Stream: Internet Engineering Task Force (IETF)
RFC: 9538
Category: Standards Track
Published: February 2024
ISSN: 2070-1721
Authors: F. Fieau, Ed. *Orange* E. Stephan *Orange* S. Mishra *Verizon*

RFC 9538
Content Delivery Network Interconnection (CDNI) Delegation Using the Automated Certificate Management Environment

Abstract

This document defines metadata to support delegating the delivery of HTTPS content between two or more interconnected Content Delivery Networks (CDNs). Specifically, this document defines a Content Delivery Network Interconnection (CDNI) Metadata interface object to enable delegation of X.509 certificates leveraging delegation schemes defined in RFC 9115. Per RFC 9115, delegating entities can remain in full control of the delegation and can revoke it at any time. This avoids the need to share private cryptographic key material between the involved entities.

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/rfc9538.

Copyright Notice

Table of Contents

1. Introduction

Content delivery over HTTPS using two or more cooperating CDNs along the path requires credential management, specifically when DNS-based redirection is used. In such cases, an upstream CDN (uCDN) needs to delegate its credentials to a downstream CDN (dCDN) for content delivery.

[RFC9115] defines delegation methods that allow a uCDN on behalf of the content provider, the holder of the domain, to generate on-demand an X.509 certificate that binds the designated domain name with a key pair owned by the dCDN. For further details, please refer to Sections 1 and 5.1.2.1 of [RFC9115].

This document defines CDNI Metadata to make use of HTTPS delegation between a uCDN and a dCDN based on the mechanism specified in [RFC9115]. Furthermore, it adds a delegation method to the "CDNI Payload Types" IANA registry.

Section 2 presents delegation metadata for the Footprint & Capabilities Advertisement interface (FCI). Section 3 addresses the metadata for handling HTTPS delegation with the Metadata interface.

1.1. Terminology

This document uses terminology from CDNI framework documents such as: CDNI framework document [RFC7336] and CDNI interface specifications documents: CDNI Metadata interface [RFC8006] and CDNI Footprint and Capabilities Advertisement interface [RFC8008]. It also uses terminology from Section 1.2 of [RFC8739] and Section 1.1 of [RFC9115], including Short-Term, Automatically Renewed (STAR), as applied to X.509 certificates.

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.

2. Advertising Delegation Metadata for CDNI through FCI

The Footprint & Capabilities Advertisement interface (FCI) defined in [RFC8008] allows a dCDN to send a FCI capability type object to a uCDN.

This document uses the CDNI Metadata capability object serialization from [RFC8008] for a CDN that supports delegation methods.

The following is an example of the supported delegated methods capability object for a dCDN implementing the ACME delegation method.

```
{
  "capabilities": [
    {
      "capability-type": "FCI.Metadata",
      "capability-value": {
        "metadata": [
          // list of supported delegation methods
          "ACMEDelegationMethod"
        ]
      },
      "footprints": [
        "Footprint objects"
      ]
    }
  ]
}
```

3. ACME Delegation Metadata for CDNI

When a uCDN delegates the delivery of HTTPS traffic to a dCDN using DNS redirection [RFC7336], the dCDN must use a certificate bound to the origin's name to successfully authenticate to the end-user (see also Section 5.1.2.1 of [RFC9115]).

To that end, this section defines the AcmeDelegationMethod object, which describes metadata for using the ACME delegation interface [RFC9115].

The ACMEDelegationMethod applies to both ACME STAR delegation, which provides a delegation model based on short-term certificates with automatic renewal (Section 2.3.2 of [RFC9115]), and non-STAR delegation, which allows delegation between CDNs using long-term certificates (Section 2.3.3 of [RFC9115]).

Figure 1 provides a high-level view of the combined CDNI and ACME delegation message flows to obtain a STAR certificate from the Certification Authority (CA) bound to the Content Provider's (CP) name.

