Workgroup: Network Working Group
Internet-Draft:
draft-ietf-lamps-caa-issuemail-00
Published: 10 February 2023
Intended Status: Standards Track
Expires: 14 August 2023
Authors: C. Bonnell
DigiCert, Inc.

Certification Authority Authorization (CAA) Processing for Email Addresses

Abstract

The Certification Authority Authorization (CAA) DNS resource record type provides a mechanism for domains to express the allowed set of Certification Authorities that may issue certificates for the domain. The core CAA specification ([RFC8659]) solely defines Property Tags that restrict the issuance of certificates that certify domain names; it does not define a mechanism for domains to restrict the issuance of certificates that include email addresses. This specification defines a Property Tag that grants authorization to Certification Authorities to issue certificates which certify email addresses.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://CBonnell.github.io/caa-issuemail/draft-ietf-lamps-caa-issuemail.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lamps-caa-issuemail/.

Discussion of this document takes place on the Limited Additional Mechanisms for PKIX and SMIME (lamps) Working Group mailing list (mailto:spasm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spasm/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://github.com/CBonnell/caa-issuemail.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines a CAA Property Tag which restricts the allowed set of issuers for electronic 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 ([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)
```

Readers who are familiar with the sub-syntax of the "issue" and "issuewild" Property Tags will recognize that this sub-syntax is identical.

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 Resource Record Set (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 the Relevant RRSet 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 which 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 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.

The processing of parameters in the issuemail-value are beyond the scope of this document.

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 "ca.example.com".

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

```
mail.example.com         CAA 0 issue "ca1.example.net"
mail.example.com         CAA 0 issue "ca2.example.org"
```

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.example.com         CAA 0 issuemail ";"
```

The following RRSet contains multiple "issuemail" Properties, one of which matches the issuer-domain-name of the example Certification Authority ("ca.example.com") and one Property which does not match.

Given that there is at least one record whose issuer-domain-name matches the Certification Authority's issuer-domain-name, issuance is permitted.

```
mail.example.com         CAA 0 issuemail ";"
mail.example.com         CAA 0 issuemail "ca.example.com"
```

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.example.com     CAA 0 issuemail "%%%%%"
```

6. Security Considerations

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

CAA Properties may have the "critical" flag asserted, which specifies that the 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:

```
example.com         CAA 128 issue "ca2.example.com"
example.com         CAA 0 issuemail "ca.example.com"
```

In this case, if the Certification Authority whose issuer-domain-name matches "ca.example.com" 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 "example.com".

7. IANA Considerations

The author(s) request the registration of the following "Certification Authority Restriction Properties":

Tag	Meaning	Reference
issuemail	Authorization Entry by Email Address	[This document]

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/rfc/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/rfc/rfc5234>.

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

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/rfc5890>.

Acknowledgments

TODO acknowledge.

Author's Address

Corey Bonnell
DigiCert, Inc.

Email: corey.bonnell@digicert.com