Certification Authority Authorization (CAA) Processing for Email Addresses

Abstract

   The Certification Authority Authorization (CAA) DNS resource record
   (RR) provides a mechanism for domains to express the allowed set of
   Certification Authorities that are authorized to issue certificates
   for the domain. RFC 8659 contains the core CAA specification, where
   Property Tags that restrict the issuance of certificates that certify
   domain names are defined. This specification defines a Property Tag
   that grants authorization to Certification Authorities to issue
   certificates that contain the id-kp-emailProtection key purpose in
   the extendedKeyUsage extension and at least one rfc822Name value or
   otherName value of type id-on-SmtpUTF8Mailbox that includes the
   domain name in the subjectAltName extension.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc9495.

Copyright Notice

Table of Contents

1. Introduction

   The Certification Authority Authorization (CAA) DNS resource record
   (RR) provides a mechanism for domains to express the allowed set of
   Certification Authorities that are authorized to issue certificates
   for the domain. [RFC8659] contains the core CAA specification, where
   Property Tags that restrict the issuance of certificates that certify
   domain names are defined. [RFC8659] does not define a mechanism to
   restrict the issuance of certificates that certify email addresses.
   For the purposes of this document, a certificate "certifies" an email
   address if the certificate contains the id-kp-emailProtection key
   purpose in the extendedKeyUsage extension and at least one rfc822Name
   value or otherName value of type id-on-SmtpUTF8Mailbox that includes
   the domain name in the subjectAltName extension.

   This document defines a CAA Property Tag that restricts the allowed
   set of issuers of certificates that certify email addresses. Its
   syntax and processing are similar to the "issue" Property Tag as
   defined in Section 4.2 of [RFC8659].

2. Conventions and Definitions

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in
   BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
   capitals, as shown here.

3. Syntax of the "issuemail" Property Tag

   This document defines the "issuemail" Property Tag. The presence of
   one or more "issuemail" Properties in the Relevant Resource Record
   Set (RRSet) [RFC8659] indicates that the domain is requesting that
   Certification Authorities restrict the issuance of certificates that
   certify email addresses.

   The CAA "issuemail" Property Value has the following sub-syntax
   (specified in ABNF as per [RFC5234]):

      issuemail-value = *WSP [issuer-domain-name *WSP]

```
          [";" *WSP [parameters *WSP]]

      issuer-domain-name = label *("." label)
      label = (ALPHA / DIGIT) *( *("-") (ALPHA / DIGIT))

      parameters = (parameter *WSP ";" *WSP parameters) / parameter
      parameter = tag *WSP "=" *WSP value
      tag = (ALPHA / DIGIT) *( *("-") (ALPHA / DIGIT))
      value = *(%x21-3A / %x3C-7E)
```

The production rules for "WSP", "ALPHA", and "DIGIT" are defined in
Appendix B.1 of [RFC5234]. Readers who are familiar with the sub-
syntax of the "issue" and "issuewild" Property Tags will recognize
that this sub-syntax is identical.

The meanings of each production rule within "issuemail-value" are as
follows:

"issuer-domain-name":
   A domain name of the Certification Authority comprised of one or
   more labels

"label":
   A single domain label that consists solely of ASCII letters,
   digits, and the hyphen (known as an "LDH label")

"parameters":
   A semicolon-separated list of parameters

"parameter":
   A tag and a value, separated by an equals sign ("=")

"tag":
   A keyword that identifies the type of parameter

"value":
   The string value for a parameter

4. Processing of the "issuemail" Property Tag

   Prior to issuing a certificate that certifies an email address, the
   Certification Authority MUST check for publication of a Relevant
   RRSet. The discovery of such a Relevant RRSet MUST be performed
   using the algorithm specified in Section 3 of [RFC8659]. The input
   domain to the discovery algorithm SHALL be the domain "part"
   [RFC5322] of the email address that is being certified. If the
   domain "part" of the email address being certified is an
   Internationalized Domain Name [RFC5890] that contains one or more
   U-Labels, then all U-Labels MUST be converted to their A-Label
   representation [RFC5891] for the purpose of discovering the Relevant
   RRSet for that email address.

   If the Relevant RRSet is empty or if it does not contain any
   "issuemail" Properties, then the domain has not requested any
   restrictions on the issuance of certificates for email addresses.
   The presence of other Property Tags, such as "issue" or "issuewild",

does not restrict the issuance of certificates that certify email addresses.

For each "issuemail" Property in the Relevant RRSet, the Certification Authority SHALL compare its issuer-domain-name with the issuer-domain-name as expressed in the Property Value. If there is not any "issuemail" record whose issuer-domain-name (as expressed in the Property Value) matches the Certification Authority's issuer-domain-name, then the Certification Authority MUST NOT issue the certificate. If the Relevant RRSet contains any "issuemail" Property whose issuemail-value does not conform to the ABNF syntax as defined in Section 3 of this document, then those records SHALL be treated as if the issuer-domain-name in the issuemail-value is the empty string.

If the certificate certifies more than one email address, then the Certification Authority MUST perform the above procedure for each email address being certified.

The assignment of issuer-domain-names to Certification Authorities is beyond the scope of this document.

Parameters may be defined by a Certification Authority as a means for domains to further restrict the issuance of certificates. For example, a Certification Authority may define a parameter that contains an account identifier. If the domain elects to add this parameter in an "issuemail" Property, the Certification Authority will verify that the account that is requesting the certificate matches the account specified in the Property and will refuse to issue the certificate if they do not match.

