CDNI
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

R. van Brandenburg
Tiledmedia
K. Leung
Cisco Systems, Inc.
P. Sorber
March 5, 2018

URI Signing for CDN Interconnection (CDNI)
draft-ietf-cdni-uri-signing-14

Abstract

This document describes how the concept of URI signing supports the content access control requirements of CDNI and proposes a URI signing method as a JSON Web Token (JWT) [RFC7519] profile.

The proposed URI signing method specifies the information needed to be included in the URI to transmit the signed JWT as well as the claims needed by the signed JWT to authorize a UA. The mechanism described can be used both in CDNI and single CDN scenarios.

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 6, 2018.

Copyright Notice

Copyright (c) 2018 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 (http://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
1.1. Terminology 4
1.2. Background and overview on URI Signing 5
1.3. CDNI URI Signing Overview 6
1.4. URI Signing in a non-CDNI context 8
2. JWT Format and Processing Requirements 9
2.1. JWT Claims 9
2.1.1. Issuer (iss) claim 10
2.1.2. Subject (sub) claim 10
2.1.3. Audience (aud) claim 11
2.1.4. Expiry Time (exp) claim 11
2.1.5. Not Before (nbf) claim 11
2.1.6. Issued At (iat) claim 12
2.1.7. Nonce (jti) claim 12
2.1.8. CDNI Claim Set Version (cdniv) claim 12
2.1.9. Client IP (cdniip) claim 12
2.1.10. CDNI URI Container (cdniuc) claim 13
2.1.11. CDNI Expiration Time Setting (cdniets) claim 13
2.1.12. CDNI Signed Token Transport (cdnistt) claim 13
2.1.13. URI Container Forms 14
2.1.13.1. URI Simple Container (uri:) 14
2.1.13.2. URI Regular Expression Container (uri-regex:) . 14
2.1.13.3. URI Hash Container (uri-hash:) 14
2.2. JWT Header 15
3. URI Signing Token Renewal 15
3.1. Overview 15
3.2. Signed Token Renewal mechanism 16
3.2.1. Required Claims 16
3.3. Communicating a signed JWTs in Signed Token Renewal . . . 16
3.3.1. Support for cross-domain redirection 17
4. Relationship with CDNI Interfaces 17
4.1. CDNI Control Interface 17
4.2. CDNI Footprint & Capabilities Advertisement Interface . . 18
4.3. CDNI Request Routing Redirection Interface 18
4.4. CDNI Metadata Interface 18
4.5. CDNI Logging Interface 19
5. URI Signing Message Flow 21
5.1. HTTP Redirection 21
5.2. DNS Redirection 23
6. IANA Considerations 26

6.1. CDNI Payload Type 26
6.1.1. CDNI UriSigning Payload Type 27
6.2. CDNI Logging Record Type 27
6.2.1. CDNI Logging Record Version 2 for HTTP 27
6.3. CDNI Logging Field Names 27
6.4. CDNI URI Signing Signed Token Transport 28
6.5. JSON Web Token Claims Registration 28
6.5.1. Registry Contents 28
7. Security Considerations 29
8. Privacy 30
9. Acknowledgements 30
10. Contributors 31
11. References 31
11.1. Normative References 31
11.2. Informative References 32
Appendix A. Signed URI Package Example 33
A.1. Simple Example 34
A.2. Complex Example 35
A.3. Signed Token Renewal Example 36
Authors' Addresses 37

1. Introduction

This document describes the concept of URI Signing and how it can be used to provide access authorization in the case of redirection between interconnected CDNs (CDNI) and between a Content Service Provider (CSP) and a CDN. The primary goal of URI Signing is to make sure that only authorized User Agents (UAs) are able to access the content, with a CSP being able to authorize every individual request. It should be noted that URI Signing is not a content protection scheme; if a CSP wants to protect the content itself, other mechanisms, such as Digital Rights Management (DRM), are more appropriate. In addition to access control, URI Signing also has benefits in reducing the impact of denial-of-service attacks.

The overall problem space for CDN Interconnection (CDNI) is described in CDNI Problem Statement [RFC6707]. This document, along with the CDNI Requirements [RFC7337] document and the CDNI Framework [RFC7336], describes the need for interconnected CDNs to be able to implement an access control mechanism that enforces the CSP's distribution policy.

Specifically, CDNI Framework [RFC7336] states:

> The CSP may also trust the CDN operator to perform actions such as ..., and to enforce per-request authorization performed by the CSP using techniques such as URI signing.

In particular, the following requirement is listed in CDNI Requirements [RFC7337]:

> MI-16 {HIGH} The CDNI Metadata interface shall allow signaling of authorization checks and validation that are to be performed by the Surrogate before delivery. For example, this could potentially include the need to validate information (e.g., Expiry time, Client IP address) required for access authorization.

