CDNI Metadata for Delegated Credentials

draft-ietf-cdni-https-delegation-subcerts-00

Abstract

The delivery of content over HTTPS involving multiple CDNs raises credential management issues. This document defines metadata in CDNI Control and Metadata interface to setup HTTPS delegation using Delegated Credentials 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 30 July 2022.

Copyright Notice

Copyright (c) 2022 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 ............................................. 3
2. Terminology ............................................. 3
   2.1. Change Log ......................................... 3
3. Known delegation methods ................................. 4
4. CDNI Footprint and Capabilities Advertisement interface (FCI) for delegated credentials ...................... 4
   4.1 FCI.DelegatedCredentials ............................ 5
   4.2 Expected usage of FCI.DelegatedCredentials .......... 5
5. CDNI Metadata interface (MI) for delegated credentials .... 6
6. Delegated credentials call flows ......................... 7
7. IANA Considerations .................................... 9
   7.1 CDNI MI DelegatedCredentials Payload Type .......... 9
   7.1 CDNI FCI DelegatedCredentials Payload Type .......... 9
8. Security Considerations .................................. 10
9. Privacy Considerations .................................. 10
10. References ............................................ 10
   10.1 Normative References ............................... 10
   10.2 Informative References ............................. 11
Authors' Addresses ........................................ 12
1 Introduction

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

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

This document defines the CDNI Metadata interface to setup HTTPS delegation using Delegated Credentials between an upstream CDN (uCDN) and downstream CDN (dCDN). 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 specifies the CDNI Footprint and Capabilities Advertisement interface (FCI) for delegated credentials. Section 5 specifies the CDNI Metadata interface (MI) for delegated credentials. Section 6 specifies the CDNI Metadata interface (MI) for delegated credentials. Section 6 provides overall call-flows for delegated credentials. Section 7 addresses IANA registry for delegation methods. Section 8 discusses Security Considerations. Section 9 discusses Privacy Considerations.

2. Terminology

This document uses terminology from CDNI framework documents: CDNI framework document [RFC7336], CDNI requirements [RFC7337] and CDNI interface specifications documents: CDNI Metadata interface [RFC8006] and CDNI Control interface / Triggers [RFC8007].

2.1. Change Log

draft-cdni-https-delegation-subcerts-00
3. Known delegation methods

The TLS and ACME working groups specified a set of RFCs and Internet drafts to handle delegation of HTTPS delivery between entities. [RFC8739] specifies the Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME). [RFC9115] specifies the automatic generation of...
delegated certificates in ACME. Together these two RFCs allow
managing short term delegated certificates with ACME. [I-D.ietf-cdni-
interfaces-https-delegation] specifies the HTTPS delegation between
the CDN entities using CDNI interfaces using the STAR/ACME delegation
method.

Instead of working with actual certificates, [I-D.ietf-tls-subcerts]
proposes the use of delegated credentials. This Internet Draft (I-D)
specifies the HTTPS delegation between the CDN entities using CDNI
interfaces by relying on the use of delegated credentials as a
delegation method as defined in [I-D.ietf-tls-subcerts].

4. CDNI Footprint and Capabilities Advertisement interface (FCI) for
delegated credentials

A dCDN should advertise its supported delegation methods using the
Footprint and Capabilities interface (FCI) as defined in RFC8008.
With FCI, the dCDN informs the uCDN about its capabilities and the MI
objects supported by the dCDN. Accordingly, to announce the support
for delegated credentials, the dCDN should announce the support of
MI.DelegatedCredentials.

There is also a need to announce parameters, i.e., the number of
delegated credentials needed by the dCDN in order to work properly.
For that purpose we introduce the FCI object
FCI.DelegationCredentials.

4.1 FCI.DelegatedCredentials

The FCI.DelegationCredentials object allows to announce support for
delegated credentials and to announce the number of delegated
credentials needed.

Property: number-delegated-certs-needed

Description: Number of delegated credentials needed by the
dCDN.

Type: integer

Mandatory-to-Specify: Yes.
The following is an example of the FCI.DelegatedCredentials.

```json
{
   "capabilities": [
   {
      "capability-type": "FCI.DelegatedCredentials",
      "capability-value": {
         "number-delegated-certs-needed": 10
      }
   },
   "footprints": [
      <Footprint objects>
   ]
]
}
```

### 4.2 Expected usage of FCI.DelegatedCredentials

At the first announcement of FCI.DelegatedCredentials to an uCDN, the dCDN may announce the number of endpoints as the number of required delegated credentials. When configuring the dCDN, the uCDN may decide to provide only a subset of the requested delegated credentials. Note that, within a dCDN different deployment possibilities of the delegated credentials on the endpoints exist. The dCDN may use one single delegated credential and deploy it on multiple endpoints. Alternatively, the dCDN may deploy a different delegated credential for each endpoint. (provided that the uCDN delivers enough different delegated credentials). This choice depends of course on the number of delegated credentials provided by the uCDN.

Once the dCDN has been configured with delegated credentials and a set of delegated credentials have been deployed on endpoints, the dCDN monitors the number of credentials that are about to expires (e.g. within one day), and ask for new ones by announcing this number of required delegated credentials via the FCI.DelegatedCredentials object.

When uCDN queries and retrieves the FCI object it can push the required number of delegated credentials to the dCDN.
5. CDNI Metadata interface (MI) for delegated credentials

As expressed in [I-D.ietf-tls-subcerts], when an origin has set a delegation to a downstream entity such as a downstream CDN (i.e. dCDN), the dCDN should present the "delegated_credential" during the TLS handshake [RFC8446] to the end-user client application, instead of its own certificate. The dCDN must further be in the possession of the private key corresponding to the public key in DelegatedCredential.cred [I-D.ietf-tls-subcerts]. This allows the end user client to verify the signature in CertificateVerify message sent and signed by the dCDN.

