Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2018

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

July 3, 2017

HTTPS delegation in CDNI
draft-fieau-cdni-https-delegation-02

Abstract

This document examines probable solutions for delegating encrypted content delivery within the context of CDN interconnection. The HTTPS delegation also expects delivering content without compromising security, integrity and user privacy.

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 January 4, 2018.

Copyright Notice

Table of Contents

1. Introduction

Currently, sixty percent of the HTTP traffic on the internet is encrypted, that is, it is transported over TLS [RFC5246]. At the same time, HTTP traffic served by CDNs is on the rise as well. The traffic on CDNs is estimated to raise to seventy-five percent in year 2020 [ciscotraffic].

This document discusses viability of and solution for addressing delegation of HTTP over TLS [RFC2818] traffic within the context of CDN interconnection. HTTPS delegation allows delivering party, e.g. a CDN, to deliver content for and on-behalf of an origin server.

This draft considers three approaches for delegating HTTPS traffic in a CDNI context. These include Limited Use of Remote Keys (LURK), Out-of-Band, Short-Lived Certificates and Sub-Certificates (or delegated credentials). We examine these approaches focusing on the following three issues:

- Modification (or no) changes in the user agent
- Trust delegation (transitivity, that is, Is a CDN allowed to delegate the trust it received directly from the Origin?)
- Maintain the user experience (privacy, integrity and performance)

To recap CDNi goals, the CDNi WG focuses on the relationship between the upstream CDN and the downstream CDN. Therefore, this document examines applicability of HTTPS delegation between two CDNs in response to a UA request while maintaining end-to-end integrity of UA request.

2. Terminology

- UA: User Agent
- CDNI: Content Delivery Network
- SLC: Short-Lived certificates
- LURK: Limited Use of Remote Keys
- dCDN: downstream Content Delivery Network
- uCDN: upstream Content Delivery Network
- CSP: Content Service Provider
- OOB: Out-of-Band
- PKS: Private Key Server

3. LURK for CDNI

[I-D.cdni-fieau-lurk-https-delegation] shows 2 use cases related to CDN interconnection based on LURK [I-D.mglt-lurk-tls-use-cases]:

- uCDN Key Server: uCDN is authoritative on several origin domains. Its key Server hosts certificates and private keys of these origins. An interface between uCDN and dCDN allows dCDN to query credentials per session for these origins. Note that a dCDN is typically connected to several uCDNs.
- CSP Key Server: a Content Service Provider is authoritative source for origin domains. CSPs key Server hosts certificates and private keys for its domains. An interface between this key

Server and the dCDN allows the dCDN to query credentials for a given session for these origins.

3.1. uCDN Key Server (CDNI framework)

dCDNs have an interface to a Key Server hosted at the uCDN side. It may be typically a case of CDNI regional delivery delegation.

When the UA has been redirected from the uCDN to a dCDN,it initiates a TLS connection with a dCDN cache to get its content. Since dCDN cache does not store the private keys for the requested certificate, it queries the uCDN Key Server (KS) to get credentials to establish the TLS session. Once the UA establishes a TLS connections with the dCDN, the dCDN can finally begin to deliver HTTP over TLS content to the UA.

This framework makes two assumptions:

- The UA includes the Origin domain name in the SNI field of the TLS ClientHello to enable a dCDN to select the Key Server of uCDN to generate credentials for the session.

- The uCDN Key Server is provisioned with the certificate and the private key for this Origin domain name.

3.2. CSP Key server

In this framework the CSP provides a Key Server for the origin domains it is authoritative for to ensure an end-to-end HTTPS delegation, from the origin to the dCDN which eventually delivers the HTTPS content to the UA. The CSP provides the LURK Key Server and interface.

The CSP delegates the HTTPS content delivery to an uCDN that in turn delegates the HTTPS delivery to a dCDN. The CSP provides the uCDN with a Key Server interface to delegate the content delivery. In that case, the dCDN relies on credentials received from a CSP Key Server (KS) to deliver HTTPS content.

This framework supports 2 options:

- direct: The dCDN requests directly the CSP key server

- cascaded: the dCDN session key requests are relayed by the uCDN to the Key Server

4. Out-of-Band for CDNI

This section presents the usage of HTTP Out-of-Band mechanism [I-D.reschke-http-oob-encoding] to deliver HTTPS content in CDNI.