This document proposes a method of signing URIs that allows Surrogates in interconnected CDNs to enforce a per-request authorization performed by the CSP. Splitting the role of performing per-request authorization by the CSP and the role of validating this authorization by the CDN allows any arbitrary distribution policy to be enforced across CDNs without the need of CDNs to have any awareness of the actual CSP distribution policy.

The representation of this method is a Signed JSON Web Token (JWT) [RFC7519].

1.1. 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 the terminology defined in CDNI Problem Statement [RFC6707].

This document also uses the terminology of JSON Web Token (JWT) [RFC7519].

In addition, the following terms are used throughout this document:

- Signed URI: A URI for which a signed JWT is provided.
- Target CDN URI: URI created by the CSP to direct a UA towards the Upstream CDN (uCDN). The Target CDN URI can be signed by the CSP and verified by the uCDN and possibly further Downstream CDNs (dCDNs).
- Redirection URI: URI created by the uCDN to redirect a UA towards the dCDN. The Redirection URI can be signed by the uCDN and verified by the dCDN. In a cascaded CDNI scenario, there can be more than one Redirection URI.

- Signed Token Renewal: A series of signed JWTs that are used for subsequent access to a set of related resources in a CDN, such as a set of HTTP Adaptive Streaming files. Every time a signed JWT is used to access a particular resource, a new signed JWT is sent along with the resource that can be used to request the next resource in the set. When generating a new signed JWT in Signed Token Renewal, parameters are carried over from one signed JWT to the next.

1.2. Background and overview on URI Signing

A CSP and CDN are assumed to have a trust relationship that enables the CSP to authorize access to a content item by including a set of claims in the form of a signed JWT in the URI before redirecting a UA to the CDN. Using these attributes, it is possible for a CDN to check an incoming content request to see whether it was authorized by the CSP (e.g., based on the UA's IP address or a time window). To prevent the UA from altering the claims a signed JWT is REQUIRED.

Figure 1, shown below, presents an overview of the URI Signing mechanism in the case of a CSP with a single CDN. When the UA browses for content on CSP's website (#1), it receives HTML web pages with embedded content URIs. Upon requesting these URIs, the CSP redirects to a CDN, creating a Target CDN URI (#2) (alternatively, the Target CDN URI itself is embedded in the HTML). The Target CDN URI is the Signed URI which may include the IP address of the UA and/or a time window and always contains the signed JWT which is generated by the CSP using a shared secret or private key. Once the UA receives the response with the Signed URI, it sends a new HTTP request using the Signed URI to the CDN (#3). Upon receiving the request, the CDN checks to see if the Signed URI is authentic by verifying the signed JWT. If applicable, it checks whether the IP address of the HTTP request matches that in the Signed URI and if the time window is still valid. After these claims are confirmed to be valid, the CDN delivers the content (#4).

