notitie

FORUM STANDAARDISATIE 12 december 2018
Agendapunt 3B Intakeadvies CAA

Aan: Forum Standaardisatie
Van: Stuurgroep Open Standaarden

Datum: 26 november 2018
Versie: 1.0

Bijlagen: niet van toepassing

Advies
Het Forum Standaardisatie wordt geadviseerd om de internet veiligheidstandaard *RFC 6844: DNS Certification Authority Authorization Resource Record* (kort: "CAA") in procedure te nemen voor opname op de pas-toe-of-leg-uit lijst.

Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst. In de toelichting hieronder wordt dit advies nader onderbouwd.

Toelichting
1. Korte beschrijving van de standaard
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 een certificaat kan aanvragen 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. Het gebruik van CAA betekent overigens niet dat je vastzit aan een CA.

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.

[1] Het Domain Name System (DNS) is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om URLs (zoals www.standaardisatie.nl) naar numerieke Internet-adressen (zoals "192.168.1.1") te vertalen en omgekeerd. DNS wordt zowel bij websites als bij e-mail gebruikt.

CAA 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 veranderd de manier waarop CA's DNS pad-validatie moeten doen bij CAA-records. PKIoverheid TSP's dienen deze RFC al te volgen (conform Programma van Eisen PKIoverheid), genoemde wijziging heeft geen impact op implementatie door overheidspartijen op hun servers. De publicatiedatum voor het erratum is nog niet bekend.

Het heeft eigenlijk alleen zin om CAA toe te passen als het DNS waarin het CAA-record geplaatst wordt, beschermd is 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 ten sterkste het gebruik van CAA in combinatie met DNSSEC.

Figuur 1 laat een voorbeeld zien van een CAA-record voor het domein surviveraar.nl 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[3] het CAA-record van een domeinnaam controleren als onderdeel van 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.

2. Betrokkenen en proces

DNS Certification Authority Authorization (CAA) Resource Record is eind oktober 2018 aangemeld door Jochem van den Berge van Logius. Op 9 november 2018 heeft een intakegesprek plaatsgevonden met de aanmelder. Op basis van dit intakegesprek en eigen onderzoek heeft de procedurebegeleider Arjen Brienen van Lost Lemon dit intakeadvies samengesteld.

Als het Forum Standaardisatie CAA in procedure neemt, volgt een expertonderzoek om te toetsen of CAA voldoet aan de criteria voor plaatsing op de pas-toe-of-leg-uit lijst.

[2] https://tools.ietf.org/pdf/rfc6844.pdf
[3] https://cabforum.org/2017/03/08/ballot-187-make-caa-checking-mandatory/

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

CAA voldoet aan alle vier criteria om in behandeling genomen te worden voor opname op de pas-toe-of-leg-uit lijst. Hoe de standaard is getoetst op de vier criteria[4] wordt hieronder toegelicht in paragrafen 3.1-3.4.

3.1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

Ja. CAA is van toepassing op alle met certificaten beveiligde communicatie over het Internet tussen overheidsorganisaties en burgers, bedrijven en andere overheden. Hieronder vallen alle met https beveiligde websites en met (START)TLS beveiligde e-mail.

PKIOverheid is daarnaast als CA direct een belanghebbende overheidsorganisatie.

3.2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

Ja. CAA is van toepassing op alle overheidsorganisaties die websites hebben en/of e-mail uitwisselen, en is niet gebonden aan een specifieke overheidsorganisatie of sector.

3.3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

Ja. Het gebruik van CAA-records is niet wettelijk verplicht.

3.4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits-)probleem en het voorkomen van leveranciersafhankelijkheid?

Ja. CAA verkleint de kans dat certificaten misbruikt worden. Zo maakt de standaard het moeilijker om onterecht uitgegeven certificaten te gebruiken voor man-in-the-middle aanvallen waarmee bijvoorbeeld vertrouwelijke gegevens zoals wachtwoorden buitgemaakt kunnen worden.

4. Is er zicht op een positief expertadvies?

Wanneer het Forum Standaardisatie de standaard in procedure neemt, zal een groep experts de standaard gaan toetsen op de vier inhoudelijke criteria[5] voor opname op de lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan al vaststaat dat deze in het expertonderzoek op tenminste één van de criteria zal stranden. 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 CAA op de pas-toe-of-leg-uit lijst in de weg zou kunnen staan. Dit wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1. Toegevoegde waarde

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 geeft 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.

Er zijn geen beveiligings- en privacy risico's geïdentificeerd.

