notitie

FORUM STANDAARDISATIE 6 mei 2020

Agendapunt 3C

Nummer:	FS-20200506.3C
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	1 april 2020
Versie:	1.5
Bijlagen:	Expertadvies DNS Certification Authority Authorization Resource Record (CAA) Commentaar op de openbare consultatie CAA

1. Aanleiding en achtergrond

Sinds het DigiNotar-incident in 2011 zijn er vele ontwikkelingen geweest rond het versterken van het digitale certificatenstelsel. Het heeft geleid tot inzichten die beheerders en gebruikers van certificaten helpen om hun stelsel van maatregelen te toetsen en aan te scherpen. De standaard verkleint de kans dat iemand onterecht een certificaat kan verkrijgen voor domeinen van bijvoorbeeld overheidsinstellingen of banken. Hiermee kan worden beschermd tegen aanvallen waarbij de aanvaller zich voordoet als bijvoorbeeld een overheidspartij, bijv. middels phishing. De CAA-standaard biedt ook 'certificate authorities'(CA's) als mogelijkheid aan om melding te maken van foutief aangevraagde certificaten. Hierdoor krijgen domeineigenaren meer inzicht in eventuele foutieve of frauduleuze aanvragen voor het domein.

CAA is al sinds 2013 beschikbaar als proposed standard bij het IETF. Sinds 2017 moeten CA's bij uitgifte van een certificaat verplicht de CAA-records van het bijbehorende domein controleren, wat de standaard effectief maakt. CAA wordt nog niet breed toegepast bij de overheid, maar heeft belangrijke voordelen qua veiligheid voor websites en e-mail. De verwachting is dat opname op de lijst aanbevolen standaarden een passend middel is om adoptie te bevorderen.

2. Betrokkenen en proces

Logius heeft CAA in oktober 2018 aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst. De procesbegeleider (Lost Lemon) heeft op 9 november 2018 een intakegesprek gevoerd met de indiener (Logius). Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid op het positief doorlopen van de procedure. Op basis van de intake heeft het Forum Standaardisatie op 12 december 2018 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld. 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.

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. Van 25 februari t/m 25 maart 2019 heeft de openbare consultatie plaatsgevonden. Tijdens de openbare consultatie zijn er in totaal 2 reacties ontvangen van de Kamer van Koophandel en NLnet Labs. De reactie van NLnet Labs werd in de voorbereidende stuurgroep-vergadering Openstandaarden van het Forum van 4 april 2019 zodanig

zwaarwegend geacht dat besluit over opname van CAA is aangehouden om nader onderzoek te doen. Naar aanleiding hiervan is er overleg geweest met NLnet Labs, de indiener, Bureau Forum Standaardisatie en procesbegeleiders. Hierna is besloten de standaard voor te dragen voor de lijst van aanbevolen standaarden in plaats van voor de 'pas toe of leg uit'-lijst. Zie hoofdstuk 5 voor een nadere toelichting op het verloop van het proces.

3. Consequenties en vervolgstappen

Het Forum Standaardisatie zal op basis van het Forumadvies een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid opstellen. Het Overheidsbreed Beleidsoverleg Digitale Overheid bepaalt uiteindelijk op basis van het advies of CAA op de lijst van open standaarden wordt opgenomen met als status aanbevolen standaard.

4. Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om:

1. *CAA op te nemen op de **lijst van open standaarden met als status aanbevolen standaard**.*
2. *Het functioneel toepassingsgebied voor CAA is als volgt vast te stellen: "CAA kan worden toegepast ten behoeve van het aanvraagproces van servercertificaten door overheden bij CA's ter autorisatie van één of meer CA's."*
3. *Ten aanzien van de adoptie van CAA de oproepen te doen die beschreven staan in paragraaf 5.5 hieronder.*

