



# Notitie

Aan: Forum Standaardisatie  
Van: Bureau Forum Standaardisatie  
Datum: 31 maart 2019  
Versie: 1.0  
Betreft: Reacties uit de openbare consultatie CAA

## Inleiding

Dit document bevat de reacties die tussen 25 februari en 25 maart werden ontvangen op de openbare consultatie voor plaatsing van CAA op de 'pas toe of leg uit' lijst van het Forum Standaardisatie. In totaal zijn 2 reacties ontvangen van de Kamer van Koophandel en NLnet Labs. De reacties, die als e-mail binnenkwamen, zijn in zijn originele vorm zonder bewerking weergegeven in chronologische volgorde van binnenkomst. Wel zijn de contactgegevens en is voor deze consultatie niet-relevante tekst verwijderd.

## Reacties uit de openbare consultatie

### Reactie van Kamer van Koophandel:

**Van:** Frits Maas <...>  
**Verzonden:** donderdag 28 maart 2019 10:20  
**Aan:** Forum standaardisatie <...>  
**CC:** Rob Spoelstra <...>  
**Onderwerp:** RE: Openbare consultatie reactie Kamer van Koophandel dd 25 maart 2019

Geachte heer/mevrouw,

Hiermee reageren we op uw openbare consultatie verzoek voor diverse adviezen.

#### (als bijlage):

De Kvk heeft de volgende opmerkingen.

Prima voorstel mits inderdaad voldaan aan:

1. Ook het toepassen van DNSSEC
2. Correcte configuratie van de CAA records (voor alle uitgevende CA's waar gebruik van wordt gemaakt en gebruik van een algemeen email adres en geen persoonlijk email adres)
3. De DNS services waar we gebruik van maken geschikt zijn om de CAA records te kunnen publiceren voor de drie modi.

De opmerkingen zijn, zover we kunnen beoordelen, ook al verwoord in het document.

Met vriendelijke groet,

## **Reactie van NLnet Labs:**

-----Oorspronkelijk bericht-----

Van: Ralph Dolmans <...>

Verzonden: vrijdag 29 maart 2019 12:53

Aan: Forum standaardisatie <...>

Onderwerp: Reactie openbare consultatie CAA

Hallo,

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 alles CA's de macht hebben om certificaten uit te geven voor alle domeinen. Dit betekent dat je genoodzaakt bent om alle CAs te vertrouwen. Vertrouwen dat alle CAs geen verkeerde intenties hebben (inclusief CAs van buitenlandse overheden) en vertrouwen dat alle CAs 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 CAs 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.

-- Ralph