[4] Meer informatie over de criteria voor het in procedure nemen van een standaard op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl

[5] Meer informatie over de inhoudelijke toetsingscriteria op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl

4.2. Open standaardisatieproces

TLS wordt beheerd door IETF. Het specificatiedocument is kosteloos verkrijgbaar via website van IETF. De specificatie van CAA valt onder de Simplified BSD License, waarmee het vrij te gebruiken mits de copyright tekst wordt meegegeven bij hergebruik.

IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant. Via de TLS Working Group worden regelmatig met belanghebbenden overleggen gehouden over de doorontwikkeling en het beheer van TLS.

4.3. Draagvlak

CAA is al sinds 2013 in gebruik. Sinds 2017 moeten CA's bij uitgifte van een certificaat verplicht de CAA records van het bijbehorende domein controleren, wat de standaard zeer effectief maakt. PKIOverheid is als CA een directe belanghebbende die opname van CAA op de pas-toe-of-leg-uit lijst steunt. In het expertonderzoek zal onderzocht moeten worden hoeveel draagvlak er bestaat voor verplicht gebruik van CAA bij andere overheidsorganisaties.

Gangbare DNS software (bijvoorbeeld BIND) lijkt CAA in voldoende mate te ondersteunen. Marktondersteuning zal nog wel nader moeten worden onderzocht in het expertonderzoek.

4.4. Opname op de lijst bevordert adoptie

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

5. Samenhang met andere standaarden op de lijst

TLS heeft directe samenhang met drie standaarden op de pas-toe-of-leg-uit lijst:

- *HTTPS* is een toepassing van het http protocol over TLS-verbinding met als doel de veilige uitwisseling van gegevens tussen een (web)server en client. Deze beveiligde verbinding wordt op basis van certificaten gelegd. Op de uitgifte van deze certificaten is CAA van toepassing.
- *TLS* (Transport Layer Security) en diens voorganger Secure Sockets Layer (SSL), zijn encryptie-protocollen die de communicatie tussen computers (bijvoorbeeld op het internet) beveiligen. Net als http werkt TLS op basis van certificaten.
- *DNSSEC* is een uitbreiding op het DNS-protocol dat het gebruik van domeinnamen veiliger maakt. DNSSEC beschermt het DNS tegen ongewenste manipulatie en dient als basis voor verdere beveiligende standaarden waaronder DANE[6]. De CAA specificatie (RFC 6844) adviseert ten sterkste om CAA-records alleen op te nemen in een met DNSSEC beveiligd DNS.

TLS heeft ook samenhang met de X.509 standaard (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile) die op de lijst aanbevolen standaarden staat. X.509 beschrijft een systeem van certificaten met een beperkte levensduur en de wijze waarop de intrekking van deze certificaten in een zwarte lijst (de Certificate Revocation List of CRL) geregeld wordt.

6. Welke organisaties ondersteunen deze aanmelding?

De aanmelding van CAA wordt ondersteund door het Nationaal Cyber Security Centrum (NCSC), Stichting Internet Domeinregistratie Nederland (SIDN) en het ministerie van Algemene Zaken (minAZ).

Hoe gaan deze organisaties zelf om met CAA?

- NCSC heeft CAA heeft een fact sheet[7] gepubliceerd over het veilig beheer van certificaten waarin CAA wordt aanbevolen.
- SIDN heeft CAA geïmplementeerd.

[6] https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

[7] https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html

- minAZ (overheid.nl) heeft CAA nog niet geïmplementeerd.

7. Use case

Er zijn vele organisaties, certificate authorities (CA's) genaamd, die SSL-certificaten kunnen afgeven die instaan voor de identiteit van uw domein. Om te voorkomen dat een willekeurig CA een certificaat uitgeeft aan een partij die doet alsof het de eigenaar is van uw domein kan er en CAA record worden opgenomen in het DNS. Met CAA (Certification Authority Authorization) kunt u aangeven welke certificaatautoriteiten u daadwerkelijk gebruikt, waarbij u de anderen verbiedt certificaten uit te geven voor uw domein.

Doordat er online hulpmiddelen vrij beschikbaar zijn voor het opstellen van een CAA-record en het opnemen van een CAA-record in een DNS niet moeilijk is, is het een makkelijk manier om misbruik van een domeinnaam te voorkomen.

Omdat DNS van zichzelf geen sterk beveiligd systeem is en potentieel omzeild kan worden waardoor hackers DNS-instellingen kunnen aanpassen, biedt een CAA record maar een beperkte beveiliging. Het is daarom sterk aan te raden om ook DNSSEC in te stellen. DNSSEC beveiligt de instellingen van een domeinnaam door een versleutelde handtekening toe te voegen aan de DNS-records.