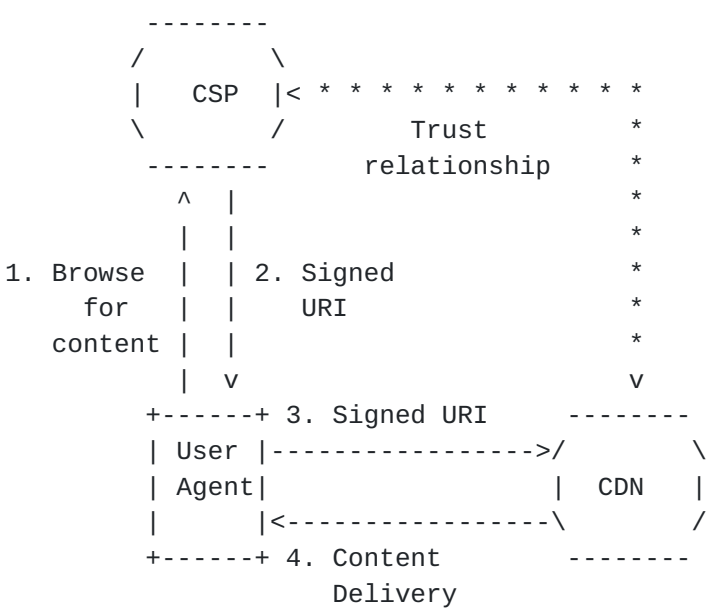
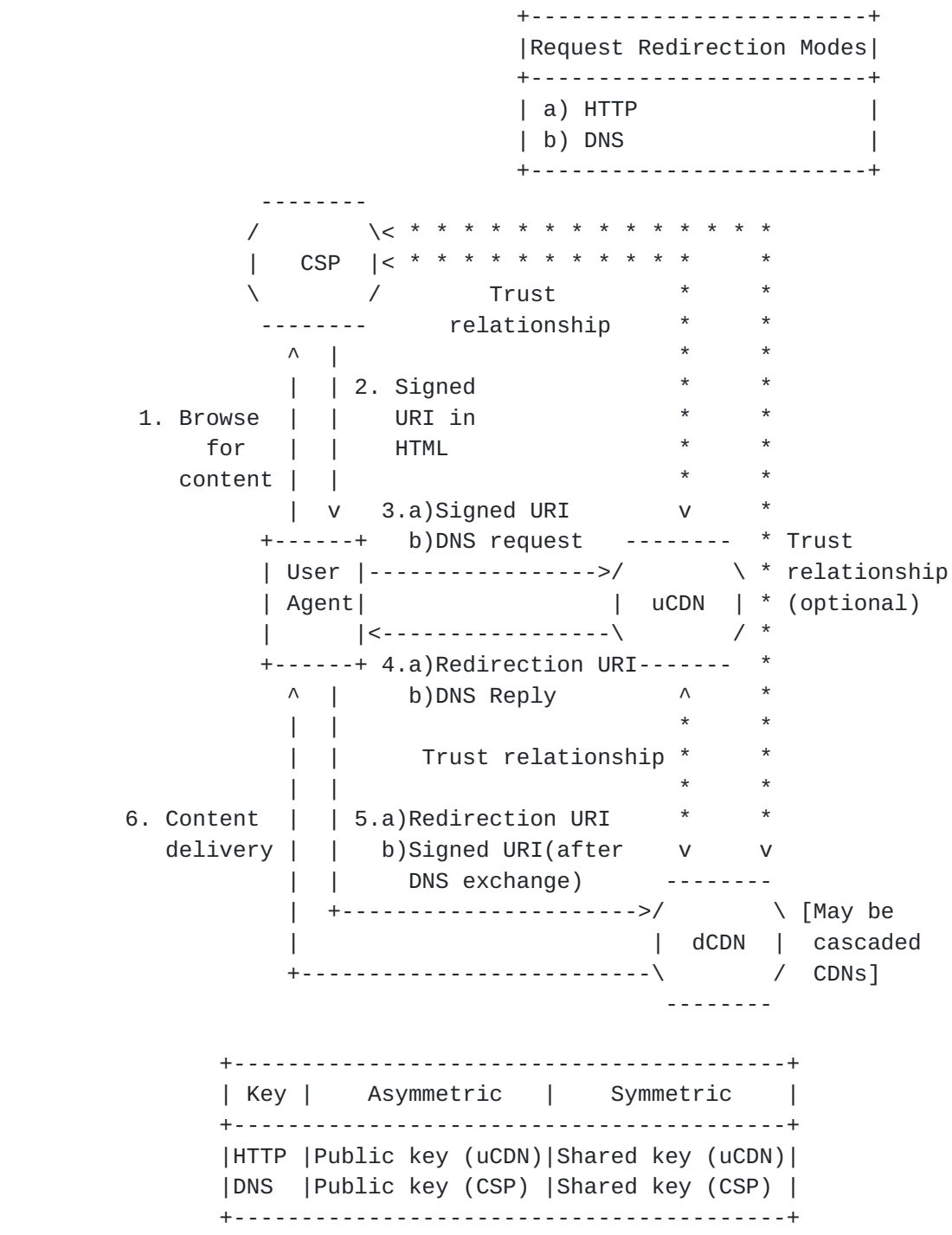


Figure 1: Figure 1: URI Signing in a CDN Environment

1.3. CDNI URI Signing Overview

In a CDNI environment, URI Signing operates the same way in the initial steps #1 and #2 but the later steps involve multiple CDNs in the process of delivering the content. The main difference from the single CDN case is a redirection step between the uCDN and the dCDN. In step #3, UA may send an HTTP request or a DNS request. Depending on whether HTTP-based or DNS-based request routing is used, the uCDN responds by directing the UA towards the dCDN using either a Redirection URI (which is a Signed URI generated by the uCDN) or a DNS reply, respectively (#4). Once the UA receives the response, it sends the Redirection URI/Target CDN URI to the dCDN (#5). The received URI is validated by the dCDN before delivering the content (#6). This is depicted in the figure below. Note: The CDNI call flows are covered in Detailed URI Signing Operation (Section 5).



Key	Asymmetric	Symmetric
HTTP	Public key (uCDN)	Shared key (uCDN)
DNS	Public key (CSP)	Shared key (CSP)

Figure 2: URI Signing in a CDNI Environment

The trust relationships between CSP, uCDN, and dCDN have direct implications for URI Signing. In the case shown in Figure 2, the CDN that the CSP has a trust relationship with is the uCDN. The delivery of the content may be delegated to the dCDN, which has a relationship with the uCDN but may have no relationship with the CSP.

