Internet Engineering Task Force (IETF)
Request for Comments: 9677
Category: Standards Track
ISSN: 2070-1721

F. Fieau
E. Stephan
Orange
G. Bichot
C. Neumann
Broadpeak

October 2024

Content Delivery Network Interconnection (CDNI) Metadata for Delegated Credentials

Abstract

The delivery of content over HTTPS involving multiple Content Delivery Networks (CDNs) raises credential management issues. This document defines metadata in the Content Delivery Network Interconnection (CDNI) Control and Metadata interface to set up HTTPS delegation using delegated credentials from an upstream CDN (uCDN) to a downstream CDN (dCDN).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9677.

Table of Contents

1. Introduction

Content delivery over HTTPS utilizing one or more Content Delivery Networks (CDNs) along the delivery path necessitates the management of credentials. This requirement is particularly pertinent when an entity delegates the delivery of content via HTTPS to another trusted entity.

This document specifies the CDNI Metadata interface for establishing HTTPS delegation through the use of delegated credentials, as defined in [RFC9345], between an upstream CDN (uCDN) and a downstream CDN (dCDN).

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses terminology from the CDNI specifications -- CDNI framework [RFC7336], CDNI requirements [RFC7337], and CDNI Metadata interface [RFC8006].

3. CDNI Footprint and Capabilities Advertisement Interface (FCI) Capabilities Object for Delegated Credentials

A dCDN should advertise its supported delegation methods using the Footprint and Capabilities Advertisement interface (FCI) as defined in [RFC8008]. The FCI.Metadata object enables a dCDN to communicate its capabilities and the Metadata interface (MI) objects it supports. To indicate support for delegated credentials, the dCDN should announce the support for MI.DelegatedCredentials, as illustrated in the example below.

```
{
  "capabilities": [
    {
      "capability-type": "FCI.Metadata",
      "capability-value": {
        "metadata": [
          "MI.DelegatedCredentials",
          "... other supported MI objects ..."
        ]
      },
      "footprints": [
        "Footprint objects"
      ]
    }
  ]
}
```

This document also defines an object that informs the uCDN of the number of delegated credentials supported by the dCDN, enabling the uCDN to supply the appropriate number of delegated credentials. To

this end, the FCI object, FCI.DelegationCredentials, is introduced.

3.1. FCI.DelegatedCredentials

The FCI.DelegationCredentials object enables advertising the maximum number of delegated credentials supported by the dCDN. This number typically (but not necessarily) corresponds to the number of servers designated by the dCDN to support delegated credentials.

The property PrivateKeyEncryptionKey contains a public key provided by the dCDN that MUST be used by the uCDN to encrypt private keys whenever such private keys are transmitted to the dCDN using MI.DelegatedCredentials (see Section 4).

Property: number-delegated-certs-supported
Description: Number of delegated credentials supported by the dCDN.
Type: integer
Mandatory-to-Specify: Yes

Property: PrivateKeyEncryptionKey
Description: Public key in JSON Web Key (JWK) format [RFC7517] of the dCDN to be used by the uCDN to encrypt private keys.
Type: string
Mandatory-to-Specify: No

The following is an example of the FCI.DelegatedCredentials.

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

3.2. Expected Usage of the Property Number of Supported Delegated Credentials

The dCDN uses the FCI.DelegatedCredentials object to announce the number of servers that support delegated credentials.

When the uCDN receives the FCI.DelegatedCredentials object, it can issue the supported number of delegated credentials to the dCDN. When configuring the dCDN, the uCDN MAY decide to provide less than the maximum supported delegated credentials to the dCDN. 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 is at the discretion of the dCDN and depends on the number of delegated credentials provided by the uCDN.

