Workgroup: CDNI Working Group
Internet-Draft:
draft-ietf-cdni-interfaces-https-delegation-09
Published: 11 July 2022
Intended Status: Standards Track
Expires: 12 January 2023
Authors: F. Fieau, Ed. Orange
E. Stephan Orange
S. Mishra Verizon

CDNI extensions for HTTPS delegation

Abstract

This document defines a new Footprint and Capabilities metadata objects to support HTTPS delegation between two or more interconnected CDNs. Specifically, this document outlines CDNI Metadata interface objects for delegation method as published in the ACME-STAR document [RFC9115].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 12 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Content delivery over HTTPS using one or more CDNs along the path requires credential management. This specifically applies when an entity delegates delivery of encrypted content to another trusted entity.

[RFC9115] defines a mechanism where an upstream entity, that is, holder of a X.509 certificate can give a temporary delegated authority, via issuing a certificate to one or more downstream entities for the purposes of delivering content on its behalf. Furthermore, the upstream entity has the ability to extend the duration of the certificate automatically and iteratively until it allows the last renewal to end and therefore terminate the use of certificate authority to the downstream entity.

More specifically, [RFC9115] defines a process where the upstream Content Delivery Network (uCDN), the holder of the domain, generates on-demand a X.509 certificate for the downstream CDN (dCDN). The certificate generation process ensures that the certified public key corresponds to a private key controlled by the downstream CDN. [RFC9115] follows [RFC8739] for Short-Term, Automatically Renewed Certificate (STAR) in the Automated Certificate Management Environment (ACME).

This document defines CDNI Metadata to make use of HTTPS delegation between an upstream CDN (uCDN) and a downstream CDN (dCDN) based on mechanism specified in [RFC9115]. Furthermore, it includes a proposal of IANA registry to enable adding of delegation methods.

Section 2 defines terminology used in this document. Section 3 presents delegation metadata for the FCI interface. Section 4 addresses the metadata for handling HTTPS delegation with the Metadata Interface. Section 5 addresses IANA registry for delegation methods. Section 6 covers the security considerations.

2. 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].

3. Delegation metadata for CDNI FCI

The Footprint and Capabilities interface as defined in [RFC8008], allows a dCDN to send a FCI capability type object to a uCDN. This draft adds an object named FCI.SupportedDelegationMethods.

This object shall allow 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 CDN supporting STAR delegation method.

```
{
"capabilities": [
  {
    "capability-type": "FCI.SupportedDelegationMethods",
    "capability-value": {
      "delegation-methods": [
               "AcmeStarDelegationDelegationMethod",
               "... Other supported delegation methods ..."
      ]
    }
    "footprints": [
      <Footprint objects>
    ]
  }
 ]
}
```

4. Delegation metadata for CDNI

This section defines Delegation metadata using the current Metadata interface model. This allows bootstrapping delegation methods between a uCDN and a delegate dCDN.

4.1. Usage example related to an HostMatch object

This section presents the use of CDNI Delegation metadata to apply to an HostMatch object, as defined in [RFC8006] and as specified in the following sections.

The existence of delegation method in the CDNI metadata Object shall enable the use of this method, as chosen by the delegating entity. In the case of an HostMatch object, the delegation method will be activated for the set of Host defined in the HostMatch. See Section 4.2 for more details about delegation methods metadata specification.

The HostMatch object can reference a host metadata that points at the delegation information. Delegation metadata are added to a Metadata object.

Those "delegation" metadata can apply to other MI objects such as PathMatch object metadata.

Below shows both HostMatch and its Metadata related to a host, for example, here is a HostMatch object referencing "video.example.com":

```
HostMatch:
   {
     "host": "video.example.com",
     "host-metadata": {
       "type": "MI.HostMetadata",
       "href": "https://metadata.ucdn.example/host1234"
     }
   }
```

Following the example above, the metadata is modeled for ACMEStarDelegationMethod as follows:

```
  "generic-metadata-value": {
    "acme-delegations": [
      "https://acme.ucdn.example/acme/delegation/ogfr8EcolOT",
      "https://acme.ucdn.example/acme/delegation/wSi5Lbb61E4"
    ]
  }
```

4.2. AcmeStarDelegationMethod object

This section defines the AcmeStarDelegationMethod object which describes metadata related to the use of ACME/STAR API presented in [RFC9115]

As expressed in [RFC9115], when an origin has set a delegation to a specific domain (i.e. dCDN), the dCDN should present to the end-user client, a short-term certificate bound to the master certificate.

