Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

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

March 13, 2017

CDNI interfaces update for HTTPS delegation
draft-fieau-cdni-interfaces-https-delegation-00

Abstract

Content delivery includes one or more CDNs and in many instances involves cascaded delegation when handling encrypted data. The delivery of such content over HTTPS though raises credential management issues. Two models of HTTPS delegation can be considered: direct delegation, and "cascaded" delegation. While the first model of delegation is addressed by most of the work at the IETF, in the latter case, it is up to downstream CDN(s) delivering the content to an end-user to present legacy credentials of either the origin or of the upstream CDN which delegated the delivery to the aforementioned dCDN. This document presents updates needed in CDNI Control and Metadata interfaces to setup HTTPS delegation between an uCDN and 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 http://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 September 14, 2017.

Table of Contents

1. Introduction

In most cases, content is delivered over HTTP or HTTPS using one and more CDNs along the delivery path in the direction of end-user. The delivery of the content over HTTPS raises credential management issues. This document presents updates needed in CDNI Control and Metadata interfaces to setup HTTPS delegation between an uCDN and dCDN.

It is up to the downstream CDN which delivers the content to the end-user to present credentials of either the origin or of the upstream CDN which delegated the delivery to the aforementioned dCDN. The domain of the certificate presented to the end-user must match the domain delivering content. However, in a model when an entity other than the origin has been delegated to serve secured content on behalf of the certificate owner, then in such case of "cascaded" delegation, an end-user (UA) may not know (or have the ability to know) if the domain of the just authenticated entity delivering the content is the same as the origin domain. Current IETF work on credential delegations do not yet include solutions for cascaded delegation that

would allow an UA validate whether content is delivered by origin domain or by a delegated entity on behalf of the origin domain.

CDNi framework supports implicit cascade delegation whereas, HTTPS delegation requires explicit transitive delegation to carry the credentials from the origin to dCDN passing through all intermediate CDNs.

Several delegation methods are currently proposed within several IETF working groups. The specifications of the provisioning of their credentials (how key is transported and stored) are out of the scope of the document. The intent of the document is to identify update to the CDNI interfaces, namely CDNI control / Triggers and Metadata interfaces to support multiple levels of delegation in CDNI for HTTPS.

Section 2 is about terminology used in this document. Section 3 shows the delegation models in delivery architectures. Section 4 presents delegation methods specified at the IETF. Section 5 introduces delegation metadata for CDNI. Section 6 discusses the management of credentials in delegation. Section 7 is about an IANA registry for delegation methods. Section 8 discussed how to address the expiration of a delegation. Section 9 is about logging delegation data. Section 10 shows 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. HTTPS Delegation Models

This document considers two models for HTTPS delegation and their applicability to CDN interconnection.

- Direct HTTPS delegation

A uCDN delegates HTTPS delivery to dCDN. The dCDN can deliver contents to the UA on behalf of the uCDN: the uCDN domain stays visible in the UA, the UA accepts a (sub) certificate bound to the uCDN. Only one level of delegation is considered here.

Figure 1: Direct HTTPS delegation in CDNI

- Cascaded HTTPS delegation:

An origin delegates HTTPS delivery to uCDN which in turn delegates delivery to dCDNs. The dCDN can deliver contents to the UA on behalf of the Origin: the origin domain stays visible to the UA, the UA accepts a (sub) certificate bound to the origin. N levels of cascade might be considered here.

-- sub-case 1: delivery with origin domain

Figure 2: cascaded HTTPS delegation in CDNI

-- sub-case 2: delivery with uCDN domain

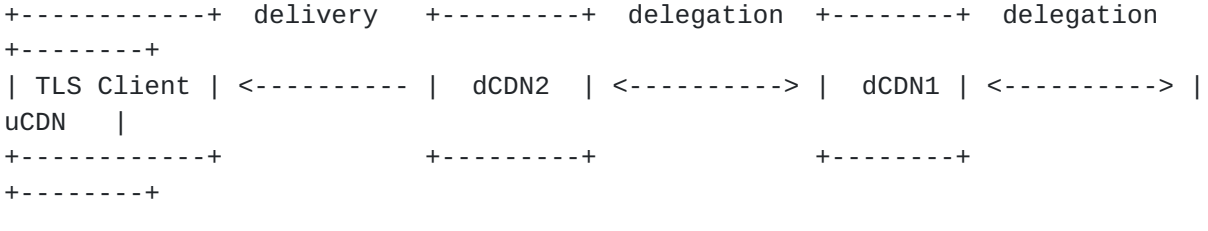

Figure 3: cascaded HTTPS delegation in CDNI

In both models, a uCDN could give its private keys to one or more dCDNs. Some virtual hosting providers have required this method of credentials sharing, such as private keys and certificates. However, this is not desirable for the assignee of the credentials, as it significantly degrades the security of the entire architecture.