The FCI.DelegationCredentials object does not address expiry or renewal of delegated credentials. Once the uCDN has provided delegated credentials via the MI, the uCDN SHOULD monitor the provided credentials and their expiry times and SHOULD refresh dCDN credentials via the MI in a timely manner. The uCDN may decide not to monitor the validity period of delegated credentials and not to

refresh the credentials, for example, in cases of short-term one-shot deployments or once it has decided to deprovision a dCDN. If the delegated credential is not renewed on time by the uCDN, the servers of the dCDN that only have expired delegated credentials MUST refuse any new TLS connection that requires an up-to-date delegated credential.

4. CDNI Metadata Interface (MI) Metadata Object for Delegated Credentials

As expressed in [RFC9345], when an uCDN has delegated to a dCDN, the dCDN presents the "delegated_credential" (rather than its own certificate) during the TLS handshake [RFC8446] to the User Agent. This implies that the dCDN is also in the possession of the private key corresponding to the public key in DelegatedCredential.cred [RFC9345]. This allows the User Agent to verify the signature in a CertificateVerify message (Section 4.4.3 of [RFC8446]) sent and signed by the dCDN.

This section defines the MI.DelegatedCredentials object containing an array of delegated credentials and optionally the corresponding private keys. The CDNI MI [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 of DelegatedCredentialObject objects
Mandatory-to-Specify: Yes

The DelegatedCredentialObject object is composed of the following properties:

Property: delegated-credential
Description: Base64-encoded (as defined in Section 4 of [RFC4648]) version of a CertificateEntry as defined in Section 4.4.2 of [RFC8446]. The CertificateEntry MUST contain a DelegatedCredential structure (as defined in [RFC9345]) using the extension in the CertificateEntry of its end-entity certificate (see Section 4.1.1 of [RFC9345]).
Type: string
Mandatory-to-Specify: Yes

Property: private-key
Description: Encrypted private key corresponding to the public key contained in the DelegatedCredential. The envelope format for this property is JSON Web Encryption (JWE) [RFC7516] using the base64 compact serialization (Section 7.1 of [RFC7516]).
Type: string
Mandatory-to-Specify: No

The private-key property is not mandatory. If not specified, it is assumed that the dCDN generated the public-private key pair for the delegated credential itself and provided the public key information with an out-of-band mechanism to the uCDN. See Section 7 for constraints regarding the usage of the private key.

If the private-key property is used, the transported private key MUST be encrypted using the PrivateKeyEncryptionKey specified in FCI.DelegatedCredentials. The envelope format for this property MUST use JWE [RFC7516] using the base64 compact serialization (Section 7.1 of [RFC7516]), whereas the private key is included as JWE Ciphertext in the JWE. The JWE content-type field MAY be used to signal the media type of the encrypted key.

Below, please see an example of an MI.DelegatedCredentials object.

```
    {
    "generic-metadata-type": "MI.DelegatedCredentials",
    "generic-metadata-value": {
        "delegated-credentials": [
                {"delegated-credential":
                    "cBBfm8KK6pPz/tdgKyedwA...
                    iXCCIAmzMM0R8FLI3Ba0UQ=="},
                {"delegated-credential":
                    "4pyIGtjFdys1+9y/4sS/Fg...
                    J+h9lnRY/xgmi65RLGKoRw=="},
                {"delegated-credential":
                    "6PWFO0g2AXvUaULXLObcVA...
                    HXoldT/qaYCCNEyCc8JM2A=="}
            ]
        }
    }
```

5. Delegated Credentials Call Flow

An example call-flow using delegated credentials is depicted in Figure 1. The steps are as follows.

1. It is assumed 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., which Content Service Provider) the uCDN acquired its certificate.