4.1. OOB overview

Out-of-Band HTTPS content delivery (OOB) relies on the use of the "out-of-band" value in "Accept-encoding" HTTP header of the request. It indicates that the UA supports downloading the resource from alternative locations than the Origin. To that purpose, when the out-of-band content encoding is set, the Origin server may respond with a list of caches to fetch the requested resource.

Example:

```
{sr: [{r:"https://ori/path/content1", r:"https://cdn1/path/content1"}]}
```

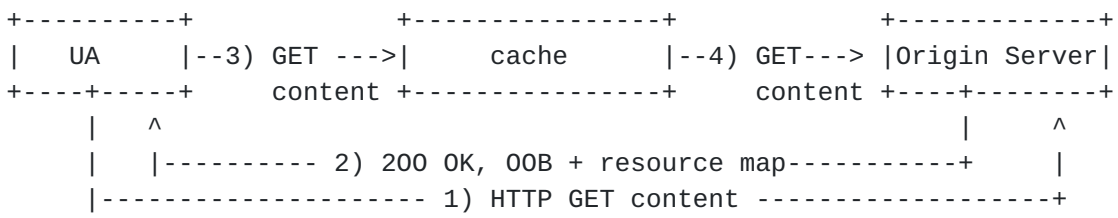

Figure 1: OOB general principle

Out-of-Band framework involves the following functional entities:

Origin server:

- OOB specifies the first step of the HTTPS delivery delegation: the soft redirection toward alternative locations that Origin trusts in a resource map.
- The Origin server receives new HTTP header value "accept-encoding" and responses with a "content-encoding"

UA:

- must store resource map received from the Origin server
- must support new HTTP header "accept-encoding" values to comply with OOB

Cache server:

- has standard cache functions, and supports TLS for delivery and content provisioning from origin.

- When the cache receives a request from the UA, it uses the "http referer" of the request to know the origin url from where to pull and store the requested content.

4.2. OOB applied to CDNI

In CDNI, uCDN may use OOB to direct a UA to dCDN by indicating a resource map where it can fetch content. In CDNI, an end-to-end delegation allows an origin delegate HTTPS delivery to uCDN which in turns delegates it to dCDN.

For instance, end-to-end delegation may involve cascaded resource maps. The Origin delegates HTTPS delivery to the uCDN using OOB, and uCDN delegates HTTPS delivery to dCDN through OOB. In that case, the UA requests Origin that sends back a resource map pointing at the uCDN. Then UA requests the uCDN which sends back a resource map (OOB) pointing at dCDN hosted resources.

figure 2: OOB with successive resource maps in CDNI

5. Sub-certificates and Short-lived Certificates for CDNI

The need to scale is a central requirement to generalize HTTPS content delivery across CDNs. Both [I-D.rescorla-tls-subcerts] and [I-D.ietf-acme-star] share the same paradigm. They aim to decouple credentials provisioning from content delivery.

The [I-D.ietf-acme-star] cert architecture adds interactions between the CDN and the Origin and between the Origin and the CA which signs the limited authority delegation;

[I-D.ietf-acme-star] certificate implementation do not require modifications in the UA, but requires specific certificate request from CSP to CA and retrieval of certificate by CDN from the CA. The [I-D.rescorla-tls-subcerts] proposes an architecture where the TLS server by itself can create a sub-certificate (also referred to as "delegated credentials") based on the original certificate issued to it by the CA. This sub-certificate's scope is only to the credentials issued by the CA corresponding to the original certificate the CA authorized the TLS server.

A possible applicability of this may be where a uCDN may issue "delegated_credentials" to a dCDN for any HTTPS content it delegates to dCDN for delivery.

This new "delegated certificate" will have a validity interval (7 days) along with the public key issued to the Content Service Provider (CSP) or to its surrogate (CDN) by the CA.

The Subcerts require changes to the user agent. The [I-D.rescorla-tls-subcerts] draft proposes User Agent to send an empty "delegated_credential" extension in its ClientHello. The draft also defines a new "DelegationUsage" extension to X.509. Only presence of this this extension shall permit usage of delegated credentials. The draft advises "clients MUST NOT accept delegated credentials associated with certificates without this extension." The applicability of subcerts in case of CDN would be when a uCDN with a certificate can issue a "delegated credentials" to a dCDN.

5.1. Short-lived certs use case for CDNI - ACME

[I-D.ietf-acme-star] specifies mechanisms to allow a third party such as a CDN to terminate a TLS session on behalf of a content owner (described as domain name owner) The proposal calls for an extension to the ACME protocol to enable the issuance of short term and automatically renewed certificates and a protocol that allows a Domain Name Owner (DNO) to delegate to a third party control over a certificate that bears its own name.