4. Known delegation methods

A few methods are currently being proposed at the IETF to handle delegation of HTTPS delivery between entities respecting those constraints. Note that these methods are still an ongoing work at the IETF within specific WG. We however anticipate the need to handle delegation in interconnected CDNs and a need to address within

the CDNI WG. Despite the types of delegation methods, we might need a common framework in CDNI that would provide new requirements on the CDNI interfaces.

This document considers three methods supporting HTTPS delegation and 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 and short-term certificates

In sub-certs [I-D.rescorla-tls-subcerts], a dCDN might be able to present a "delegated_credentials" to UA, containing a cryptographic assertion that it is an authorized delegate of the uCDN. This solution requires changes in the UA. A Delegated credentials has a validity period (no longer than 7 days) and a public key.

Short-term certificates [I-D.sheffer-lurk-cert-delegation] are standard certificates with a short period of validity, which can be renewed as long as the delegation is true. Unlike the subcerts, this solution does not require any changes in the UA. In both cases however, periodic certificates provisioning on the CDNs is required.

- Keyless SSL / LURK [I-D.mglt-lurk-tls]

KeyLess SSL approaches (e.g. LURK) might allow a dCDN get credentials when the UA requests a TLS session establishment. The main objective of keyless SSL is to keep the uCDN (or the origin) private keys stored in a secured Key Server (for instance hosted on the uCDN), so that they would never be exposed to the dCDN caches.

- Out-of-Band redirection [I-D.reschke-http-oob-encoding]

OOB redirection is a method to enable an Origin to delegate the delivery of contents to another server. This method suggests the use of a resource map that will be downloaded from the origin by the user-agent, instead of the content itself. The UA will be able to contact secondary sources (i.e., CDN caches) to get the content on behalf of the Origin.

OOB advantages are dual for the uCDN and the Origin. First, there might be no need to deal with delegated credentials nor private keys at uCDN nor dCDNs, and second, the content can remain encrypted on the dCDN which can be of interest for the Origin.

Supporting these delegation methods might end up with the definition of new metadata and triggers, specific to each of them.

5. Delegation definition

When HTTPS delegation has been set for a specific domain, the dCDN should present the Origin or uCDN certificate or "delegated_credential" instead of its own certificate when content delivery is requested.

CDNI might needs to advertise support of HTTPS delegation information and parameters from uCDN to dCDNs. Delegation related metadata might for instance include the delegated domain, and delegation period. Multiple delegations might be advertised for a same domain.

We might also consider the dCDN discovery of the key server interface endpoint as well as the mutual authentication of the dCDN and uCDN key server.

For instance, the uCDN might advertise to the dCDNs metadata such as the delegation validity (start, end), certificate renewal periodicity (if needed), the delegated domain FQDN. Such information could be for instance, conveyed over the CDNI metadata interface. We might also advertise what is/are the delegation method(s) to use for a given delegated domain (ex. OOB, Subcerts, etc.) between a uCDN and a dCDN. The above information could be carried in a delegationMethodOptions object in the DeliveryDelegation metadata.

For instance, delegation might be seen as a new metadata DeliveryDelegation object.

Example DeliveryDelegation object:

```
{
        "generic-metadata-type": "MI.DeliveryDelegation",
        "generic-metadata-value":
        {
                times: [{
                        "window": [{start: delegationStart, end:
delegationEnd}]
                        }],
                delegationMethodType: "subcerts", // refer to IANA
considerations
                delegationMethodOptions: {
                        "delegatedDomain": domain,
                        "credentialLocationURI": locationURI,
                        "renewalPeriodicity": periodicity,
                        "renewalMode": mode, // "pull" or "push"
                        "KeyServerEndpoint": endpoint
                }
        }
```

```
        }
```

According to HTTPS delegation models, we might consider delivery delegation rights to be expressed through a set of metadata received at uCDN or dCDN. As an example, the metadata might indicate if, for instance, the uCDN has been given the right to delegate delivery to other dCDN domains. This could be expressed by "delegabilityAllowed" boolean. Finer granularity might be expected.

