

Certification Authority Authorization (CAA)

Berechtigung ausgewählter Zertifizierungsstellen zur Ausstellung von Zertifikaten



Stand: 17.10.2022, BETA

Management Summary

Sehr viele Zertifizierungsstellen (CA) können gültige Verschlüsselungszertifikate für beliebige Webseiten ausstellen. Um das Vertrauen in das Zertifikat ihres OZG-Dienstes zu er-

höhen, wird technisch eingeschränkt, welche CA berechtigt ist, für die Internetadresse ihres OZG-Dienstes Verschlüsselungszertifikate auszustellen.

Ressourcenabschätzung

-  Gering (< 5 PT)
-  Ohne neue Hardware

Erläuterung für OZG-Dienstverantwortliche

Ein Verschlüsselungszertifikat ist ein nahezu fälschungssicherer Ausweis des OZG-Dienstes gegenüber den Bürgerinnen und Bürgern. Sehr viele Zertifizierungsstellen (CA) können gültige Verschlüsselungszertifikate für beliebige Webseiten ausstellen. DNS Certification Authority Authorization (CAA) schränkt hierbei ein, dass nur eine bestimmte CA ein gültiges Zertifikat für ihre Domain aus-

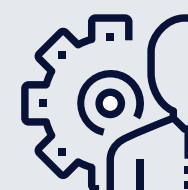
tellen kann. Mittlerweile sind diese Zertifizierungsstellen verpflichtet, vor Ausstellung eines Zertifikats zu prüfen, ob diese einer anderen Zertifizierungsstelle vorbehalten ist.

Referenz



RFC 8659

Umsetzung



RZ-Betrieb

Technischer Umsetzungsansatz

Die CAA-Ressource wird über die DNS-Verwaltung konfiguriert. Es können hierbei eine oder mehrere Zertifizierungsstellen angegeben werden, die berechtigt sind, Zertifikate für einen Domännennamen auszustellen (Wildcards sind möglich). Die CAA Konfiguration muss dem RFC 8659 entsprechen. Es müssen mindestens

die "issue" Eigenschaft zur Definition der CA und "iodef" Eigenschaft zur Angabe eines Kontakts (z. B. E-Mail) gesetzt werden.

Die Kombination mit DNSSEC ist besonders empfehlenswert.

`bsi.bund.de.`

`IN CAA 0`
`issue "dtrust.de"`

`IN CAA 0`
`iodef "mailto:isb@bsi.bund.de"`

CAA Einträge der Domäne bsi.bund.de