CDNI extensions for HTTPS delegation
draft-fieau-cdni-interfaces-https-delegation-05

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

Copyright Notice

the Trust Legal Provisions and are provided without warranty as
described in the Simplified 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.

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).
Furthermore, it includes a proposal of IANA registry to enable the
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 is about an IANA
registry for delegation methods. Section 7 raises the security
issues.

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

   This I-D proposes standardizing HTTPS delegation between the entities
   using CDNI interfaces.

   This document considers the following two I-D that supports HTTPS
   delegation:

   - Sub-certificates [I-D.ietf-tls-subcerts]

   - Short-term certificates in ACME using STAR API [I-D.ietf-acme-star]

4. 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.

4.1. Extension to PathMetadata object

   This extension reuses PathMetadata object, as defined in [RFC8006],
   by adding new "Delegation methods" objects as specified in the
   following sections.

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

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

Below shows the PathMetaData Object related to /movie/*
(located at https://metadata.ucdn.example/video.example.com/movies)

PathMetadata:
```
{
    "metadata": [
     {
      "generic-metadata-type": "MI.TimeWindowACL",
      "generic-metadata-value": {
      "times": [{
       "windows": [
        {
         "start": "1213948800",
         "end": "1478047392"
        }]}],
       "action": "allow",
     }},
     {
        "generic-metadata-type": "MI.AcmeStarDelegationMethod",
        "generic-metadata-value": {
        "starproxy": "10.2.2.2",
        "acmeserver" : "10.2.3.3",
        "credentialslocationuri": "www.ucdn.com/credentials",
        "periodicity": 36000
     }}]
}
```

The existence of the "MI.AcmeStarDelegationMethod" object in a
PathMetaData Object shall enable the use of one of the
AcmeStarDelegation Methods, chosen by the delegate. The delegation
method will be activated for the set of Path defined in the
PathMatch. See next section for more details about delegation
methods metadata specification.

4.2. Delegation methods

   This section defines the delegation methods objects metadata. Those
   metadata allows bootstrapping a secured delegatioin by providing the
   dCDN with the needed parameters to set it up.

4.2.1. AcmeStarDelegationMethod object

   This section defines the AcmeStarDelegationMethod object which
   describes metadata related to the use of Acme Star API presented in
   [I-D.ietf-acme-star]

   As expressed in [I-D.ietf-acme-star], 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.

   Property: starproxy

      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: acmeserver

      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: credentialslocationuri

      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 next section on simple meta data type.

Type: Periodicity

Mandatory-to-Specify: Yes

As an example, AcmeStarDelegationMethod object could express the Acme-Star delegation as the following:

```
AcmeStarDelegationMethod: {
    "generic-metadata-type": "MI.AcmeStarDelegationMethod",
    "generic-metadata-value": {
        "starproxy": "10.2.2.2",
        "acmeserver": "10.2.3.3",
        "credentialslocationuri": "www.ucdn.com/credentials",
        "periodicity": 36000
    }
}
```

4.2.2. SubcertsDelegationMethod object

This section defines the SubcertsDelegationMethod object which describes metadata related to the use of Subcerts as presented in [I-D.ietf-tls-subcerts]

As expressed in [I-D.ietf-tls-subcerts], when an origin has set a delegation to a specific domain (i.e. dCDN), the dCDN should present the Origin or uCDN certificate or "delegated_credential" during the TLS handshake [RFC8446] to the end-user client application, instead of its own certificate.

Property: credentialsdelegatingentity

Description: Endpoint ID (IP) of the delegating Entity (uCDN). Endpoint type defined in RFC8006, section 4.3.3

Type: Endpoint

Mandatory-to-Specify: Yes

Property: credentialrecipiententity

Description: Endpoint ID (IP) of the delegated entity (dCDN). Endpoint type is defined in RFC8006, section 4.3.3

      Type: Endpoint

      Mandatory-to-Specify: Yes

   Property: credentialslocationuri

      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
      next section on simple meta data type.

      Type: Periodicity

      Mandatory-to-Specify: Yes

   As an example, when a uCDN has delegated HTTPS delivery to dCDN, a
   SubcertsDelegationMethod object can express the SubCerts delegation
   as the following:

   SubcertsDelegationMethod: {
       "generic-metadata-type": "MI.SubcertsDelegationMethod",
       "generic-metadata-value": {
           "credentialsdelegatingentity": "10.2.2.2",
           "credentialsrecepiententity": "10.2.3.3",
           "credentialslocationuri": "www.ucdn.com/credentials",
           "periodicity": 36000
       }
   }

[5](#). **Metadata Simple Data Type Descriptions**

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

5.1. Periodicity

   A time value expressed in seconds to indicate a periodicity.

   Type: Integer

6. 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       |
   | MI.SubCertDelegationMethod  | RFCthis       |
   +-----------------------------+---------------+
```

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

6.1. 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

6.2. CDNI MI SubCertsDelegationMethod Payload Type

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

   Interface: MI/FCI

   Encoding: see Section 4.2.2

7. Security considerations

Extensions proposed here do not change Security Considerations as
outlined in the CDNI Metadata and Footprint and Capabilities RFCs
[RFC8006].

8. References

8.1. Normative References

   [RFC7937] Le Faucheur, F., Ed., Bertrand, G., Ed., Oprescu, I.,
Ed.,
              and R. Peterkofsky, "Content Distribution Network
              Interconnection (CDNI) Logging Interface", RFC 7937,
              DOI 10.17487/RFC7937, August 2016,
              <https://www.rfc-editor.org/info/rfc7937>.

   [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>.

   [RFC8446] Rescorla, E., "The Transport Layer Security (TLS)
Protocol
              Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August
2018,
              <https://www.rfc-editor.org/info/rfc8446>.

8.2. Informative References

   [I-D.ietf-acme-star]
              Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T.
              Fossati, "Support for Short-Term, Automatically-Renewed
              (STAR) Certificates in Automated Certificate Management
              Environment (ACME)", draft-ietf-acme-star-03 (work in
              progress), March 2018.

   [I-D.ietf-tls-subcerts]
              Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla,
              "Delegated Credentials for TLS", draft-ietf-tls-
              subcerts-02 (work in progress), August 2018.

   [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
   Chatillon 92320
   France

   Email: frederic.fieau@orange.com

   Emile Stephan
   Orange
   2, avenue Pierre Marzin
   Lannion 22300
   France

   Email: emile.stephan@orange.com

   Sanjay Mishra
   Verizon
   13100 Columbia Pike
   Silver Spring MD 20904
   USA

   Email: sanjay.mishra@verizon.com