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

CDNI extensions for HTTPS delegation

Abstract

   The delivery of content over HTTPS involving one or more CDNs raises
   credential management issues. This document defines new CDNI FCI and
   Metadata objects to support HTTPS delegation, especially the ACME-
   STAR [RFC9115] method.

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 8 September 2022.

Copyright Notice

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.

The ACME WG has published ACME STAR [RFC9115] allowing a dCDN to
request a x.509 certificate from uCDN.

This document proposes the CDNI Metadata interface to setup HTTPS
delegation between an upstream CDN (uCDN) and downstream CDN (dCDN)
using the ACME STAR proposal. 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. 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 will 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 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 of an
HostMatch object, as defined in [RFC8006] as specified in the
following sections.

The existence of the delegation methods in metadata in a CDNI Object
shall enable the use of one of this methods, 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.

Below shows both HostMatch 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 can be modeled
for ACMEStarDelegationMethod as:

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

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.

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

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.

```
dCDN                   uCDN           Content Provider          CA
            ACME/STAR proxy         ACME/STAR client      ACME/STAR srv
  |                     |                     |                    |
  | 1. GET Metadata incl. Delegation Method object with CSR template|
  +-------------------->|                     |                    |
  | 200 OK + Metadata incl. CSR template [CDNI]                    |
  |<-------------------+                      |                    |
  | 2. Request delegation: video.dcdn.example + dCDN public key    |
  +-------------------->|                     |                    |
  |                     | 3. Request STAR Cert + dCDN public key   |
  |                     +-------------------->| 4. Request STAR cert|
  |                     |                     |      + Pubkey       |
  |                     |                     |-------------------->|
  |                     |                     | 5. STAR certificate |
  |                     | 6. STAR certificate |<-------------------|
  | 7. STAR certificate |<-------------------+                     |
  +<-------------------|                      |                    |
  |                     |                     |                    |
  | 8. Retrieve STAR certificate (credential-location-uri)         |
  +-------------------------------------------------------------->|
  |                     |                     |      9. renew +--|
  |                     |                     |         cert  |  |
  | 10. Star certificate                      |             +->|
  |<-------------------------------------------------------------+
  |  ...                |                     |                    |
```
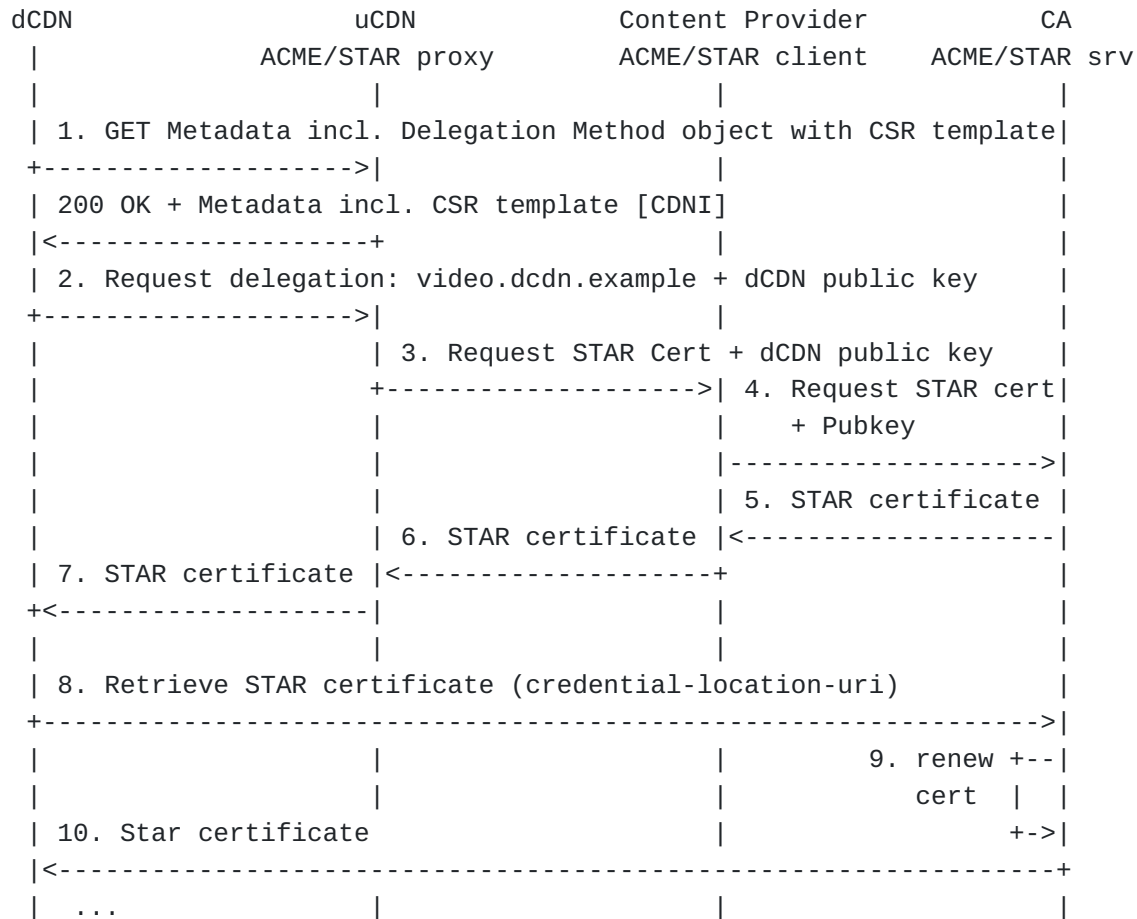
Figure 1: Example call-flow of STAR delegation in CDNI showing 2 levels
of delegation

   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

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

However there are still some security questions that should be
addressed such as: Are there concerns about using this incorrectly
or limitations on how this can safely be used?

7. Privacy considerations

Some privacy questions are still pending: Are there any concerns
with sharing the information that is in the metadata? Is the
metadata safe to redistribute, or is it something that is only valid
between adjacent CDNs?

8. References

8.1. 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>.

[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>.

8.2. 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