In CDNI, there are two methods for request routing: DNS-based and HTTP-based. For DNS-based request routing, the Signed URI (i.e., Target CDN URI) provided by the CSP reaches the dCDN directly. In the case where the dCDN does not have a trust relationship with the CSP, this means that either an asymmetric public/private key method needs to be used for computing the signed JWT (because the CSP and dCDN are not able to exchange symmetric shared secret keys), or the CSP needs to allow the uCDN to redistribute shared keys to a subset of their dCDNs.

For HTTP-based request routing, the Signed URI (i.e., Target CDN URI) provided by the CSP reaches the uCDN. After this URI has been verified to be correct by the uCDN, the uCDN creates and signs a new Redirection URI to redirect the UA to the dCDN. Since this new URI could have a new signed JWT, a new signature can be based around the trust relationship between the uCDN and dCDN, and the relationship between the dCDN and CSP is not relevant. Given the fact that such a relationship between uCDN and dCDN always exists, both asymmetric public/private keys and symmetric shared secret keys can be used for URI Signing with HTTP-based request routing. Note that the signed Redirection URI MUST maintain the same, or higher, level of security as the original Signed URI.

Two types of keys can be used for URI Signing: asymmetric keys and symmetric keys. Asymmetric keys are based on a public/private key pair mechanism and always contain a private key only known to the entity signing the URI (either CSP or uCDN) and a public key for the verification of the Signed URI. With symmetric keys, the same key is used by both the signing entity for signing the URI as well as by the validating entity for validating the Signed URI. Regardless of the type of keys used, the validating entity has to obtain the key (either the public or the symmetric key). There are very different requirements for key distribution (out of scope of this document) with asymmetric keys and with symmetric keys. Key distribution for symmetric keys requires confidentiality to prevent another party from getting access to the key, since it could then generate valid Signed URIs for unauthorized requests. Key distribution for asymmetric keys does not require confidentiality since public keys can typically be distributed openly (because they cannot be used for URI signing) and private keys are kept by the URI signing function.

1.4. URI Signing in a non-CDNI context

While the URI signing method defined in this document was primarily created for the purpose of allowing URI Signing in CDNI scenarios, e.g., between a uCDN and a dCDN or between a CSP and a dCDN, there is nothing in the defined URI Signing method that precludes it from being used in a non-CDNI context. As such, the described mechanism

could be used in a single-CDN scenario such as shown in Figure 1 in Section 1.2, for example to allow a CSP that uses different CDNs to only have to implement a single URI Signing mechanism.

2. JWT Format and Processing Requirements

The concept behind URI Signing is based on embedding a signed JSON Web Token (JWT) [RFC7519] in the UA request: The signed JWT contains a number of claims that can be validated to ensure the UA has legitimate access to the content.

This document specifies the following attribute for embedding a signed JWT in a Target CDN URI or Redirection URI:

- URI Signing Package (URISigningPackage): The URI attribute that encapsulates all the URI Signing claims in a signed JWT encoded format. This attribute is exposed in the Signed URI as a URI query parameter or as a URL path parameter.

The parameter name of the URI Signing Package Attribute is defined in the CDNI Metadata (Section 4.4). If the CDNI Metadata interface is not used, or does not include a parameter name for the URI Signing Package Attribute, the parameter name can be set by configuration (out of scope of this document).

The URI Signing Package will be found by searching the URI, left-to-right, for the following sequence:

- a reserved character (as defined in [RFC3986] Section 2.2),
- the URI Signing Package Attribute name,
- if the last character of the URI Singing Package Attribute name is not a reserved character, an equal symbol ('='),
- and a sequence of non-reserved characters that will be interpreted as a signed JWT,
- terminated by either a reserved character or the end of the URI.

The first such match will be taken to provide the signed JWT; the URI will not be searched for multiple signed JWTs.

2.1. JWT Claims

This section identifies the set of claims that can be used to enforce the CSP distribution policy. New claims can be introduced in the future to extend the distribution policy capabilities.

In order to provide distribution policy flexibility, the exact subset of claims used in a given signed JWT is a runtime decision. Claim requirements are defined in the CDNI Metadata (Section 4.4) If the CDNI Metadata interface is not used, or does not include claim requirements, the claim requirements can be set by configuration (out of scope of this document).

The following claims (where the "JSON Web Token Claims" registry claim name is specified in parenthesis below) are used to enforce the distribution policies. All of the listed claims are mandatory to implement in a URI Signing implementation, but are not mandatory to use in a given signed JWT. (The "optional" and "mandatory" identifiers in square brackets refer to whether or not a given claim MUST be present in a URI Signing JWT.) A CDN MUST be able to parse and process all of the claims listed below. If the signed JWT contains any other claims which the CDN does not understand (i.e., is unable to parse and process), the CDN MUST reject the request.

Note: See the Security Considerations (Section 7) section on the limitations of using an expiration time and client IP address for distribution policy enforcement.

