Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2018

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

October 30, 2017

CDNI extensions for HTTPS delegation
draft-fieau-cdni-interfaces-https-delegation-02

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 a uCDN to a 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 May 3, 2018.

Table of Contents

1. Introduction

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

Several delegation methods are currently proposed within different IETF working groups (refer to [I-D.fieau-cdni-https-delegation] for an overview of delegation works ongoing at the IETF). They specify different methods for provisioning HTTPS delivery credentials.

This document proposes an extension to the CDNI control / Triggers and Metadata interfaces to setup HTTPS delegation between an uCDN and dCDN. Furthermore, it includes a proposal of registry to enable the adding of new methods in the future.

Section 2 is about terminology used in this document. Section 3 presents delegation methods specified at the IETF. Section 4 introduces delegation metadata in CDNI. Section 5 addresses the delegation methods objects. Section 6 describes simple data types.

Section 7 is about an IANA registry for delegation methods.
Section 8 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], CDNI Control interface / Triggers [RFC8007] and Logging interface [RFC7937].

3. Known delegation methods

A few methods are currently being proposed at the IETF to handle delegation of HTTPS delivery between entities, refer to [I-D.fieau-cdni-https-delegation].

Regading the existing delegation methods, we need a common framework in CDNI that provides new requirements on the CDNI interfaces.

This document considers the following methods supporting HTTPS delegation. It may be used between two or more CDNs with applicable interface support following the CDNI framework, such as the CI/ Triggers and Metadata Interface:

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

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

4. Specifying Delegation metadata

Two metadata models for enforcing delegation in CDNI between two entities are suggested in this document:

- New standalone object: SecureDelegation

- Extension to current CDNI metadata model

4.1. SecureDelegation object definition

This section presents an alternative to the approach presented in section 5.1. The section proposes to specify a new metadata object, SecureDelegation, dedicated to provide delegation information between two entities. It aims at fully describing a secured delegation between an uCDN and dCDN by indicating the delegated domain, the start and end duration of a delegation, and the delegation method used.

property: delegateddomains

type: Array

Description: List of delegated hostname indicated by an HostMatch object as defined in RFC8006 section 4.3.3. This value should match the SAN value in certificates.

property: pathpatterns

type: Array

Description: List that contains PathPattern objects with a path to match against a resource's URI path in order to trigger the delegation. It is described in RFC8006, 4.1.4.

property: timewindow

type: TimeWindow

Description: Describes delegation start and end times. Timewindow is defined in RFC8006 section 4.2.

Property: supporteddelegationmethods

type: Array

Description: List of delegation method(s) types that are enabled between a uCDN and a dCDN (ex. "MI.SubcertsDelegationMethod", "MI.AcmeStarDelegationMethod", etc.), as defined in the next section.

As an example: a SecureDelegation object (which contains a TimeWindow, SupportedDelegationMethods and a HostMatch metadata) that only allows the dCDN to deliver content to clients between 09:00 01/01/2000 UTC and 17:00 01/01/2000 UTC:

```
 SecureDelegation object:
 {
         "generic-metadata-type": "MI.SecureDelegation",
         "generic-metadata-value":
         {
           "timewindow": {start: 946717200, end: 946746000},
           "supporteddelegationmethods": ["MI.AcmeStarDelegationMethod",
         "MI.SubcertsDelegationMethod"],
           "pathpatterns": [{
               "pattern": "/movies/*",
               "case-sensitive": true
           }],
           "delegatedDomains": ["www.origin.com"]
         }
 }
```

Such an object shall be conveyed over the CDNI metadata interface.

4.2. Extension to the current CDNI metadata model

This approach consists of reusing the current metadata model by adding delegation information, like the aforementioned "supportedDelegationMethod" property.