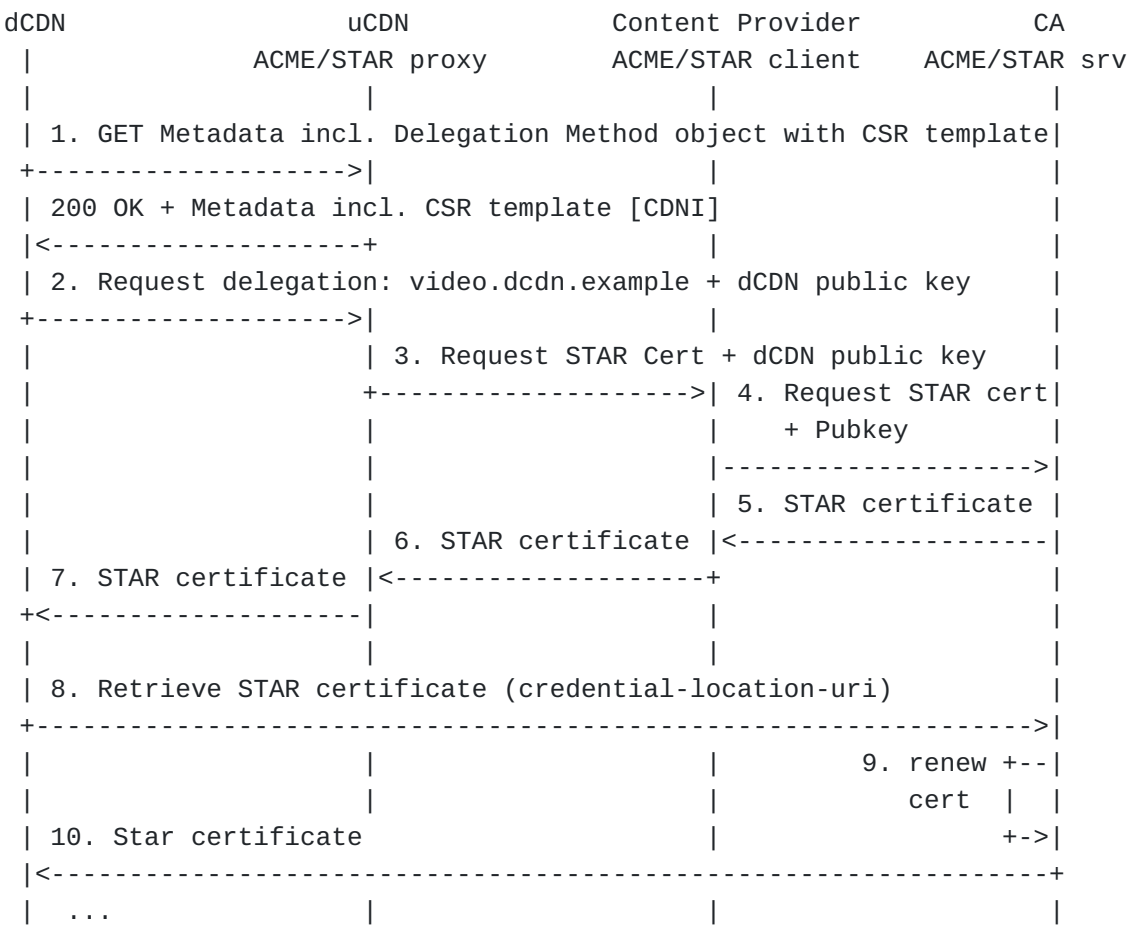

Figure 1: Example call-flow of STAR delegation in CDNI showing 2 levels of delegation

Property: acme-delegations

Description: an array of delegation objects associated with the dCDN account on the uCDN ACME server (see Section 2.3.1 of [RFC9115] for the details).

Type: Objects

Mandatory-to-Specify: Yes

5. IANA considerations

This document requests the registration of the following entries under the "CDNI Payload Types" registry hosted by IANA regarding "CDNI delegation":

Payload Type	Specification
MI.AcmeStarDelegationMethod	RFCthis
FCI.SupportedDelegationMethods	RFCthis

[RFC Editor: Please replace RFCthis with the published RFC number for this document.]

5.1. CDNI MI AcmeStarDelegationMethod Payload Type

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

Interface: MI

Encoding: see Section 5

5.2. CDNI FCI SupportedDelegationMethods Payload Type

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

Interface: FCI

Encoding: see Section 4

6. Security considerations

Delegation metadata proposed here do not alter nor change Security Considerations as outlined in the following RFCs: An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates [RFC9115]; the CDNI Metadata [RFC8006] and CDNI Footprint and Capabilities [RFC8008].

7. References

7.1. 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/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>.

[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>.

7.2. 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>.

[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/info/rfc7337>.

Authors' Addresses

Frederic 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