2.1.1. Issuer (iss) claim

Issuer (iss) [optional] - The semantics in [RFC7519] Section 4.1.1 MUST be followed. This claim MAY be used to validate authorization of the issuer of a signed JWT and also MAY be used to confirm that the indicated key was provided by said issuer. If the CDN validating the signed JWT does not support Issuer validation, or if the Issuer in the signed JWT does not match the list of known acceptable Issuers, the CDN MUST reject the request. If the received signed JWT contains an Issuer claim, then any JWT subsequently generated for CDNI redirection MUST also contain an Issuer claim, and the Issuer value MUST be updated to identify the redirecting CDN. If the received signed JWT does not contain an Issuer claim, an Issuer claim MAY be added to a signed JWT generated for CDNI redirection.

2.1.2. Subject (sub) claim

Subject (sub) [optional] - The semantics in [RFC7519] Section 4.1.2 MUST be followed. If this claim is used, it MUST be a JSON Web Encryption (JWE [RFC7516]) Object in compact serialization form, because it contains personally identifiable information. This claim contains information about the subject (for example, a user or an agent) that MAY be used to validate the signed JWT. If the received signed JWT contains a Subject claim, then any JWT subsequently generated for CDNI redirection MUST also contain a Subject claim, and the Subject value MUST be the same as in the received signed JWT. A

signed JWT generated for CDNI redirection MUST NOT add a Subject claim if no Subject claim existed in the received signed JWT.

2.1.3. Audience (aud) claim

Audience (aud) [optional] - The semantics in [RFC7519] Section 4.1.3 MUST be followed. This claim is used to ensure that the CDN that validates the JWT identifies itself with the value in this claim.

2.1.4. Expiry Time (exp) claim

Expiry Time (exp) [optional] - The semantics in [RFC7519] Section 4.1.4 MUST be followed, though URI Signing implementations MUST NOT allow for any time synchronization "leeway". Note: The time on the entities that generate and validate the signed URI SHOULD be in sync. In the CDNI case, this means that CSP, uCDN, and dCDN servers need to be time-synchronized. It is RECOMMENDED to use NTP [RFC5905] for time synchronization. If the CDN validating the signed JWT does not support Expiry Time validation, or if the Expiry Time in the signed JWT corresponds to a time earlier than the time of the content request, the CDN MUST reject the request. If the received signed JWT contains a Expiry Time claim, then any JWT subsequently generated for CDNI redirection MUST also contain an Expiry Time claim, and the Expiry Time value MUST be the same as in the received signed JWT. A signed JWT generated for CDNI redirection MUST NOT add an Expiry Time claim if no Expiry Time claim existed in the received signed JWT.

2.1.5. Not Before (nbf) claim

Not Before (nbf) [optional] - The semantics in [RFC7519] Section 4.1.5 MUST be followed, though URI Signing implementations MUST NOT allow for any time synchronization "leeway". Note: The time on the entities that generate and validate the signed URI SHOULD be in sync. In the CDNI case, this means that the CSP, uCDN, and dCDN servers need to be time-synchronized. It is RECOMMENDED to use NTP [RFC5905] for time synchronization. If the CDN validating the signed JWT does not support Not Before time validation, or if the Not Before time in the signed JWT corresponds to a time later than the time of the content request, the CDN MUST reject the request. If the received signed JWT contains a Not Before time claim, then any JWT subsequently generated for CDNI redirection MUST also contain a Not Before time claim, and the Not Before time value MUST be the same as in the received signed JWT. A signed JWT generated for CDNI redirection MUST NOT add a Not Before time claim if no Not Before time claim existed in the received signed JWT.

2.1.6. Issued At (iat) claim

Issued At (iat) [optional] - The semantics in [RFC7519] Section 4.1.6 MUST be followed. Note: The time on the entities that generate and validate the signed URI SHOULD be in sync. In the CDNI case, this means that CSP, uCDN, and dCDN servers need to be time-synchronized. It is RECOMMENDED to use NTP [RFC5905] for time synchronization. If the received signed JWT contains an Issued At claim, then any JWT subsequently generated for CDNI redirection MUST also contain an Issued At claim, and the Issuer value MUST be updated to identify the time the new JWT was generated. If the received signed JWT does not contain an Issued At claim, an Issued At claim MAY be added to a signed JWT generated for CDNI redirection.

2.1.7. Nonce (jti) claim

Nonce (jti) [optional] - The semantics in [RFC7519] Section 4.1.7 MUST be followed. A Nonce can be used to prevent replay attacks if the CDN stores a list of all previously used Nonce values, and validates that the Nonce in the current JWT has never been used before. If the signed JWT contains a Nonce claim and the CDN validating the signed JWT does not support Nonce storage, then the CDN MUST reject the request. If the received signed JWT contains a Nonce claim, then any JWT subsequently generated for CDNI redirection MUST also contain a Nonce claim, and the Nonce value MUST be the same as in the received signed JWT. If the received signed JWT does not contain a Nonce claim, a Nonce claim MUST NOT be added to a signed JWT generated for CDNI redirection.