6. Credentials management

In case of certificates based approaches, aka subcerts [I-D.rescorla-tls-subcerts] and short-lived certs [I-D.sheffer-lurk-cert-delegation], there might be a need in CDNI to periodically provision and update credentials (certificates or private keys) on the dCDNs for a given delegated domain. This provisioning phase might be done off-line and is not in the scope of CDNI.

We might also need to control credentials, e.g., sub-certificates, renewal demands incoming from dCDNs, or from the uCDN itself. This might be specified in delegation metadata (see Delegation definition). The credentials can be downloaded, either using dCDN pull requests to the uCDN, triggered or not by an UA request, or uploaded via an uCDN push request. Both ways of provisioning might be specified in the corresponding metadata.

In Keyless SSL approaches, like LURK [I-D.mglt-lurk-tls], we might have similar needs for CDNI: discovery of the key server, interface for credentials exchanges. The credentials exchanges interface that allows live delivery of credentials (e.g., session keys) at the TLS session setup between the UA and the dCDN should be out of scope of CDNI.

OOB redirection [I-D.reschke-http-oob-encoding] might require other specific needs because of its way of working. For example, a uCDN might allow the creation of a resource map pointing at dCDNs pertaining to a delegation.

The uCDN and dCDN might accept connections when BC header is positioned to true. In case of expired delegation, enforcement might consist of creating a resource map not containing expired dCDN sources, or a uCDN not giving the necessary keys to decrypt the content stored on the revoked dCDN.

7. Handling delegation expiration

When the delegation has terminated for a given domain, an uCDN might have to enforce the expiration of the delegation. Expiration of

delegation can occur for multiple reasons: changes in delegation rights, delegation validity is over.

The uCDN might have then to prevent any dCDN to renew certificates, or access credentials, and might advertise consequently the expiration status to the requesting dCDN for that delegated domain.

Removing of credentials in cascade might be ensured by the Control Interfaces / Triggers.

CDNI Metadata Interface already provides deliveryAuthorization metadata [RFC8006] (see 7.1.17) which might be used for handling delegation expiration

8. Logging delegation related data

Regarding logging aspects, we might consider to log usages and errors related to a delegated domain.

As an example, CDNI logs might 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.

9. IANA considerations

The document might consider specifying a registry of delegation methods, e.g. [1] OOB, [2] subcert, [3] shortlivedcert, that might be used in the delegation metadata in CDNI.

10. Security considerations

The CI/T interface and Metadata interface need only to specify mechanisms for delegation between uCDN and dCDN without the use of actual transfer of encrypting keys within the interface messages. The uCDN actions must be limited to in specifying its support for methods it prefers for delegation, actual delegation and revocation of any delegation. The dCDN similarly, must indicate delegation methods it supports. Any subsequent communications enabling delegation must be limited to the agreed delegation method. Additionally, the HTTPS delegation framework must comply with security considerations as specified within RFC 8007 [CDNI Control Interfaces].

11. References

11.1. Normative References

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <http://www.rfc-editor.org/info/rfc2818>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://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, <http://www.rfc-editor.org/info/rfc5280>.

[RFC6844] Hallam-Baker, P. and R. Stradling, "DNS Certification Authority Authorization (CAA) Resource Record", RFC 6844, DOI 10.17487/RFC6844, January 2013, <http://www.rfc-editor.org/info/rfc6844>.

[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, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc8007>.

11.2. Informative References

[I-D.cairns-tls-session-key-interface]
Cairns, K., Mattsson, J., Skog, R., and D. Migault, "Session Key Interface (SKI) for TLS and DTLS", draft-cairns-tls-session-key-interface-01 (work in progress), October 2015.

[I-D.cdni-fieau-lurk-https-delegation]
Fieau, F. and S. Emile, "Limited Use of Remote Keys for Interconnected CDNs", draft-cdni-fieau-lurk-https-delegation-00 (work in progress), July 2016.

[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.reschke-http-oob-encoding]
Reschke, J. and S. Loreto, "'Out-Of-Band' Content Coding for HTTP", draft-reschke-http-oob-encoding-11 (work in progress), March 2017.

[I-D.rescorla-tls-subcerts]
Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS", draft-rescorla-tls-subcerts-01 (work in progress), March 2017.

[I-D.sheffer-lurk-cert-delegation]
Sheffer, Y., "Delegating TLS Certificates to a CDN", draft-sheffer-lurk-cert-delegation-00 (work in progress), May 2016.

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