Workgroup:
Content Delivery Networks Interconnection
Internet-Draft:
draft-ietf-cdni-interfaces-https-delegation-13
Published: 14 December 2022
Intended Status: Standards Track
Expires: 17 June 2023

Authors: F. Fieau, Ed. E. Stephan S. Mishra
Orange Orange Verizon

CDNI extensions for HTTPS delegation

Abstract

This document defines metadata objects to support delegating the delivery of HTTPS content between two or more interconnected CDNs. Specifically, this document defines CDNI Metadata interface objects to enable delegation of X.509 certificates leveraging delegation schemes defined in RFC9115. RFC 9115 allows delegating entities to remain in full control of the delegation and be able to revoke it any time and avoids the need to share private cryptographic key material between the involved entities.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-cdni-interfaces-https-delegation/.

Discussion of this document takes place on the Content Delivery Networks Interconnection Working Group mailing list (mailto:cdni@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/cdni/. Subscribe at https://www.ietf.org/mailman/listinfo/cdni/.

Source for this draft and an issue tracker can be found at https://github.com/FredericFi/cdni-wg.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Content delivery over HTTPS using two or more cooperating Content Delivery Networks (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 (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 Section 1 of [RFC9115] and Section 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 1.1 defines terminology used in this document. Section 2 presents delegation metadata for the FCI interface. Section 3 addresses the metadata for handling HTTPS delegation with the Metadata Interface. Section 4 addresses IANA registry for delegation methods. Section 5 covers the security considerations.

1.1. Terminology

This document uses terminology from CDNI framework documents such as: CDNI framework document [RFC7336], CDNI requirements [RFC7337] and CDNI interface specifications documents: CDNI Metadata interface [RFC8006] and CDNI Footprint and capabilities [RFC8008]. It also uses terminology from Section 1.1 of [RFC8739].

2. Advertising Delegation Metadata for CDNI through FCI

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

The FCI.Metadata object allows a dCDN to advertise the capabilities regarding the supported delegation methods and their configuration.