Compared to per session key exchange, it decouples the credentials provisioning from the content delivery to limit the burden on the CSP side. It limits signaling to periodic short term certificate requests (CSR) sent from the uCDN to the content owner:

- As a Bootstrap process, the CDN generates a key-pair and wraps it into a Certificate Signing Request (CSR) according to the agreed CSR template and sends a request over the pre-established LURK channel requests to the DNO. The DNO in turn forwards request over an ACME protocol to an ACME CA to create the corresponding short-term and auto-renewed (STAR) certificate;

- The ACME CA posts the certifcate and notifies the DNO and DNO in turn notifies the CDN which downloads the certificate.

- The connection between CDN and the Origin is mutually authenticated. The additional requests are processed as such as:

Auto-renewal: the ACME CA periodically re-issues the short-term certificate and posts it to a public URL. The CDN would periodically retrieve the certificate

Termination: the DNO (indirectly) stops name delegation by explicitly requesting the ACME CA to discontinue the automatic renewal of the certificate.

CDN and DNO have agreed on a "CSR template" to use, including subject name, Validity, Requested Algorithm, Key length and Key usage.

The ACME issued CA has a short validity (24 hours to 72 hours).

6. Discussions

6.1. LURK

A LURK interface may provide advantages to HTTPS delegation in CDNI such as:

- The origin of the information can be preserved, provided that DNS is used to redirect a UA from the uCDN to a dCDN

- It mitigates the risks of CSP private keys leak by centralizing them.

- It doesn't impact the UA nor TLS stack

- Revocation of delegation may be straightforward by denying any access to private key server

However, preserving UX performances cannot be guaranteed as additional RTT are needed to fetch the needed session credentials from the Key Server.

6.2. OOB

OOB may provide advantages to HTTPS delegation in CDNI such as:

- CDNs can be agnostic of the cached contents; contents can actually remain encrypted on the cache when HTTP encryption encoding [I-D.ietf-httpbis-encryption-encoding] is used, which can be valuable for the Content owner/provider.

- Origin URL stays unchanged in the address bar. So that Origin of information is preserved.

However, the use of OOB to ensure HTTPS delegation in CDNI should be clarified in many cases:

- Origin issue: how to preserve Origin in case of OOB chaining in CDNI?

- How to improve OOB performance in E2E delegation, i.e., from the Origin to dCDN, within a single OOB resource map received by the UA?

- OOB for ensuring E2E delegation would raise delegation issues in certain cases:

1. For instance, an E2E delegation using OOB with DNS redirect would raise a delegation issue where the requested domain doesn't match the URI which may trigger a warning on the UA. As such, delegation is not solved (HARD problem).

The Origin delegates the delivery to uCDN with OOB, next the uCDN delegates HTTPS delivery to a dCDN using DNS.In that case, the UA requests origin that sends back a resource map pointing at uCDN, UA DNS then queries uCDN.com which is resolved to a dCDN server IP, the UA requests contents on dCDN server

2. In another example, an E2E delegation using 302 redirect first and OOB next, would raise a delegation issue where the origin of information is the uCDN, not the Origin.

The Origin delegates HTTPS delivery to uCDN through a 302 redirect, next uCDN delegates HTTPS delivery to dCDN using OOB. In that case, the UA requests Origin who redirects it to the uCDN using 302 HTTP,

then UA requests the uCDN which answers OOB content pointing at dCDN, then UA requests content on dCDN.

Finally, some clarifications about OOB draft are needed:

- How to avoid circular redirection
- Does the UA insert the out-of-band header in any request?
- Does the UA insert the out-of-band header when it requests a resource it selected in a resource map it received in an "out-of-band" response received from the origin?

6.3. Subcerts and SLC

The motivation of [I-D.rescorla-tls-subcerts] draft is to remove dependency between the Origin Server or its surrogates and the CA specifically for enabling the ability to issue credentials (sub-certificates) under the authority of its own certificate and importantly, manage lifetime of the certificates and also have the ability to support any new cryptographic algorithms. The intent for the authors is to give Origin Servers (or their surrogates) operational independence when needing to either limit the life of a certificate or when needing to issue a sub-certificate with limited life. This process may be expeditious over needing to work with the CA for either of the aforementioned changes while still preserving the security and integrity of the content and communications between the origin server or it's and surrogate and the client.