Example:

As an example, the PathMatch object can reference a path-metadata that would point 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"
 }
}
```

PathMetaData Object related to /movie/*

```
PathMetadata:
{
 "metadata": [
  {
  "generic-metadata-type": "MI.TimeWindowACL",
  "generic-metadata-value": {
   "times": [
    "windows": [
    {
     "start": "1213948800",
     "end": "1478047392"
    }
   ],
   "action": "allow",
  }},
  {
  "generic-metadata-type": "MI.SecureDelegation"
  "generic-metadata-type": {
   "supporteddelegationmethods ": ["MI.AcmeStarDelegationMethod"],
  }
  }
 ]
}
```

The existence of the "MI.SecureDelegation" object in a PathMetaData Object shall enable the use of one of the supported Methods, chosen by the delegate. See next section for more details about delegation methods metadata specification.

5. Delegation methods

This section defines the delegation methods objects metadata. Each object of the section consists in defining metadata related to the following steps:

- Bootstrapping: bootstrapping a secured delegation consists in providing the dCDN with enough parameters to set it up, e.g. ACME servers, Key Servers, etc..

- Credential renewal: In case of certificates based approaches, [I-D.rescorla-tls-subcerts] and [I-D.ietf-acme-star], there is a need in CDNI to periodically provision and update credentials (certificates or private keys) on the dCDNs for a given delegated domain.

- Expiration/Revocation: expiration of delegation can occur for multiple reasons: changes in delegation rights, delegation validity is over. In [I-D.rescorla-tls-subcerts] or [I-D.ietf-acme-star] approaches, the uCDN may implicitly enforce revocation and will prevent any dCDN to renew certificates, or access credentials, when delegation is expired.

- Logging: Regarding logging aspects, we consider to log usages and errors related to a delegated domain. As an example, CDNI logs include: supported delegation method(s), credentials renewal requests, credential revocation notice, mutual agreement for selected credential method to use, credentials download status for a specific domain, as well as errors, related to credentials transfer, or crypto aspects such as bad cypher suite supports, revoked delegations, etc.

5.1. 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] and [I-D.nir-saag-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-time certificate bound to the master certificate.

Property: starproxy

Type: Endpoint

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

Property: acmeserver

Type: Endpoint

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

Property: credentialslocationuri

Type: Link

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

Property: periodicity

Type: Periodicity

description: expresses the credentials renewal periodicity. See next section on simple meta data type.

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
    }
}
```

5.2. SubcertsDelegationMethod object

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

As expressed in [I-D.rescorla-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 to the end-user client application, instead of its own certificate.

Property: credentialsdelegatingentity

Type: Endpoint

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

Property: credentialrecipiententity

Type: Endpoint

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

Property: credentialslocationuri

Type: Link

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

Property: periodicity

Type: Periodicity

description: expresses the credentials renewal periodicity. See next section on simple meta data type.

As an example, AcmeStarDelegationMethod object could express the Acme-Star-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
    }
}
```

6. Metadata Simple Data Type Descriptions

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

6.1. Periodicity

A time value expressed in seconds to indicate a periodicity.

Type: Integer

7. 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.SecureDelegation	TBD
MI.AcmeStarDelegationMethod	TBD
MI.SubCertDelegationMethod	TBD
...	

7.1. CDNI MI SecureDelegation Payload Type

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

Interface: MI/FCI

Encoding: see Section 5.1

7.2. 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 5.1

7.3. 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 5.2

8. Security considerations

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

9. References

9.1. Normative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

[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>.

9.2. Informative References

[I-D.fieau-cdni-https-delegation] Fieau, F., Emile, S., and S. Mishra, "HTTPS delegation in CDNI", draft-fieau-cdni-https-delegation-02 (work in progress), July 2017.

[I-D.ietf-acme-star] Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Use of Short-Term, Automatically-Renewed (STAR) Certificates to Delegate Authority over Web Sites", draft-ietf-acme-star-00 (work in progress), June 2017.

[I-D.mglt-lurk-tls] Migault, D., "LURK Protocol for TLS/DTLS1.2 version 1.0", draft-mglt-lurk-tls-01 (work in progress), March 2017.

[I-D.nir-saag-star] Nir, Y., Fossati, T., and Y. Sheffer, "Considerations For Using Short Term Certificates", draft-nir-saag-star-00 (work in progress), October 2017.

[I-D.reschke-http-oob-encoding] Reschke, J. and S. Loreto, "'Out-Of-Band' Content Coding for HTTP", draft-reschke-http-oob-encoding-12 (work in progress), June 2017.

[I-D.rescorla-tls-subcerts] Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS", draft-rescorla-tls-subcerts-02 (work in progress), October 2017.

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