten al gebruikmaakt van CAA en in combinatie met DNSSEC.

5.3.3 Conclusie criteria 'Draagvlak'

Ja, er is voldoende draagvlak voor opname op de pas-toe-of-leg-uit lijst.

5.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Met de lijst wil het OBDO de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).
- Met de pas-toe-of-leg-uit lijst beoogt het OBDO standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de lijst aanbevolen standaarden beoogt het OBDO standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

5.4.1 Is opname op de pas-toe-of-leg-uit lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja. CAA wordt nog niet breed toegepast bij de overheid, maar heeft belangrijke voordelen qua veiligheid van websites. Een pas-toe-of-leg-uit verplichting is daarom een passend middel om adoptie te bevorderen.

5.4.2 Is opname op de lijst aanbevolen standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee.

5.4.3 Conclusie criteria 'Opname bevordert adoptie'

Ja, opname van de CAA standaard op de pas-toe-of-leg-uit lijst bevordert de adoptie. Er zijn wel een aantal aanbevelingen die de adoptie verder bevorderen.

5.5 Adoptieactiviteiten

Gebruik van de standaard is het uiteindelijke doel van het Forum Standaardisatie en OBDO. Plaatsing op de pas-toe-of-leg-uit lijst of de lijst aanbevolen standaarden is hiervoor een eerste stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep adviseert het Forum Standaardisatie en OBDO om bij de opname op de lijst voor pas-toe-of-leg-uit de volgende oproepen ten aanzien van de adoptie van CAA te doen:

- Aan Logius: Maak een implementatiehandleiding (met voorbeeld) hoe op de juiste manier een CAA-record opgenomen kan worden voor PKIoverheidscertificaten, met de duidelijke verwijzing naar de te gebruiken referenties. Beschrijf daarbij ook de verschillende mogelijkheden en de implicaties van die mogelijkheden. Maak duidelijk wat de mogelijke consequentie(s) is (zijn) bij het foutief configureren van een CAA-record. Zoals bijvoorbeeld dat het heruitgeven of verlengen van een certificaat door dezelfde CA geblokkeerd worden.

- Aan het Forum Standaardisatie en het OBDO: Beschrijf het implementatieproces of beschrijf een implementatieadvies voor het inkoopproces, dit om belemmeringen weg te nemen. Beschrijf daarin in welk (inkoop-)proces je te maken krijgt voor de keuze voor implementatie van CAA.

- Aan Internet.nl: Voeg de mogelijkheid op controle van een CAA record toe op Internet.nl

- Opname van CAA op de pas-toe-of-leg-uit lijst belemmert het gebruik van ‘interne-netwerken’ niet omdat het niet gebruiken van CAA altijd beargumenteerd kan worden in het jaarverslag van de eigenaar van dat interne-netwerk.

- Aan het NCSC: Publiceer een beveiligingsadvies voor het gebruik van CAA, waaronder het voorwaardelijke gebruik van DNSSEC. (Hiertoe stuurt het NCSC een link).

- Aan alle overheden: Hanteer bij de implementatie van CAA de beveiligingsadviezen van het NCSC. https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html

- Aan het Forum Standaardisatie en het OBDO: Plaats de nieuwe CAA versie zoals onder 5.3.2.6 zonder verdere toetsing op de ‘pas toe en leg uit’-lijst vanaf het moment dat deze minimaal de IETF-status ‘proposed standard’ heeft.

- Aan DPC – Zodra internet.nl op CAA-ondersteuning kan testen en de standaard op de PTOLU-lijst staat: Breid de gepubliceerde testresultaten in het publieke websiteregister van de Rijksoverheid (http://websiteregisterrijksoverheid.nl/) uit met CAA-scores