

Workgroup: CDNI Working Group  
Internet-Draft:  
draft-ietf-cdni-interfaces-https-delegation-06  
Published: 10 September 2021  
Intended Status: Standards Track  
Expires: 14 March 2022  
Authors: F.F. Fieau, Ed.    E.S. Stephan    S.M. Mishra  
          Orange                    Orange            Verizon  
                                  **CDNI extensions for HTTPS delegation**

## Abstract

The delivery of content over HTTPS involving multiple CDNs raises credential management issues. This document proposes extensions in CDNI Control and Metadata interfaces to setup HTTPS delegation from an Upstream CDN (uCDN) to a Downstream CDN (dCDN).

## 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 14 March 2022.

## Copyright Notice

Copyright (c) 2021 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

- [1. Introduction](#)
- [2. Terminology](#)
- [3. Known delegation methods](#)
- [4. Extension to CDNI FCI](#)
- [5. Extending the CDNI metadata model](#)
  - [5.1. Extension to HostMetadata object](#)
  - [5.2. Extension to PathMetadata object](#)
- [6. AcmeStarDelegationMethod object](#)
- [7. Metadata Simple Data Type Descriptions](#)
  - [7.1. Periodicity](#)
- [8. IANA considerations](#)
  - [8.1. CDNI MI AcmeStarDelegationMethod Payload Type](#)
- [9. Security considerations](#)
- [10. Comments and questions](#)
- [11. References](#)
  - [11.1. Normative References](#)
  - [11.2. Informative References](#)
- [Authors' Addresses](#)

## 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.

Several delegation methods are currently proposed within different IETF working groups. They specify different methods for provisioning HTTPS delivery credentials.

This document extends the CDNI Metadata interface to setup HTTPS delegation between an upstream CDN (uCDN) and downstream CDN (dCDN) using the Standardized delegation methods. Furthermore, it includes a proposal of IANA registry to enable adding of new methods.

Section 2 is about terminology used in this document. Section 3 presents delegation methods specified at the IETF. Section 4 addresses the extension for handling HTTPS delegation in CDNI. Section 5 describes simple data types. Section 6 addresses IANA registry for delegation methods. Section 7 covers the security issues. Section 8 is about comments and questions.

## 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 Control interface / Triggers [[RFC8007](#)].

### 3. Known delegation methods

There are currently Internet drafts within the TLS and ACME working groups adopted to handle delegation of HTTPS delivery between entities.

This Internet Draft (I-D) proposes standardizing HTTPS delegation between the CDN entities using CDNI interfaces.

This document only considers the Short-term, Automatically-Renewed (STAR) certificates in Automated Certificate Management Environment(ACME) [[RFC8739](#)]

This document allows the extension to other delegation methods. Those methods can easily be extended to any further methods in the future.

### 4. Extension to CDNI FCI

In order for CDNs to negotiate on which methods are supported, the Footprint and Capabilities interface as defined in RFC8008, allows a uCDN to send a FCI capability type objects, named FCI.SupportedDelegationMethods, to dCDN.

The following example shows an exemple of the supported delegated methods capability object serialization for a CDN that supports STAR delegation method.

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

## 5. Extending the CDNI metadata model

This section defines a CDNI extension to the current Metadata interface model that allows bootstrapping delegation methods between a uCDN and a delegate dCDN.

### 5.1. Extension to HostMetadata object

This extension reuses HostMetadata object, as defined in [[RFC8006](#)], and adds new "Delegation methods" objects as specified in the following sections.

The existence of the delegation methods in a HostMetadata Object shall enable the use of one of this methods, chosen by the delegating entity. The delegation method will be activated for the set of Host defined in the HostMatch. See [Section 6](#) for more details about delegation methods metadata specification.

Example:

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

Below shows both HostMatch and HostMetadata objects 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 HostMetadata can be modeled for ACMEStarDelegationMethod as:

```
{
  "hostmetadata": [
    {
      "generic-metadata-type": "MI.AcmeStarDelegationMethod",
      "generic-metadata-value": {
        "star-proxy": "10.2.2.2",
        "acme-server" : "10.2.3.3",
        "credentials-location-uri": "www.ucdn.com/credentials",
        "periodicity": 36000,
        "CSR-template": Json/Text of the CSR template (see 4.2)
      }
    }
  ]
}
```

This extension allows to explicitly indicate support for a given method. Therefore, the presence (or lack thereof) of an AcmeStarDelegationMethod, and/or further delegation methods, implies support (or lack thereof) for the given method.