The [I-D.rescorla-tls-subcerts] draft explores several options to allow origin server or its surrogate with capabilities to issue a sub-certificate or delegated credentials with limited authority. The draft also provides for ways where a client controls issuance of sub-certificates. This control can be exerted by the clients by use of an optional "delegated_credential" extension field in the clientHello. The draft also calls out rules for its use, such as, a server cannot unilaterally send this extension but that it can only send credentials when presented by the clientHello message. The draft also defines "DelegationUsage" extension to X.509 that determines use of delegated credentials.

However, as noted in sub-sections, 5.2, the applicability of this draft may be limited in cascaded delegation that is from an up stream CDN to the downstream CDN. Further clarity may be required from the [I-D.rescorla-tls-subcerts] draft authors on ability to cascade sub-certificates.

The [I-D.ietf-acme-star] and the [I-D.rescorla-tls-subcerts] propose approaches where a TLS server, i.e., a uCDN issue certificates or a sub-certificate with limited authority and time without having to share a private key. The approaches avoid any additional infrastructure cost and potential for scaling up the solution. One of the key drawbacks with either approach is additional changes required such as uCDN with content owner and CA for [I-D.ietf-acme-star]. Additionally, a short-lived certificate creation system must be fully automated, as manual renewal of certificates every few days is not practical. An automated system requires require business relations and agreement between the SP and CDN, and an initial setup. In case of [I-D.rescorla-tls-subcerts], the proposal requires changes to TLS handshake where the client provides an extension in its ClientHello that indicates support for this mechanism.

6.4. HTTPS delegation requirements

Generic HTTPS delegations requirements that should be discussed:

- No changes in the client: delegation doesn't impact code on UA side.
- No (or few) impacts on the CSP side: e.g. the load of signaling introduced by the solution should be limited on CSP side
- Preserves the Origin of information: e.g., Origin URL in address bar is preserved.

6.5. Implementation status

At the time being, LURK, OOB and subcerts are in early stage. Currently SLC and subcerts are not available and need to be clarified. However some prototypes already exists for OOB [EricssonOOB].

6.6. E2E HTTPS delegation for CDNs

In order to ensure an end-to-end delegation from the Origin to dCDN, a CDNI HTTPS delegation solution may combine several options described in this document.

- LURK can allow the preservation of Origin of information, and mitigates the risk of private CSP keys leakage. Regarding performance, requesting a key server can lead to an increase in Time To Service (Time to First Page) for UA but does not impact downloading performances.

- OOB allows preserving origin URL while avoiding spreading of private keys on CDN caches, but impacts UA. As far performance is concerned, downloading successive resource maps and direct to the requested resource can increase Time To Service (Time to First Page), but still it does not impact content delivery performance.

- SubCerts: The motivation for sub-certificate (delegated_credential) is to give an option to certificate holder to create a sub-certificate and sign the credentials. The sub-certificate shall have a validity interval with limited scope. On top, the server cannot unilateral present a sub-certificate to the client, instead, client will indicate to the user in clientHello that it will support delegated credentials. The solution obviously requires changes in the client and additional changes to the issuance of certificate. Based upon the draft, it is not clear whether sub-certificates can be cascaded (as noted in section 5.1), that is, once a sub-certificate is issued to an entity and whether it can further use mechanism to issue a sub-certificate to the downstream CDN.

Currently, no single solution fits the cascaded CDNs approach alone. As such, these solutions could be complementary to allow an end-to-end delegation in CDNI. However, the work on these drafts are in progress or in early stages and needs further work to provide an end-to-end solution.

7. IANA Considerations

This document has no IANA considerations.

8. Security Considerations

The entire document is about security.

9. References

9.1. 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>.

9.2. Informative References

[ciscotraffic]
"The Zettabyte Era--Trends and Analysis", 2016, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html]>.

[EricssonOOB]
"Ericsson BC drafts", 2016, <https://github.com/EricssonResearch/Blind-Cache-Drafts>.

[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.ietf-acme-caa]
Landau, H., "CAA Record Extensions for Account URI and ACME Method Binding", draft-ietf-acme-caa-02 (work in progress), June 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.ietf-httpbis-encryption-encoding]
Thomson, M., "Encrypted Content-Encoding for HTTP", draft-ietf-httpbis-encryption-encoding-09 (work in progress), April 2017.

[I-D.mglt-lurk-tls-use-cases]
Migault, D., Ma, K., Salz, R., Mishra, S., and O. Dios, "LURK TLS/DTLS Use Cases", draft-mglt-lurk-tls-use-cases-02 (work in progress), June 2016.

[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-01 (work in progress), March 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