What is Certificate Authority Authorization (CAA)?

DNS Certification Authority Authorization (CAA) is designed to allow a DNS domain name holder (a website owner) to specify one or more Certificate Authorities (CAs) the authority to issue certificates for that domain or website, according to a definition in IETF draft RFC 6844.

With the latest industry standards, a CA will have to check CAA records to make sure that they have the authority to issue the certificates for a particular domain, prior to issuance. For example, if you own *thawte.com*, and wish to have certificates for that domain issued by Symantec, you would create a CAA record in DNS with Symantec as your CA of choice. You may have more than one CAA record if you work with more than one CA.

With CAA, if a malicious actor, or another employee engages a CA to issue a certificate for *thawte.com*, that CA must first check in DNS. The unlisted CA is allowed to issue the certificate for your domain if no CAA records exist. However, the unlisted CA is not allowed to issue the certificate if CAA records for other CAs exist. This new requirement helps to mitigate the risks of certificate issuance by unauthorized CAs.

The creation and modification of the CAA records are controlled by the organization or website owner. The CAA records can help with the enforcement of your corporate policies on approved CAs. By aligning the CAA records with the list of corporate approved CAs, the risk of non-compliance to the policy is minimized. An employee who is not familiar with the policy will not be able to obtain certificates issued by a CA that is not on the corporate list.

If CAA records exist but do not include an approved or preferred CA for a specific domain, the issuance of certificates by that CA to the domain cannot proceed until the creation of the appropriate CAA record is completed.

It is recommended that you create CAA records for your approved CAs to minimize business impact. With CAA, you can minimize the risk of certificate issuance by unauthorized CAs and help create a more secure and transparent online ecosystem.