CAA BEST PRACTICES

Understanding Certification Authority Authorization

Entrust Datacard™

INTRODUCTION

Certification Authority Authorization (CAA) enables a domain owner to specify in their DNS records the certification authority (CA) that is authorized to issue certificates to their domain. The new CAA policy has been defined by the CA/Browser forum and is scheduled to take effect September 8, 2017. The technical requirements for CAA are covered by standard RFC 6844.

CAA records support the following properties:

- Issue: Permits only specified CAs to issue certificates.
- Issuewild:
  - Permits a CA to issue a wildcard certificate, but does not permit the issuance of non-wildcard certificates.
  - Can prevent wildcard certificates from being issued.
- Iodef: Provides an email address or website where the CA can report requests that violate the CAA record policy.

All CAs will be required to check the CAA records for all domain names requested at the time of certificate issuance and must act as follows:

- If there is no CAA record, the CA can issue the requested certificates.
- If an "issue" CAA record matches the issuer domain name from the CA's CPS, then the CA can issue certificates.
- If there is at least one CAA "issue" record, but none of them match the no issuer domain name from the CA's CPS, then the CA cannot issue certificates.

ADVANTAGES

There are about 140 different government and global CA organizations that have their root certificates distributed within operating systems and browsers. The roots may have thousands of intermediate CAs, many of which can issue SSL/TLS certificates. CAA tightens security for domain owners by enabling them to limit certificate issuance to only those CAs they have granted permission to – this can be either none, one or many specific CAs.

CAA can also grant permission for wildcard certificates. This allows a specific CA to issue wildcard certificates or completely prevent the issuance of wildcard certificates for the domain.

CAA may be the best way to protect domain owners from having fraudulent certificates issued in their domain name. This has become increasingly important with the proliferation of unauthorized domain validated (DV) certificates.

DISADVANTAGES

Many enterprises use more than one CA. This may be due to departments sourcing their certificates differently or perhaps there is no policy in effect that limits certificate purchases to a specific CA(s). As such, if a domain owner is planning to use CAA, they should ensure they permit all of their trusted CAs. If a trusted CA is omitted from CAA users could experience issues with certificates issued by an unlisted CA.

Certificate Discovery or running a **CT Search** scan will help to uncover most of the trusted CAs who have issued certificates to their domain. Once domain owners know who their trusted CAs are, they can either permit or decline future issuance by indicating in the CAA record.

DEPLOYMENT

Each CA must define their issuer domain name in their certification practice statement (CPS). Domain owners who want to use CAA to permit only specific CA(s) to issue certificates must create a CAA record with the issuer domain name and add it to their DNS.

Authorized CA

Here is an example of a CAA issue record for domain example.com:

```
example.com.    IN    CAA    0 issue "ca.issuer-one.com"
```

The CAA *issue* record allows a CA that owns the right to use “ca.issuer-one.com” to issue certificates for domain name “example.com.”

Here is an example of CAA *issue* records where two CAs have been authorized:

```
example.com.    IN    CAA    0 issue "ca.issuer-one.com"

example.com.    IN    CAA    0 issue "ca.issuer-two.com"
```

Certificate issuance can be prohibited by setting a CAA issue record that does not identify an authorized CA:

```
example.com.    IN    CAA    0 issue ";"
```

NOTE: If there is no CAA *issuewild* record, the CAA issue record will also authorize requested wildcard certificates to be issued.

Wildcard Certificate Authorization

Wildcard certificates can also be authorized with the CAA ***issuewild*** record. The *issuewild* record has precedence over an issue record. Here is an example of a CAA *issuewild* record:

```
example.com.    IN    CAA    0 issuewild "ca.issuer-one.com"
```

Wild certificate issuance can be prohibited by setting a CAA issuewild record that does not identify an authorized CA. For example:

```
example.com.    IN    CAA    0 issuewild ";"
```

Authorization Policy Issues

In some cases, a CA may be declined from issuing a requested certificate due to the CAA record. The certificate requester may not understand that the authorized CAs have been restricted. The CAA policy owner can be advised of these request if a CAA iodef record is provided. The iodef record may provide an email or a website address.

```
example.com.    IN    CAA    0 iodef "mailto:security@example.com"

example.com.    IN    CAA    0 iodef "http://iodef.example.com"
```

If a CA rejects a certificate request due to a CAA record, they may respond to the CAA iodef

RECOMMENDATIONS

- Since it will be mandatory for all CAs to check the CAA records beginning in September 2017, it will be a great benefit for domains to register approved CAs to prevent fraudulent certificates from being issued to your domains.
- Before you deploy a CAA record, ensure you identify your current trusted CAs. This can be done by performing a CT search or by using a certificate discovery tool. Once CAs are identified, deploy CAA records for all CAs you plan to continue using.
- If you only use one CA for a particular domain, it is prudent to allow for at least one fallback CA.
- Be aware if your domain is used in any CDN (Content Delivery Network, like Cloudflare or Akamai) web server certificates, which may be issued from other than your preferred CA.
- Your security policy may not allow the use of wildcard certificates. If this is the case, deploy a CAA record prohibiting the issuance of wildcard certificates.
- Although responding to the CAA iodef record is not mandatory, it is recommended to have an iodef record to support investigation into unauthorized certificate requests.
- You can set a CAA Record for any unused high value sub-domains as well (such as www, secure, shop, mail, etc) preventing issuance of any certificates.
- Here is an example of a CAA record that: authorizes two CAs; prohibits wildcard certificates and provides an email address for fraudulent certification notification:

```
example.com.    IN    CAA    0 issue "ca.issuer-one.com"
example.com.    IN    CAA    0 issue "ca.issuer-two.com"
example.com.    IN    CAA    0 issuewild ";"
example.com.    IN    CAA    0 iodef "mailto:security@example.com"
```

ENTRUST DATACARD AND CAA

Entrust Datacard supports CAA. By specifying Entrust Datacard as one of your trusted CAs in the CAA records (as shown below), it allows us to issue certificates to your domain:

```
example.com.    IN    CAA    0 issue "entrust.net"
example.com.    IN    CAA    0 issuewild "entrust.net"
```

@EntrustDatacard   /EntrustVideo   /EntrustSecurity   datacard-group

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust Datacard products and services, call **888-690-2424**, email **sales@entrustdatacard.com** or visit **www.entrustdatacard.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™