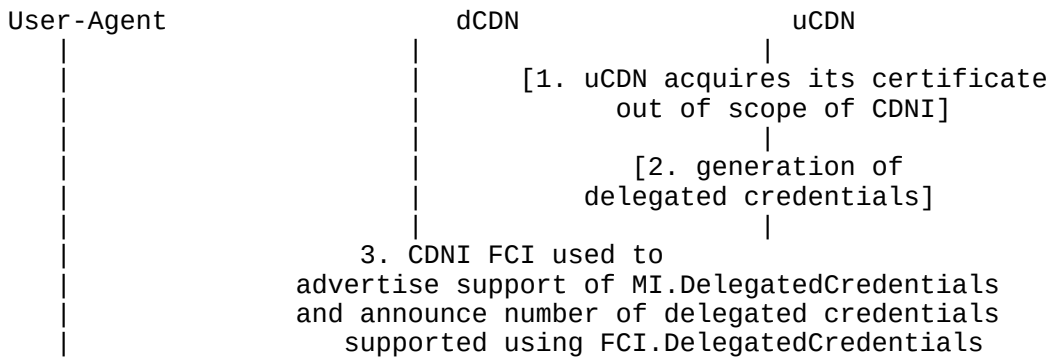
2. The uCDN generates a set of delegated credentials (here it is assumed that public keys of the dCDN are known). Note that the uCDN may generate this material at different points in time, e.g., in advance to have a pool of delegated credentials or on demand when the dCDN announces its maximum number of supported delegated credentials.

3. Using the CDNI FCI [RFC8008], the dCDN advertises MI.DelegatedCredentials capabilities to the uCDN. The dCDN further uses FCI.DelegatedCredentials to advertise the maximum number of supported delegated credentials.

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

5. The client establishes a TLS connection with an endpoint of the dCDN according to [RFC9345] using the delegated credentials retrieved in step 4.

6. When some delegated credentials are about to expire, the uCDN uses the CDNI MI [RFC8006] to provide new, valid delegated credentials.



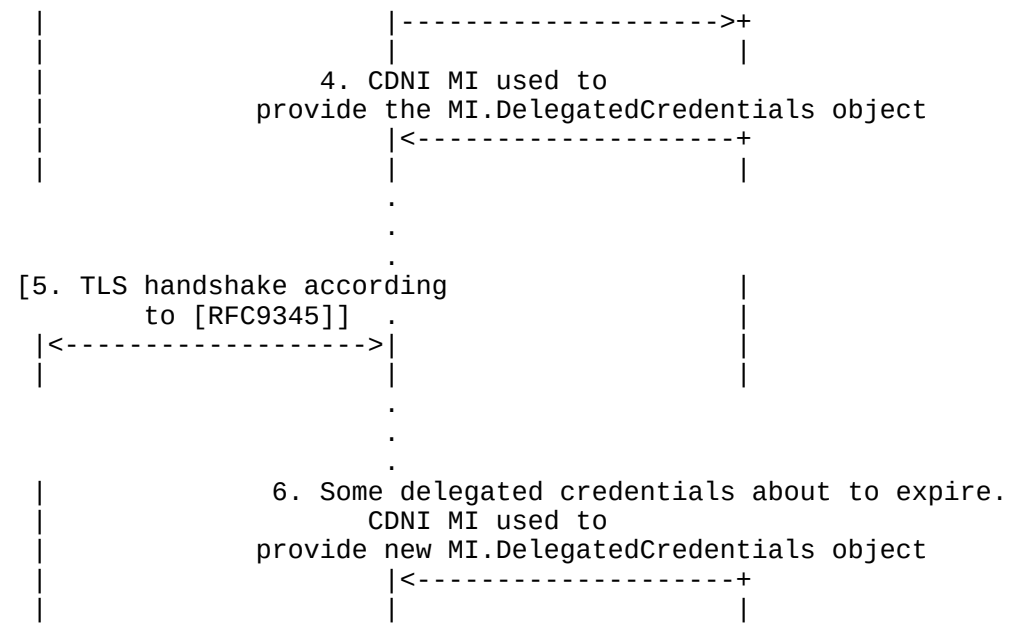


Figure 1: Example Call Flow of Delegated Credentials in CDNI

6. IANA Considerations

IANA has registered the following payload types in the "CDNI Payload Types" registry in the "Content Delivery Network Interconnection (CDNI) Parameters" registry group.