2.1.8. CDNI Claim Set Version (cdniv) claim

CDNI Claim Set Version (cdniv) [optional] - The CDNI Claim Set Version (cdniv) claim provides a means within a signed JWT to tie the claim set to a specific version of a specificiation. This is intended to allow changes in and facilitate upgrades across specifications. The type is JSON integer and the value MUST be set to "1", for this version of the specification. In the absence of this claim, the value is assumed to be "1". For future versions this claim will be mandatory. Implementations MUST reject signed JWTs with unsupported CDNI Claim Set versions.

2.1.9. Client IP (cdniip) claim

Client IP (cdniip) [optional] IP address, or IP prefix, for which the Signed URI is valid. This is represented in CIDR notation, with dotted decimal format for IPv4 or canonical text representation for IPv6 addresses [RFC5952]. The request is rejected if sourced from a client outside of the specified IP range. Since the client IP is

considered personally identifiable information this field MUST be a JSON Web Encryption (JWE [RFC7516]) Object in compact serialization form. If the CDN validating the signed JWT does not support Client IP validation, or if the Client IP in the signed JWT does not match the source IP address in the content request, the CDN MUST reject the request. The type of this claim is a JSON string that contains the JWE. If the received signed JWT contains a Client IP claim, then any JWT subsequently generated for CDNI redirection MUST also contain a Client IP claim, and the Client IP value MUST be the same as in the received signed JWT. A signed JWT generated for CDNI redirection MUST NOT add a Client IP claim if no Client IP claim existed in the received signed JWT.

2.1.10. CDNI URI Container (cdniuc) claim

URI Container (cdniuc) [optional] - Container for holding the URI representation before a URI Signing Package is added. This representation can take one of several forms detailed in Section 2.1.13. If the URI regex in the signed JWT does not match the URI of the content request, the CDN validating the signed JWT MUST reject the request. When comparing the URI, the percent encoded form as defined in [RFC3986] Section 2.1 MUST be used. When redirecting a URI, the CDN generating the new signed JWT MAY change the URI Container to comport with the URI being used in the redirection.

2.1.11. CDNI Expiration Time Setting (cdniets) claim

CDNI Expiration Time Setting (cdniets) [optional] - The CDNI Expiration Time Setting (cdniets) claim provides a means for setting the value of the Expiry Time (exp) claim when generating a subsequent signed JWT in Signed Token Renewal. Its type is a JSON numeric value. It denotes the number of seconds to be added to the time at which the JWT is validated that gives the value of the Expiry Time (exp) claim of the next signed JWT. The CDNI Expiration Time Setting (cdniets) SHOULD NOT be used when not using Signed Token Renewal and MUST be present when using Signed Token Renewal.

2.1.12. CDNI Signed Token Transport (cdnistt) claim

CDNI Signed Token Transport (cdnistt) [optional] - The CDNI Signed Token Transport (cdnistt) claim provides a means of signalling the method through which a new signed JWT is transported from the CDN to the UA and vice versa for the purpose of Signed Token Renewal. Its type is a JSON integer. Values for this claim can be defined in Section 6.4. If using this claim you MUST also specify a CDNI Expiration Time Setting (cdniets) as noted above.

2.1.13. URI Container Forms

The URI Container (cdniuc) claim takes one of the following forms. More forms may be added in the future to extend the capabilities.

Before comparing a URI against this container, the signed JWT must be removed from the URI. This removal is only for the purpose of determining if the URI matches; all other purposes will use the original URI. If the signed JWT is terminated by anything other than a sub-delimiter (as defined in [RFC3986] Section 2.2), everything from the reserved character (as defined in [RFC3986] Section 2.2) that precedes the URI Signing Package Attribute to the last character of the signed JWT will be removed, inclusive. Otherwise, everything from the first character of the URI Signing Package Attribute to the sub-delimiter that terminates the signed JWT will be removed, inclusive.

2.1.13.1. URI Simple Container (uri:)

When prefixed with 'uri:', the string following 'uri:' is the URI that MUST be matched with a simple string match to the requested URI.

2.1.13.2. URI Regular Expression Container (uri-regex:)

Prefixed with 'uri-regex:', this string is any PCRE [PCRE839] compatible regular expression used to match against the requested URI.

Note: Because '\' has special meaning in JSON [RFC7159] as the escape character within JSON strings, the regular expression character '\' MUST be escaped as '\\'.

An example of a 'uri-regex:' is the following:

```
[^:]*\\://[^/]*/folder/content/quality_[^/]*/segment.{3}\\.mp4(\?.*)?
```

Note: Due to computational complexity of executing arbitrary regular expressions, it is RECOMMENDED to only execute after validating the JWT to ensure its authenticity.