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": [
          "ACMEDelegationMethod",
          "... Other supported delegation methods ..."
        ]
      },
      "footprints": [
        "Footprint objects"
      ]
    }
  ]
}
```

3. ACME Delegation Metadata for CDNI

When a uCDN delegates to a dCDN to deliver HTTPS traffic using DNS Redirection [RFC7975], 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 STAR certificate bound to the origin's name.

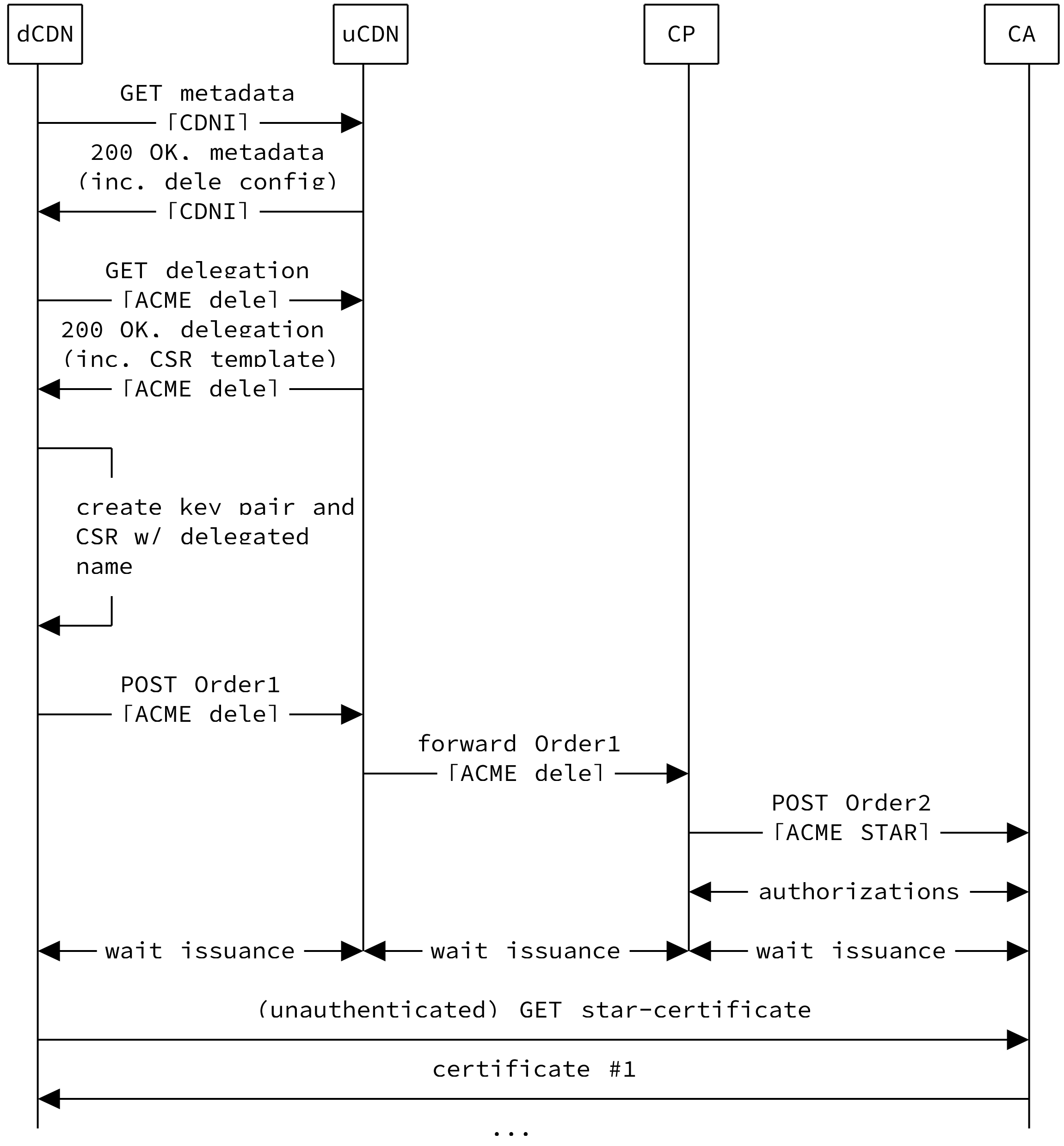

Figure 1: Example call-flow of STAR delegation in CDNI showing 2 levels of delegation

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 both define STAR and non-STAR delegation depending on the delegation certificate validity. The ACMEDelegationMethod object is defined with several 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 of [RFC9115] for the details).

-Type: Link object, according to Section 4.3.1 of [RFC8006]

-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 of the window. In case of 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 Epoch time format. In the case of the 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 Section 3.1.1 of [RFC8739]

-Type: Time, see Section 4.3.4 of [RFC8006]

-Mandatory-to-Specify: Yes, only if a STAR delegation method is specified

*Property: lifetime-adjust

-Description: See Section 3.1.1 of [RFC8739]

-Type: Time

-Mandatory-to-Specify: Yes, only if a STAR delegation method is specified

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

This document requests the registration of the following entry under the "CDNI Payload Types" registry:

Payload Type	Specification
MI.ACMEDelegationMethod	RFCthis

Table 1

RFC Editor: please replace RFCthis with the RFC number of this RFC and remove this note.

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

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 7.3 of [RFC9115]), in particular the criticality around the protection of the user account associated with the delegation.

In addition, the requirements defined by CDNI Metadata and CDNI Footprint and Capabilities regarding the integrity, (mutual) authentication and confidentiality of the communication channel used to transport the metadata object apply.

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

[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/rfc/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/rfc/rfc8008>.

[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/rfc/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/rfc/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/rfc/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/rfc/rfc7336>.

[RFC7337] Leung, K., Ed. and Y. Lee, Ed., "Content Distribution Network Interconnection (CDNI) Requirements", RFC 7337, DOI 10.17487/RFC7337, August 2014, <https://www.rfc-editor.org/rfc/rfc7337>.

[RFC7975] Niven-Jenkins, B., Ed. and R. van Brandenburg, Ed., "Request Routing Redirection Interface for Content Delivery Network (CDN) Interconnection", RFC 7975, DOI 10.17487/RFC7975, October 2016, <https://www.rfc-editor.org/rfc/rfc7975>.

Acknowledgments

We would like to thank authors of the [RFC9115], Antonio Augustin Pastor Perales, Diego Lopez, 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 Republique
92320 Chatillon
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