This section defines the object, MI.DelegatedCredentials containing an array of delegated credentials and optionally the corresponding private keys. The CDNI Metadata Interface [RFC8006] describes the CDNI metadata distribution mechanisms according to which a dCDN can retrieve the MI.DelegatedCredentials object from the uCDN.

The properties of the MI.DelegatedCredentials object are as follows.

Property: delegated-credentials

Description: Array of delegated credentials.

Type: array

Mandatory-to-Specify: Yes

Each item of the array of the property delegated-credentials is composed of the following two properties:

Property: delegated-credential

Description: Hex-encoded delegated credential structure DelegatedCredential as defined in [I-D.ietf-tls-subcerts].

Mandatory-to-Specify: Yes

Property: private-key

Description: private key corresponding to the public key
contained in the DelegatedCredential.

Mandatory-to-Specify: No

The private-key property is not mandatory. If not used we suppose that the dCDN generated the public-private key pair for the delegated credential itself and provided the public key information with a mechanism outside of this specification to the uCDN.

Find below an example MI.DelegatedCredential object.

```json
{
  "generic-metadata-type": "MI.DelegatedCredentials",
  "generic-metadata-value": {
    "delegated-credentials": [
      {"delegated-credential": "70105f9bc28aea93f3fed7602b279dc0...
       8970822009b330cd11f052c8dc16b451"},
      {"delegated-credential": "e29c881ad8c5772b35fbdcbe2c4bf16...
       27e87d96458ff18268bae512c62a847"},
      {"delegated-credential": "e8f5853b4836017bd46942d72ce6dc54...
       1d7a25753fea698082344c8273c24cd8"}
    ]
  }
}
```

6. Delegated credentials call flows

An example call-flow using delegated credentials in CDNI is depicted in Figure 1.

1. We suppose that the uCDN has been provisioned and configured with a certificate. Note that it is out of scope of CDNI and the present document how and from where (e.g. CSP) the uCDN acquired its certificate.

2. The uCDN generates a set of delegated credentials (here we suppose that public keys of the dCDN are known). Note, that the uCDN may generate this material at different points in time, e.g. in advance
to have a pool of delegated credentials or on-demand when dCDN request new delegated credentials.

3. Using CDNI Footprint and Capabilities interface [RFC8008], the dCDN advertises MI.DelegatedCredentials capabilities to the uCDN. The dCDN further uses FCI.DelegatedCredentials to ask for a certain number of delegated credentials.

4. Using CDNI the Metadata interface [RFC8006], the dCDN acquires the MI.DelegatedCredentials, therefore retrieving an array of delegated credentials.

5. The client establishes a TLS connection with an endpoint of the dCDN according to [I-D.ietf-tls-subcerts] using the delegated credentials retrieved in step 4.

6. Some delegated credentials are about to expire. The dCDN uses FCI.DelegatedCredentials to announce the number of delegated credentials needed.

7. Using CDNI the Metadata interface [RFC8006], the dCDN acquires the MI.DelegatedCredentials, therefore retrieving an new array of delegated credentials.
6. Some delegated credentials about to expire. CDNI FCI interface used to announce number of delegated credentials needed using FCI.DelegatedCredentials +---------------------> |

7. CDNI Metadata interface used to provide the MI.DelegatedCredential object <--------------------- |

Figure 1: Example call-flow of Delegated credentials in CDNI

7. IANA Considerations

This document requests the registration of the following entries under the "CDNI Payload Types" registry hosted by IANA regarding "CDNI delegation":

<table>
<thead>
<tr>
<th>Payload Type</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCI.DelegatedCredentials</td>
<td>RFCthis</td>
</tr>
<tr>
<td>MI.DelegatedCredentials</td>
<td>RFCthis</td>
</tr>
</tbody>
</table>

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

7.1 CDNI MI DelegatedCredentials Payload Type

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

Interface: MI/FCI

Encoding: see corresponding section

7.1 CDNI FCI DelegatedCredentials Payload Type

Purpose: The purpose of this Payload Type is to advertise the number of delegated credentials needed (and any associated capability advertisement)
8. Security Considerations

The extensions defined in the present document allow to provide delegated credentials to dCDNs. The delegated credentials themselves are short-lived and as such a single leaked delegated credential represents a limited security risk. However, it is important to ensure that an attacker is not able to systematically retrieve a more important number of delegated credentials. Such an attack would allow the attacker to systematically impersonate dCDN nodes.

The FCI and MI objects defined in the present document are transferred via the interfaces defined in CDNI [RFC8006]. [RFC8006] describes how to secure these interfaces, protecting the integrity, confidentiality and ensuring the authenticity of the dCDN and uCDN. The security provide by [RFC8006] should therefore address the above security concerns.

9. Privacy Considerations

The information, FCI and MI objects defined in the present document do not contain any personally identifiable information (PII). As such this document does not change or alter the Confidentiality and Privacy Consideration outlined in the CDNI Metadata and Footprint and Capabilities RFCs [RFC8006].

10 References

10.1 Normative References


10.2 Informative References


Frederic Fieau
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

Guillaume Bichot
Broadpeak
15, rue Claude Chappe
35510 Cesson-Sevigne
France

Email: guillaume.bichot@broadpeak.tv

Christoph Neumann
Broadpeak
15, rue Claude Chappe
35510 Cesson-Sevigne
France

Email: christoph.neumann@broadpeak.tv