## 5.2. Extension to PathMetadata object

This extension reuses PathMetadata object, as defined in [\[RFC8006\]](#), and adds new "Delegation methods" objects as specified in the following sections.

This allows to explicitly indicate support for a given method. Therefore, the presence (or lack thereof) of an AcmeStarDelegationMethod, and/or further delegation methods, implies support (or lack thereof) for the given method.

Example:

The PathMatch object can reference a path-metadata that points at the delegation information. Delegation metadata are added to PathMetaData object.

Below shows both PathMatch and PathMetadata objects related to a path, for example, here /movies/\* located at https://metadata.ucdn.example/video.example.com/movies

PathMatch:

```
{
  "path-pattern": {
    "pattern": "/movies/*",
    "case-sensitive": true
  },
  "path-metadata": {
    "type": "MI.PathMetadata",
    "href": "https://metadata.ucdn.example/video.example.com/movies"
  }
}
```

Following the example above, the PathMetadata can be modeled for ACMEStarDelegationMethod as:

```
{
  PathMetadata:
  {
    "metadata": [
      {
        "generic-metadata-type": "MI.AcmeStarDelegationMethod",
        "generic-metadata-value": {
          "star-proxy": "10.2.2.2",
          "acme-server" : "10.2.3.3",
          "credentials-location-uri": "www.ucdn.com/credentials",
          "periodicity": 36000,
          "CSR-template": "Json/Text of the CSR template (see section 4.2)"
        }
      }
    ]
  }
}
```

The existence of the "MI.AcmeStarDelegationMethod" object in a PathMetadata Object shall enable the use of one of the AcmeStarDelegation Methods, chosen by the delegating entity. The delegation method will be activated for the set of Path defined in the PathMatch. See [Section 6](#) for more details about delegation methods metadata specification.

## 6. AcmeStarDelegationMethod object

This section defines the AcmeStarDelegationMethod object which describes metadata related to the use of ACME/STAR API presented in [\[RFC8739\]](#)

As expressed in [\[RFC8739\]](#), 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.