2.1.13.3. URI Hash Container (uri-hash:)

Prefixed with 'uri-hash:', this string is a URL Segment form ([RFC6920] Section 5) of the URI.

2.2. JWT Header

The header of the JWT MAY be passed via the CDNI Metadata interface instead of being included in the URISigningPackage. The header value must be transmitted in the serialized encoded form and prepended to the JWT payload and signature passed in the URISigningPackage prior to validation. This reduces the size of the signed JWT token.

3. URI Signing Token Renewal

3.1. Overview

For content that is delivered via HTTP in a segmented fashion, such as MPEG-DASH [MPEG-DASH] or HTTP Live Streaming (HLS) [RFC8216], special provisions need to be made in order to ensure URI Signing can be applied. In general, segmented protocols work by breaking large objects (e.g. videos) into a sequence of small independent segments. Such segments are then referenced by a separate manifest file, which either includes a list of URLs to the segments or specifies an algorithm through which a User Agent can construct the URLs to the segments. Requests for segments therefore originate from the manifest file and, unless the URLs in the manifest file point to the CSP, are not subjected to redirection and URI Signing. This opens up the vulnerability of malicious User Agents sharing the manifest file and deep-linking to the segments.

One method for dealing with this vulnerability would be to include, in the manifest itself, Signed URIs that point to the individual segments. There exist a number of issues with that approach. First, it requires the CDN delivering the manifest to rewrite the manifest file for each User Agent, which would require the CDN to be aware of the exact segmentation protocol used. Secondly, it could also require the expiration time of the Signed URIs to be valid for an extended duration if the content described by the manifest is meant to be consumed in real time. For instance, if the manifest file were to contain a segmented video stream of more than 30 minutes in length, Signed URIs would require to be valid for a at least 30 minutes, thereby reducing their effectiveness and that of the URI Signing mechanism in general. For a more detailed analysis of how segmented protocols such as HTTP Adaptive Streaming protocols affect CDNI, see Models for HTTP-Adaptive-Streaming-Aware CDNI [RFC6983].

The method described in this section allows CDNs to use URI Signing for segmented content without having to include the Signed URIs in the manifest files themselves.

3.2. Signed Token Renewal mechanism

In order to allow for effective access control of segmented content, the URI signing scheme defined in this section is based on a mechanism through which subsequent segment requests can be linked together. As part of the JWT validation procedure, the CDN can generate a new signed JWT that the UA can use to do a subsequent request. More specifically, whenever a UA successfully retrieves a segment, it receives, in the HTTP 2xx Successful message, a signed JWT that it can use whenever it requests the next segment. As long as each successive signed JWT is correctly validated before a new one is generated, the model is not broken and the User Agent can successfully retrieve additional segments. Given the fact that with segmented protocols, it is usually not possible to determine a priori which segment will be requested next (i.e., to allow for seeking within the content and for switching to a different representation), the Signed Token Renewal uses the URI Regular Expression Container scoping mechanisms in the URI Container (cdniuc) claim to allow a signed JWT to be valid for more than one URL.

In order for this renewal of signed JWTs to work, it is necessary for a UA to extract the signed JWT from the HTTP 2xx Successful message of an earlier request and use it to retrieve the next segment. The exact mechanism by which the client does this depends on the exact segmented protocol and since this document is only concerned with the generation and validation of incoming request, this process is outside the scope of this document. However, in order to also support legacy UAs that do not include any specific provisions for the handling of signed JWTs, the folowing section defines a mechanism using HTTP Cookies that allows such UAs to support the concept of renewing signed JWTs without requiring any support on the UA side.

3.2.1. Required Claims

The cdnistt claim (Section 2.1.12) and cdniets claim (Section 2.1.11) MUST both be present to utilize Signed token Renewal. Either one MUST NOT appear alone. You MAY set cdnistt to a value of '0' to mean no Signed Token Renewal, but you still MUST have a corresponding cdniets that validates as a JSON number. However, if you do not want to use Signed Token Renewal, it is RECOMMENDED to simply omit both.

3.3. Communicating a signed JWTs in Signed Token Renewal

This section assumes the value of the CDNI Signed Token Transport (cdnistt) claim has been set to 1. Other values of cdnistt are out of scope of this document.

When using the Signed Token Renewal mechanism, the signed JWT is transported to the UA via a 'URISigningPackage' cookie added to the HTTP 2xx Successful message along with the content being returned to the UA, or to the HTTP 3xx Redirection message in case the UA is redirected to a different server.

