RapidSSL™

GUIDE TO CAA

RapidSSL Technical Report

This report explains Certification Authority Authorization (CAA), a technology that uses the Domain Name System (DNS) to inform Certificate Authorities (CAs) of the customer's preferred certificate issuer. Use this report to determine if CAA is right for you and your website.

Introduction

DNS Certificate Authority Authorization (CAA) is defined in an IETF draft RFC. Its stated purpose is to allow a DNS domain name holder to specify the certificate signing certificate(s) authorized to issue certificates for that domain. The use of CAA can reduce the risk of unintended certificate mis-issuance, either by malicious actors or by honest mistake.

For example, if you own example.com, and wish to express your preference that certificates for that domain should only be issued by Primary CA, Inc., you would create a record in DNS indicating such. If a malicious actor, or an employee who is not aware of your preference, engages a different CA, Secondary CA, Inc. to purchase a certificate, Secondary CA might first check in DNS. If they see that you have a CAA record that does not specify Secondary CA as a preferred certificate issuer, Secondary CA could alert you of that. You could then choose to deny the certificate purchase, or change or add to DNS your preference to allow Secondary CA to issue certificates for your domain.

Advantages

CAA is a simple way to express your preference of CA. Since you own your domain name and control all DNS information for that domain, you can add CAA information to DNS, and change it when you wish. No other party, including the CA, needs to be involved.

If you are responsible for your company's certificate infrastructure, you may benefit by using CAA. For example, you may have negotiated a volume discount with a particular CA, and wish to purchase all your certificates from that CA to save money. With CAA, you may be alerted when an employee enrolls for a certificate with a different CA.

CAA also includes a feature that enables CAs to report invalid certificate requests. Any compliant CA could notify you via email, web service, or both, about any certificate request they received that did not match the preference you set in your CAA record.

If you use CAA, you're not tied to one CA. It's possible to create multiple CAA records for multiple CAs that you wish to do business with. Or you can use CAA to specify that no CA should issue certificates to your domain.

Disadvantages

There are several disadvantages of CAA to be aware of:

Compliance with CAA is voluntary. CAs are not required to check for a CAA record or comply with its contents if they do. However, many public CAs are now considering support for CAA.

A compliant CA could still ignore your CAA record, as long as they conform to whatever CAA policy is expressed in their Certification Practices Statement (CPS).

It isn't necessarily secure. Attackers have ways of subverting DNS, and although Domain Name System Security Extensions (DNSSEC) can prevent some of those attacks, the use of DNSSEC is not mandatory with CAA.

It may be difficult for you to make changes in your DNS information. You may have to engage other people within your company or an external vendor to make the necessary changes.

It may slow down certificate issuance if a compliant CA checks your CAA record and determines that it is not specified in that record. The CA may want you to update your CAA record before issuing the certificate, or may wish to get a waiver from you approving the certificate issuance.

What is RapidSSL Doing About CAA?

RapidSSL believes in helping to prevent mis-issuance of certificates, and CAA may assist in that effort. We're adding CAA records to own zone files. More importantly, in the near future we'll be adding a CAA check to all our certificate enrollment processes. If you have a CAA record and enroll for a certificate from any of RapidSSL's portals, we'll check the contents of your CAA record to see if we're listed as a preferred CA (see Details below). If not, we'll block issuance of the certificate and contact you. You'll be asked to either update your CAA record, give us permission to issue the certificate, or cancel the request.

Details

If you would like to list RapidSSL as your CA preference in a CAA record, here's what to do:

In the simplest case, where you simply want to express a preference to use RapidSSL for your domain example.com, you would simply edit your example.com DNS zone file to include:

```
$ORIGIN example.com
.  CAA 0 issue "rapidssl.com"
```

The single CAA record will apply to all web servers in your domain, like www.example.com, shop.example.com, checkout.example.com, etc. It indicates your preference that SSL certificates for any web server in that domain should be issued by RapidSSL.

Note that if you wish to indicate a preference for two or more CAs, say, RapidSSL and GeoTrust, you simply use two CAA records like this:

```
$ORIGIN example.com
.   CAA 0 issue "rapidssl.com"
.   CAA 0 issue "geotrust.com"
```

That signifies that either RapidSSL or GeoTrust can issue certificates for your domain.

Because CAA records are checked hierarchically in DNS from a leaf up to the root, the above line will also apply to servers in any subdomains too. Let's say your company has two divisions, East and West, and you create a subdomain for each, east.example.com and west.example.com. Each subdomain will probably have its own DNS zone file, and if you want the RapidSSL preference to apply to those too, there's nothing else you need to do.

But let's say you want to let OtherCA issue certificates for the East division. All you need to do is add a CAA record to the zone file for east.example.com:

```
$ORIGIN east.example.com
.   CAA 0 issue "otherca.com"
```

Any CA that checks for CAA records for, say, hr.east.example.com will first check in the zone file for east.example.com and see the CAA record for otherca.com. This will override the CAA record in the zone file for example.com.

You may specify a different preference in the west.example.com DNS zone file, but if you don't, any CA that checks for CAA records will find none in west.example.com, but will then find the CAA record in example.com.

If you have multiple sub-domains and certificates from different CAs on web servers in those sub-domains, you'll want to do an inventory of your certificates and sub-domains. Note that you don't need to create CAA records that reflect your current certificates and the CAs that issued them – CAA records are checked only when one enrolls for a new certificate. These records won't be checked by browsers when someone visits your website.

Finally, if you try CAA but decide it's not advantageous, you can simply remove your CAA record(s) from DNS.

Conclusion

CAA is a relatively low-cost approach to preventing certificate mis-issuance, although it's not foolproof. By itself, CAA does not provide high levels of security, but it might be appropriate as one of many tools in your toolkit to protect your domain name, web site and brand.

Contact RapidSSL:

RapidSSL.com US
350 Ellis Street, Bldg. J
Mountain View, CA 94043
USA

Tel: 1-650-426-7202
Toll Free: 1-866-795-4669
Office hours: 8:30am to 4:30pm EST

UID - 214/11/13