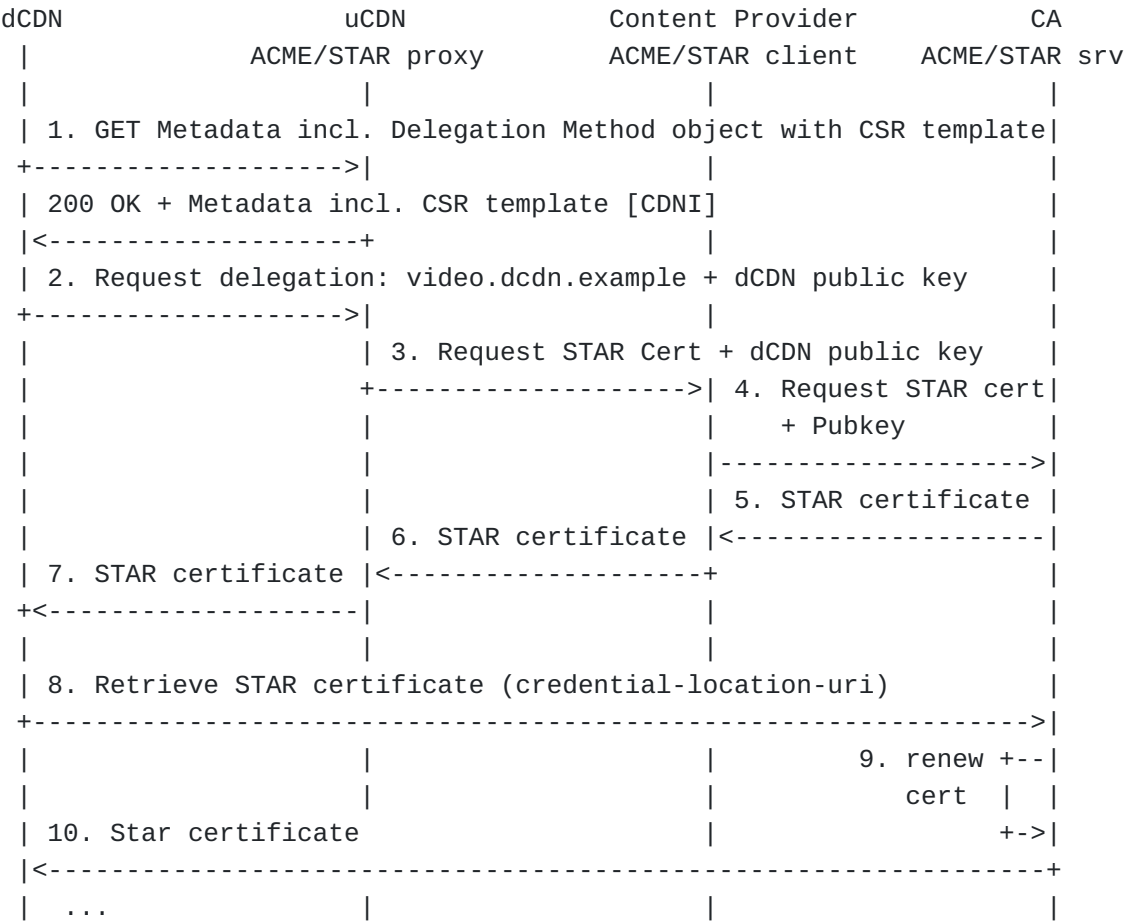


Figure 1: Example call-flow of STAR delegation in CDNI showing 2 levels of delegation

Property: star-proxy

Description: Used to advertise the STAR Proxy to the dCDN.  
Endpoint type defined in RFC8006, Section 4.3.3.

Type: Endpoint

Mandatory-to-Specify: Yes

Property: acme-server

Description: used to advertise the ACME server to the dCDN.  
Endpoint type is defined in RFC8006, Section 4.3.3.

Type: Endpoint

Mandatory-to-Specify: Yes

Property: credentials-location-uri

Description: expresses the location of the credentials to be fetched by the dCDN. Link type is as defined in RFC8006, Section 4.3.1.

Type: Link

Mandatory-to-Specify: Yes

Property: periodicity

Description: expresses the credentials renewal periodicity. See [Section 7.1](#).

Type: Periodicity

Mandatory-to-Specify: Yes

Property: CSR-template

Description: The CSR template must be included in the metadata when dealing with AcmeStarDelegation Methods. It shall follow the description in [[RFC8739](#)] section 3. It should be included in JSON/text format.

Type: JSON

Mandatory-to-Specify: Yes

## **7. Metadata Simple Data Type Descriptions**

This section describes the simple data types that are used for properties for objects in this document.

### **7.1. Periodicity**

A time value expressed in seconds to indicate a periodicity.

Type: Integer

## **8. 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
-----+-----		-----+-----

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

### 8.1. 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/FCI

Encoding: see Section 4.2.1

## 9. Security considerations

Extensions proposed here do not alter nor change Security Considerations as outlined in the CDNI Metadata and Footprint and Capabilities RFCs [[RFC8006](#)].

## 10. Comments and questions

Should dCDN be visible from the Content Provider or not? This would lead to different solutions to handle delegation towards the CP. In most cases, the dCDNs should never be visible to the CP, in order to reduce the burden of certificates generation for dCDN.

## 11. References

### 11.1. 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>>.
- [RFC8007] Murray, R. and B. Niven-Jenkins, "Content Delivery Network Interconnection (CDNI) Control Interface /

Triggers", RFC 8007, DOI 10.17487/RFC8007, December 2016, <<https://www.rfc-editor.org/info/rfc8007>>.

[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>>.

## 11.2. 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](mailto:frederic.fieau@orange.com)

Emile Stephan  
Orange  
2, avenue Pierre Marzin  
22300 Lannion  
France

Email: [emile.stephan@orange.com](mailto:emile.stephan@orange.com)

Sanjay Mishra  
Verizon  
13100 Columbia Pike  
Silver Spring, MD 20904  
United States of America

Email: [sanjay.mishra@verizon.com](mailto:sanjay.mishra@verizon.com)