The processing of parameters in the issuemail-value is specific to each Certification Authority and is beyond the scope of this document. In particular, this document does not define any parameters and does not specify any processing rules for when parameters must be acknowledged by a Certification Authority. However, parameters that do not conform to the ABNF syntax as defined in Section 3 will result in the issuemail-value being not conformant with the ABNF syntax. As stated above, a Property whose issuemail-value is malformed SHALL be treated as if the issuer-domain-name in the issuemail-value is the empty string.

5. Examples of the "issuemail" Property Tag

Several illustrative examples of Relevant RRSets and their expected processing semantics follow. All examples assume that the issuer-domain-name for the Certification Authority is "authority.example".

5.1. No "issuemail" Property

The following RRSet does not contain any "issuemail" Properties, so there are no restrictions on the issuance of certificates that certify email addresses for that domain:

```
mail.client.example          CAA 0 issue "authority.example"
mail.client.example          CAA 0 issue "other-authority.example"
```

5.2. Single "issuemail" Property

The following RRSet contains a single "issuemail" Property where the issuer-domain-name is the empty string, so the issuance of certificates certifying email addresses for the domain is prohibited:

```
mail.client.example          CAA 0 issuemail ";"
```

5.3. Single "issuemail" Property with Parameters

The following RRSet contains a single "issuemail" Property where the issuer-domain-name is "authority.example" and contains a single "account" parameter of "123456". In this case, the Certification Authority MAY issue the certificate, or it MAY refuse to issue the certificate, depending on its practices for processing the "account" parameter:

```
mail.client.example
        CAA 0 issuemail "authority.example; account=123456"
```

5.4. Multiple "issuemail" Properties

The following RRSet contains multiple "issuemail" Properties, where one Property matches the issuer-domain-name of the example Certification Authority ("authority.example") and one Property does not match. Although this example is contrived, it demonstrates that since there is at least one record whose issuer-domain-name matches the Certification Authority's issuer-domain-name, issuance is permitted.

```
mail.client.example          CAA 0 issuemail ";"
mail.client.example          CAA 0 issuemail "authority.example"
```

5.5. Malformed "issuemail" Property

The following RRSet contains a single "issuemail" Property whose sub-syntax does not conform to the ABNF as specified in Section 3. Given that "issuemail" Properties with malformed syntax are treated the same as "issuemail" Properties whose issuer-domain-name is the empty string, issuance is prohibited.

```
malformed.client.example     CAA 0 issuemail "%%%%"
```

6. Security Considerations

The security considerations that are expressed in [RFC8659] are relevant to this specification.

The processing of "issuemail" Properties as specified in this document is a supplement to the Certification Authority's validation process. The Certification Authority MUST NOT treat solely the presence of an "issuemail" Property with its issuer-domain-name specified within the Relevant CAA RRSet as sufficient validation of the email address. The Certification Authority MUST validate the email address according to the relevant policy documents and practice statements.

CAA Properties may have the "critical" flag asserted, which specifies that a given Property is critical and must be processed by conforming Certification Authorities. If a Certification Authority does not understand the Property, then it MUST NOT issue the certificate in question.

If a single CAA RRSet is processed by multiple Certification Authorities for the issuance of multiple certificate types, then a Certification Authority's lack of support for a critical CAA Property in the RRSet will prevent the Certification Authority from issuing any certificates for that domain.

For example, assume that an RRSet contains the following Properties:

```
client.example           CAA 128 issue "other-authority.example"
client.example           CAA 0 issuemail "authority.example"
```

In this case, if the Certification Authority whose issuer-domain-name matches "authority.example" does not recognize the "issue" Property Tag, then that Certification Authority will not be able to issue S/MIME certificates that certify email addresses for "client.example".

7. IANA Considerations

IANA has registered the following entry in the "Certification Authority Restriction Properties" subregistry of the "Public Key Infrastructure using X.509 (PKIX) Parameters" registry group:

Tag	Meaning	Reference
issuemail	Authorization Entry by Email Address	RFC 9495

Table 1

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <https://www.rfc-editor.org/info/rfc2119>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
           Specifications: ABNF", STD 68, RFC 5234,
           DOI 10.17487/RFC5234, January 2008,
           <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322,
           DOI 10.17487/RFC5322, October 2008,
           <https://www.rfc-editor.org/info/rfc5322>.

[RFC5891] Klensin, J., "Internationalized Domain Names in
           Applications (IDNA): Protocol", RFC 5891,
           DOI 10.17487/RFC5891, August 2010,
           <https://www.rfc-editor.org/info/rfc5891>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8659] Hallam-Baker, P., Stradling, R., and J. Hoffman-Andrews,
           "DNS Certification Authority Authorization (CAA) Resource
           Record", RFC 8659, DOI 10.17487/RFC8659, November 2019,
           <https://www.rfc-editor.org/info/rfc8659>.

8.2. Informative References

[RFC5890] Klensin, J., "Internationalized Domain Names for
           Applications (IDNA): Definitions and Document Framework",
           RFC 5890, DOI 10.17487/RFC5890, August 2010,
           <https://www.rfc-editor.org/info/rfc5890>.

Acknowledgments

Author's Address

Corey Bonnell
DigiCert, Inc.
Email: corey.bonnell@digicert.com