Payload Type	Reference
MI.DelegatedCredentials	RFC 9677
FCI.DelegatedCredentials	RFC 9677

Table 1

Sections 6.1 and 6.2 provide additional necessary information for the registration of those CDNI payload types (see Section 2.2 of [RFC7736]).

6.1. CDNI MI.DelegatedCredentials Payload Type

Purpose: The purpose of this payload type is to distinguish delegated credentials MI objects.

Interface: MI/FCI

Encoding: See Section 4.

6.2. 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).

Interface: FCI

Encoding: See Section 3.1.

7. Security Considerations

The extensions defined enable providing delegated credentials to

dCDNs. A delegated credential can only be used by a dCDN if it is in possession of the associated private key. Similarly, an attacker requires access to the private key in order to exploit a delegated credential and impersonate dCDN nodes. Thus, leakage of only the delegated credential without the private key represents a limited security risk.

Delegated credentials and associated private keys are short-lived (per default, the maximum validity period is set to 7 days in [RFC9345]) and as such a single leaked delegated credential with its private key represents a limited security risk. Still, it is NOT RECOMMENDED to send private keys through the MI. Omitting the private key further limits the possible ways an attacker could exploits the delegated credential.

If this recommendation is not followed, i.e., the private key is communicated via the MI, the transported private key MUST be encrypted within a JWE envelope using the encryption key (PrivateKeyEncryptionKey) provided within the FCI.DelegatedCredentials by the dCDN. The JWE encryption key (PrivateKeyEncryptionKey) MUST have a strength equal to or larger than the private key it is encrypting for transport. Note that the specified encryption method does not offer forward secrecy. If the dCDN’s encryption key becomes compromised in the future, then all encrypted JWEs will become compromised. Due to the short-lived nature of delegated credentials, the impact is limited.

It is also important to ensure that an attacker is not able to systematically retrieve a consecutive or consistent set of delegated credentials and associated private keys. Such an attack would allow the attacker to systematically impersonate dCDN nodes. The 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 and confidentiality, as well as ensuring the authenticity of the dCDN and uCDN, which should prevent an attacker from systematically retrieving delegated credentials and associated private keys.

8. Privacy Considerations

The FCI and MI objects and the information 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 considerations outlined in Section 8.2 of [RFC8006] and Section 7 of [RFC8008].

A single or systematic retrieval of delegated credentials and associated private keys would allow the attacker to decrypt any data sent by the end user intended for the end service, which may include PII.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015,

<https://www.rfc-editor.org/info/rfc7516>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[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>.

[RFC8008] Seedorf, J., Peterson, J., Previdi, S., van Brandenburg, R., and K. Ma, "Content Delivery Network Interconnection (CDNI) Request Routing: Footprint and Capabilities Semantics", RFC 8008, DOI 10.17487/RFC8008, December 2016, <https://www.rfc-editor.org/info/rfc8008>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC9345] Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS and DTLS", RFC 9345, DOI 10.17487/RFC9345, July 2023, <https://www.rfc-editor.org/info/rfc9345>.

9.2. 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>.

[RFC7736] Ma, K., "Content Delivery Network Interconnection (CDNI) Media Type Registration", RFC 7736, DOI 10.17487/RFC7736, December 2015, <https://www.rfc-editor.org/info/rfc7736>.

Authors' Addresses

Frdric Fieau
Orange
40-48, avenue de la Rpublique
92320 Chtillon
France
Email: frederic.fieau@orange.com

Emile Stephan
Orange
2, avenue Pierre Marzin
22300 Lannion
France
Email: emile.stephan@orange.com

Guillaume Bichot
Broadpeak

3771 Boulevard des Allis
35510 Cesson-Svign
France
Email: guillaume.bichot@broadpeak.tv

Christoph Neumann
Broadpeak
3771 Boulevard des Allis
35510 Cesson-Svign
France
Email: christoph.neumann@broadpeak.tv