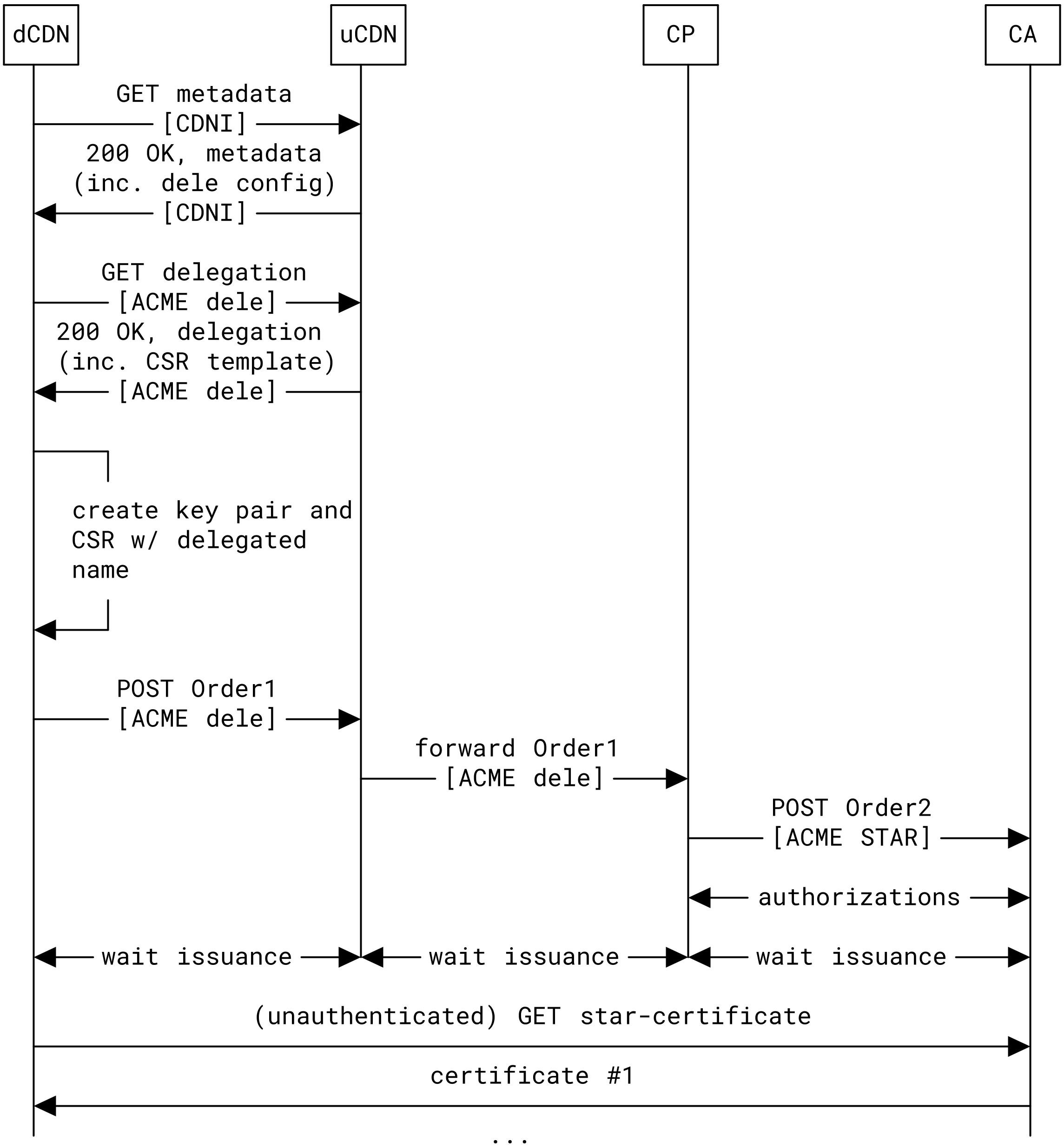

Figure 1: Example Call Flow of STAR Delegation in CDNI Showing Two Levels of Delegation

> Note: The delegation object defined in Section 2.3.1.3 of [RFC9115] only allows DNS mappings to be specified using CNAME RRs. A future document updating [RFC9115] could expand the delegation object to also include SVCB/HTTPS-based mappings [RFC9460].

Section 3.1 defines the objects used for bootstrapping the ACME delegation method between a uCDN and a delegate dCDN.

3.1. ACMEDelegationMethod Object

The ACMEDelegationMethod object allows a uCDN to define both STAR and non-STAR delegations. The dCDN, the consumer of the delegation, can determine the type of delegation by the presence (or absence) of the "lifetime" property. That is, the presence of the "lifetime" property explicitly means a short-term delegation with lifetime of the certificate based on that property (and the optional "lifetime-adjust" attribute). A non-STAR delegation will not have the "lifetime" property in the delegation. See also the examples in Section 3.1.1.

The ACMEDelegationMethod object is defined with the properties shown below.

- Property: acme-delegation
  - Description: A URL pointing at an ACME delegation object, either STAR or non-STAR, associated with the dCDN account on the uCDN ACME server (see Section 2.3.1.3 of [RFC9115] for the details). The URL **MUST** use the https scheme.
  - Type: String
  - Mandatory-to-Specify: Yes
- Property: time-window
  - Description: Validity period of the certificate. According to Section 4.3.4 of [RFC8006], a TimeWindow object is defined by a window "start" time and a window "end" time. In the case of a STAR method, the "start" and "end" properties of the window **MUST** be understood respectively as the start-date and end-date of the certificate validity. In the case of a non-STAR method, the "start" and "end" properties of the window **MUST** be understood, respectively, as the notBefore and notAfter fields of the certificate.
  - Type: TimeWindow
  - Mandatory-to-Specify: Yes
- Property: lifetime
  - Description: See lifetime in Section 3.1.1 of [RFC8739]
  - Type: Integer
  - Mandatory-to-Specify: Yes, only if a STAR delegation method is specified
- Property: lifetime-adjust
  - Description: See lifetime-adjust in Section 3.1.1 of [RFC8739]
  - Type: Integer
  - Mandatory-to-Specify: No