5. Toelichting

5.1 Over de standaard

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

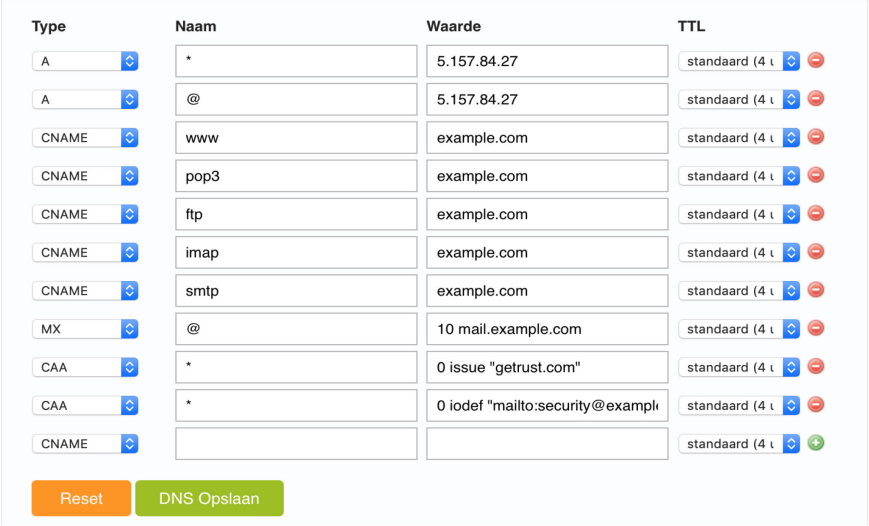
De CAA-specificatie wordt beheerd door de IETF. Op het moment van bespreking van CAA met de expertgroep werd het DNS CAA-record beschreven in RFC 6844: DNS CAA Resource Record. Dit is de versie van CAA aangemeld voor de lijst aanbevolen standaarden betreft versie 1.0 uit januari 2013. Na bespreking met de expertgroep is erratum 5065 vastgesteld en vervolgens is RFC 8659 aangenomen, die RFC 6844 vervangt. Beiden bieden verbeteringen van de standaard, maar brengen geen wijzigingen met impact die heroverweging nodig maken. (Op hoofdlijnen: veranderingen in de manier waarop CA's DNS padvalidatie moeten doen en efficiëntere algoritmiek).

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 (e-mail en/of webservice) waarnaar een uitgevende instantie mogelijk certificaat uitgifteaanvragen 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 alleen effectief als het DNS waarin het CAA-record geadministreerd wordt, is beschermd met DNSSEC. 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 uitdrukkelijk 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 welk e-mailadres onregelmatigheden gemeld moeten worden.



Figuur 1: Voorbeeld CAA-Record

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

CAA biedt bescherming bij de volgende scenario's:

- ***Scenario 1 (collega)***: Collega vraagt certificaat aan voor domein bij een andere dan de preferred Certificate Authority die in CAA-record staat. Deze andere Certificate Authority controleert het CAA-record en wijst de aanvraag af.
- ***Scenario 2 (aanvaller vraagt certificaat aan)***: Aanvaller probeert certificaat voor domein aan te vragen bij zomaar een andere Certificate Authority om een certificaat in handen te krijgen. Deze controleert de aanvraag en wijst deze af. Dit scenario beschermt alleen indien elke CA wereldwijd betrouwbaar is. De kans daarop is klein (systeem van zwakke schakel). Het zal in veel gevallen wel helpen maar het is niet waterdicht voor het beschermen tegen aanvallen.

CAA biedt geen bescherming bij de volgende scenario's:

- ***Scenario 1 (DNS-spoofing, te verhelpen met DNSSEC)***: Aanvaller spooft DNS-antwoord van CAA-record richting Certificate Authority en verkrijgt 'illegaal' certificaat voor domein.
- ***Scenario 2 (inbreken op DNS)***: Aanvaller breekt in op DNS van domein en verandert CAA-record en verkrijgt 'illegaal' certificaat voor domein.
- ***Scenario 3 (onbetrouwbare, vertrouwde CA / Diginotar)***: Aanvaller breekt in bij vertrouwde Certificate Authority, of Certificate Authority doet bewust (of per ongeluk) niets met CAA-record, en verkrijgt 'illegaal' certificaat voor domein.

5.2 Hoe is het proces verlopen?

Logius heeft CAA eind oktober 2018 aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst. De procesbegeleider (Lost Lemon) heeft op 9 november 2018 een intakegesprek gevoerd met de indiener. Op basis van de intake heeft het Forum Standaardisatie op 12 december 2018 besloten CAA in procedure te nemen.

