Network Working Group F. Fieau, Ed.
Internet-Draft E. Stephan
Intended status: Standards Track Orange
Expires: January 3, 2019 S. Mishra
Verizon
July 02, 2018

CDNI extensions for HTTPS delegation
draft-fieau-cdni-interfaces-https-delegation-04

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

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 (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 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 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

There are currently I-D drafts 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, this additional CDNI framework 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.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 a delegation method between a uCDN and a delegate dCDN.

4.1. SecureDelegation object

This document reuses PathMetadata object, as defined in [RFC8006], by adding a new "SecureDelegation" object containing a "supportedDelegationMethods" property.

This object will allow a uCDN delegating HTTPS delivery to a dCDN to indicate whether there is a delegation occurring on a PathMatch and which are the delegation methods that can be applied when the UA requests contents on the dCDN.

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, according to the IANA registry defined in section 8.

Example:

As an 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.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. 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 are related to the following aspects of a delegation:

- Bootstrapping: bootstrapping a secured delegation consists in providing the dCDN with parameters to set it up, e.g. ACME servers, Key Servers, etc... Please refer to next section for the bootstrapping objects.

- Credential renewal: In case of certificates based approaches, [I-D.ietf-tls-subcerts] and [I-D.ietf-acme-star], CDNI should enable certificates and credentials update on given delegated domains.

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

- Logging: considering delegation logging (usages, errors), CDNI logs should 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.

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] 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-term 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
    }
}
```

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 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, 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
    }
}
```

4.2.3. LurkDelegationMethod object

This section defines the LurkDelegationMethod object which describes metadata related to the use of LURK as defined in [I-D.mglt-lurk-tls].

Property: keyserver

Type: Endpoint

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

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

```
LurkDelegationMethod: {
    "generic-metadata-type": "MI.LurkDelegationMethod",
    "generic-metadata-value": {
        "keyserver": "10.2.2.2",
    }
}
```

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.SecureDelegation	TBD
MI.AcmeStarDelegationMethod	TBD
MI.SubCertDelegationMethod	TBD
MI.LurkDelegationMethod	TBD
...	

6.1. 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

6.2. 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

6.3. 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

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

[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>.

8.2. 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, "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-00 (work in progress), October 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., Sheffer, Y., and T. Eckert, "Considerations For Using Short Term Certificates", draft-nir-saag-star-01 (work in progress), March 2018.

[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.

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