3.1.1. Examples

The following example shows an `ACMEDelegationMethod` object for a STAR-based ACME delegation.

```
{
  "generic-metadata-type": "MI.ACMEDelegationMethod",
  "generic-metadata-value": {
    "acme-delegation": "https://acme.ucdn.example/delegation/ogfr",
    "time-window": {
      "start": 1665417434,
      "end": 1665676634
    },
    "lifetime": 345600,
    "lifetime-adjust": 259200
  }
}
```

The example below shows an `ACMEDelegationMethod` object for a non-STAR ACME delegation. The delegation object is defined as per Section 4.3 of [RFC8006].

```
{
  "generic-metadata-type": "MI.ACMEDelegationMethod",
  "generic-metadata-value": {
    "acme-delegation": "https://acme.ucdn.example/delegation/wSi5",
    "time-window": {
      "start": 1570982234,
      "end": 1665417434
    }
  }
}
```

4. IANA Considerations

Per this document, the following type has been registered in the "CDNI Payload Types" registry:

Payload Type	Reference
MI.ACMEDelegationMethod	RFC 9538

Table 1

4.1. CDNI MI ACMEDelegationMethod Payload Type

Purpose: The purpose of this Payload Type is to distinguish AcmeDelegationMethod MI objects (and any associated capability advertisement)

Interface: MI/FCI

Encoding: See Section 3.1

5. Security Considerations

The metadata object defined in this document does not introduce any new security or privacy concerns over those already discussed in [RFC9115], [RFC8006], and [RFC8008].

The reader is expected to understand the ACME delegation trust model (Section 7.1 of [RFC9115]) and security goal (Section 7.2 of [RFC9115]). In particular, the reader is expected to understand that it is critical to protect the user account associated with the delegation; this account authorizes all the security-relevant operations between a dCDN and a uCDN over the ACME channel. The dCDN's ACME account is also relevant to the privacy of the entire scheme; for example, the `acme-delegation` resource in the Metadata object is only accessible to the holder of the account key, who is allowed to fetch its content exclusively via POST-as-GET (Section 2.3.1.2 of [RFC9115]).

In addition, the Metadata interface authentication and confidentiality requirements defined in Section 8 of [RFC8006] **MUST** be followed.

Implementers **MUST** adhere to the security considerations defined in Section 7 of [RFC8008], "Content Delivery Network Interconnection (CDNI) Request Routing: Footprint and Capabilities Semantics".

When TLS is used to achieve the above security objectives, the general TLS usage guidance in [RFC9325] **MUST** be followed.

6. References

6.1. 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>.

[RFC8006] Niven-Jenkins, B., Murray, R., Caulfield, M., and K. Ma, "Content Delivery Network Interconnection (CDNI) Metadata", RFC 8006, DOI 10.17487/RFC8006, December 2016, <https://www.rfc-editor.org/info/rfc8006>.

[RFC8008] Seedorf, J., Peterson, J., Previdi, S., van Brandenburg, R., and K. Ma, "Content Delivery Network Interconnection (CDNI) Request Routing: Footprint and Capabilities Semantics", RFC 8008, DOI 10.17487/RFC8008, December 2016, <https://www.rfc-editor.org/info/rfc8008>.

[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>.

[RFC8739] Sheffer, Y., Lopez, D., Gonzalez de Dios, O., Pastor Perales, A., and T. Fossati, "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)", RFC 8739, DOI 10.17487/RFC8739, March 2020, <https://www.rfc-editor.org/info/rfc8739>.

[RFC9115] Sheffer, Y., López, D., Pastor Perales, A., and T. Fossati, "An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates", RFC 9115, DOI 10.17487/RFC9115, September 2021, <https://www.rfc-editor.org/info/rfc9115>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

6.2. Informative References

[RFC7336] Peterson, L., Davie, B., and R. van Brandenburg, Ed., "Framework for Content Distribution Network Interconnection (CDNI)", RFC 7336, DOI 10.17487/RFC7336, August 2014, <https://www.rfc-editor.org/info/rfc7336>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

Acknowledgments

We would like to thank authors of the [RFC9115], Antonio Augustín Pastor Perales, Diego López, Thomas Fossati, and Yaron Sheffer. Additionally, our gratitude to Thomas Fossati who participated in the drafting, reviewing, and giving his feedback in finalizing this document. We also thank CDNI co-chair Kevin Ma for his continual review and feedback during the development of this document.

Authors' Addresses

Frédéric Fieau (EDITOR)
Orange
40-48, avenue de la République
92320 Châtillon
France
Email: frederic.fieau@orange.com

Emile Stephan
Orange
2, avenue Pierre Marzin
22300 Lannion
France
Email: emile.stephan@orange.com

Sanjay Mishra
Verizon
13100 Columbia Pike
Silver Spring, MD 20904
United States of America
Email: sanjay.mishra@verizon.com