Op 24 januari 2019 heeft een expertonderzoek plaatsgevonden waaraan experts van Logius, NCSC, DPC, SIDN, SURFnet, NLnet Labs, KPN, VNG Realisatie, PowerDNS, Stichting RINIS, Infoblox, Ministerie BZK, Gemeente 's-Hertogenbosch en Inlichtenbureau deelnamen. De leden van

de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding en het intake onderzoek. Tijdens de bijeenkomst zijn de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder besproken. Tevens zijn het toepassings- en werkingsgebied vastgesteld. Van 25 februari t/m 25 maart 2019 heeft de openbare consultatie plaatsgevonden. Tijdens de openbare consultatie zijn er in totaal 2 reacties ontvangen van de Kamer van Koophandel en NLnet Labs.

Op 4 april 2019 is versie 1.0 van het Forumadvies CAA besproken in de voorbereidende stuurgroep-vergadering Openstandaarden van het Forum. Hier is besloten het advies aan te houden en een nader onderzoek te doen naar de ingediende bezwaren van NLnet Labs tijdens de openbare consultatie. Op 7 november 2019 is er overleg geweest met: de indiener van de standaard (Logius), met de bezwaarmaker tijdens de openbare consultatie (NLnet Labs), Bureau Forum Standaardisatie en de procesbegeleider (Lost Lemon). In dit overleg geeft NLnet Labs aan dat het voornaamste bezwaar zit op de toegevoegde waarde van de standaard. Volgens NLnet Labs komt niet goed naar voren wat en waar CAA wel of niet op beveiligt. De suggestie kan worden gewekt dat CAA voldoende bescherming biedt maar dit is slechts beperkt en dat CAA hiervoor het enige middel is, wat niet het geval is. Bovendien heeft CAA beperkingen, het gaat uit van het vertrouwen in de CA: een kwaadwillende CA kan CAA immers ook negeren. Hiertoe heeft NLnet Labs een aantal scenario's aangedragen (zie scenario's in paragraaf 5.1).

Uit het overleg blijkt ook dat er bedenkingen zijn bij het plaatsen van CAA op de 'Pas toe of leg uit'-lijst. De toegevoegde waarde van CAA is te gering omdat het op zichzelf te weinig beveiligingszekerheid biedt. Het rechtvaardigt daarom eerder een plaatsing op de lijst Aanbevolen standaarden. Logius kan als indiener van CAA deze beredenering volgen, maar heeft bij het ministerie Algemene Zaken en bij het Nationaal Cyber Security Centrum (NCSC) consulatie gedaan of er toch gegronde, zwaarwegende argumenten zijn om CAA alsnog op te nemen op de 'Pas toe of leg uit'-lijst. Beiden geven aan voorstander te zijn om CAA op te nemen op de 'Pas toe of leg uit'-lijst, maar komen niet met sterkere argumentatie dan in paragraaf 5.1 staat beschreven. De indiener sluit zich dan ook aan op het bezwaar van NLnet Labs en gaat akkoord met het aangepaste Forumadvies om CAA voor te dragen voor de lijst van aanbevolen standaarden. De conclusie van het nader onderzoek is daarom CAA wel op te nemen als standaard, maar op de lijst van aanbevolen standaarden.

De conclusie van het nader onderzoek is daarom CAA wel op te nemen als standaard, maar op de lijst van aanbevolen standaarden. Hiervoor moest het advies wel aangescherpt worden op wat CAA wel en niet beveiligt doormiddel van de scenario's (zie paragraaf 5.1).

5.3 Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht. The Internet Engineering Task Force (IETF) kent een goed gedocumenteerd en open beheerproces. De besluitvorming omtrent CAA is open en transparant en via o.a. de ACME Working Group wordt met belanghebbenden overlegd over de doorontwikkeling en het beheer van CAA. Het staat Nederlandse overheidspartijen vrij om deel te nemen aan de ontwikkeling en het beheer van de standaard.

Toegevoegde waarde

CAA is van toegevoegde waarde om het risico op foutieve uitgifte van certificaten te verlagen, met in achtneming van de eerder geformuleerde scenario's (zie paragraaf 5.1). Het rapportagemechanisme geeft inzicht in fouten die zijn voorkomen. Met CAA kan een organisatie beleid publiceren over welke CA-certificaten mag uitgeven voor haar domeinnaam.

CAA heeft ook beperkingen (zie paragraaf 5.1 voor de scenario's waarvoor CAA geen bescherming biedt). CAA gaat uit van vertrouwen in de CA: een kwaadwillende CA kan CAA immers ook negeren.

Bovendien kan een aanvaller die DNS-instellingen aanpassen, de CAA-record verwijderen waardoor alle CA's voor de domeinnaam certificaten kunnen uitgeven. Om de integriteit van het CAA-record onderweg te waarborgen is het van belang om dit te ondertekenen met de DNSSEC-standaard die reeds op de 'pas toe of leg uit'-lijst staat.

Draagvlak

Er is voldoende draagvlak binnen de overheid voor het opnemen van de standaard op de lijst

aanbevolen standaarden. Het is 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 in het .nl-domein. Ten tijde van de expertconsultatie (januari 2019) heeft gemeente 's-Hertogenbosch een analyse gedaan waaruit bleek dat 43 van de 355 gemeenten al gebruikmaakt van CAA in combinatie met DNSSEC.

Opname bevordert de adoptie

De experts geven tijdens de expertsessie aan dat hoewel CAA nog niet breed wordt toegepast bij de overheid, de standaard bijdraagt aan de veiligheid van websites. Gegeven de beperkte toegevoegde waarde van de standaard is een aanbevolen standaard een passend middel om adoptie te bevorderen. Er is wel een aantal aanbevelingen aangedragen die de adoptie verder bevorderen (zie paragraaf 5.5).

5.4 Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van het expertonderzoek en analyse openbare consultatie

De expertgroep adviseerde het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid om CAA op te nemen op de 'pas toe of leg uit'**-**lijst.

Analyse van reacties uit de openbare consultatie

In de openbare consultatie kwam vanuit NLnet Labs een bezwaarpunt naar voren om CAA op te nemen op de 'pas toe of leg uit'-lijst. Het gaat dan met name over de toegevoegde waarde van CAA en relatie tot DANE. De reactie is zorgvuldig afgewogen en biedt vanwege de te beperkte toegevoegde waarde **voldoende reden om af te wijken van de conclusies van het expertonderzoek**.

Hieronder de ontvangen reacties tijdens de openbare consultatie:

- "Ik heb moeite met het advies om CAA op te nemen op de 'pas toe of leg uit'-lijst. De keuze voor dit advies lijkt genomen te zijn zonder duidelijk te hebben wat de toegevoegde waarde is. Er zijn scenario's waar CAA toegevoegde waarde heeft, maar deze zijn voor zover ik het kan inzien niet voor alle organisaties van toepassing."

- "Het grote probleem met het CA systeem is dat alle CA's de macht hebben om certificaten uit te geven voor alle domeinen." ... "Vertrouwen dat alle CA's geen verkeerde intenties hebben (inclusief CA's van buitenlandse overheden) en vertrouwen dat alle CA's compleet beschermd zijn tegen alle aanvallen (zoals de Diginotar zaak)."

- "Om deze reden zou het zinvol zijn om de vertrouwensrelatie te beperken tot een enkele CA, iets wat CAA op eerste gezicht lijkt aan te bieden maar niet doet. Door de validatie door de CA te laten uitvoeren blijft de noodzaak om alle CA's te vertrouwen. Dit kan opgelost worden door de validatie op de client te laten uitvoeren, wat bijvoorbeeld het geval is bij DANE. De eventuele voordelen van CAA worden ook afgevangen als DANE zou worden gebruikt."

- Een reactie van Kamer van Koophandel onderschrijft het positieve advies uit het expertonderzoek en benoemt drie aanvullende adviezen:

    - Met de implementatie van CAA ook DNSSEC toepassen.

    - Gebruik een algemeen e-mailadres en geen persoonlijk e-mailadres voor het iodef-record.

    - DNS-services dienen wel geschikt zijn voor toepassing van CAA-records.

Tijdens het opstellen van het Forumadvies zijn de reacties zoveel mogelijk meegenomen in het advies.

5.5 Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

- Aan Logius: Maak een implementatiehandleiding (met voorbeeld) hoe op de juiste manier een CAA-record opgenomen kan worden voor PKI-overheidscertificaten, 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 Internet.nl: Voeg de mogelijkheid op controle van een CAA-record toe op Internet.nl.

- Aan alle overheden: Hanteer bij de implementatie van CAA de beveiligingsadviezen van het NCSC.

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

6. Referenties

[1] Expertadvies CAA:
https://www.forumstandaardisatie.nl/sites/bfs/files/Expertadvies%20CAA.pdf

[2] Reacties uit de consultatieronde CAA:
https://www.forumstandaardisatie.nl/sites/bfs/files/Consultatiedocument%20CAA.pdf