3.3.1. Support for cross-domain redirection

For security purposes, the use of cross-domain cookies is not supported in some application environments. As a result, the Cookie-based method for transport of the Signed Token described in the previous section might break if used in combination with a HTTP 3xx Redirection response where the target URL is in a different domain. In such scenarios, Signed Token Renewal of a signed JWT SHOULD be communicated via the query string instead, in a similar fashion to how regular signed JWTs (outside of Signed Token Renewal) are communicated. Note that the use of URL embedded signed JWTs SHOULD NOT be used in HTTP 2xx Successful messages, since UAs might not know how to extract the signed JWTs.

Note that the process described below only works in cases where both the manifest file and segments constituting the segmented content are delivered from the same domain. In other words, any redirection between different domains needs to be carried out while retrieving the manifest file.

4. Relationship with CDNI Interfaces

Some of the CDNI Interfaces need enhancements to support URI Signing. As an example: A dCDN that supports URI Signing needs to be able to advertise this capability to the uCDN. The uCDN needs to select a dCDN based on such capability when the CSP requires access control to enforce its distribution policy via URI Signing. Also, the uCDN needs to be able to distribute via the CDNI Metadata interface the information necessary to allow the dCDN to validate a Signed URI. Events that pertain to URI Signing (e.g., request denial or delivery after access authorization) need to be included in the logs communicated through the CDNI Logging interface (Editor's Note: Is this within the scope of the CDNI Logging interface?).

4.1. CDNI Control Interface

URI Signing has no impact on this interface.

4.2. CDNI Footprint & Capabilities Advertisement Interface

The CDNI Request Routing: Footprint and Capabilities Semantics document [RFC8008] defines support for advertising CDNI Metadata capabilities, via CDNI Payload Type. The CDNI Payload Type registered in Section 6.1 can be used for capability advertisement.

4.3. CDNI Request Routing Redirection Interface

The CDNI Request Routing Redirection Interface [RFC7975] describes the recursive request redirection method. For URI Signing, the uCDN signs the URI provided by the dCDN. URI Signing therefore has has no impact on this interface.

4.4. CDNI Metadata Interface

The CDNI Metadata Interface [RFC8006] describes the CDNI metadata distribution needed to enable content acquisition and delivery. For URI Signing, a new CDNI metadata object is specified.

The UriSigning Metadata object contains information to enable URI signing and validation by a dCDN. The UriSigning properties are defined below.

Property: enforce

Description: URI Signing enforcement flag. Specifically, this flag indicates if the access to content is subject to URI Signing. URI Signing requires the dCDN to ensure that the URI must be signed and validated before delivering content. Otherwise, the dCDN does not perform validation, regardless of whether or not the URI is signed.

Type: Boolean

Mandatory-to-Specify: No. The default is true.

Property: issuers

Description: A list of valid Issuers against which the Issuer claim in the signed JWT may be validated.

Type: Array of Strings

Mandatory-to-Specify: No. The default is an empty list. An empty list means that any Issuer is acceptable.

Property: package-attribute

Description: The name to use for the URI Signing Package.

Type: String

Mandatory-to-Specify: No. Default is "URISigningPackage".

Property: jwt-header

Description: The header part of JWT that is used for generating or validating a signed JWT when the JWT token in the URI Signing Package does not contain a header part.

Type: String

Mandatory-to-Specify: No. A jwt-header is not essential for all implementations of URI signing.

The following is an example of a URI Signing metadata payload with all default values:

```
{
  "generic-metadata-type": "MI.UriSigning"
  "generic-metadata-value": {}
}
```

The following is an example of a URI Signing metadata payload with explicit values:

```
{
  "generic-metadata-type": "MI.UriSigning"
  "generic-metadata-value":
    {
      "enforce": true,
      "issuers": ["csp", "ucdn1", "ucdn2"],
      "package-attribute": "usp"
    }
}
```

4.5. CDNI Logging Interface

For URI Signing, the dCDN reports that enforcement of the access control was applied to the request for content delivery. When the request is denied due to enforcement of URI Signing, the reason is logged.

The following CDNI Logging field for URI Signing SHOULD be supported in the HTTP Request Logging Record as specified in CDNI Logging Interface [RFC7937], using the new "cdni_http_request_v2" record-type registered in Section 6.2.1.

- s-uri-signing (mandatory):
  - format: 3DIGIT
  - field value: this characterises the URI signing validation performed by the Surrogate on the request. The allowed values are:
    - "000" : no signed JWT validation performed
    - "200" : signed JWT validation performed and validated
    - "400" : signed JWT validation performed and rejected because of incorrect signature
    - "401" : signed JWT validation performed and rejected because of Expiration Time enforcement
    - "402" : signed JWT validation performed and rejected because of Client IP enforcement
    - "403" : signed JWT validation performed and rejected because of URI Regular Expression enforcement
    - "404" : signed JWT validation performed and rejected because of Issuer enforcement
    - "405" : signed JWT validation performed and rejected because of Not Before enforcement
    - "500" : unable to perform signed JWT validation because of malformed URI
  - occurrence: there MUST be zero or exactly one instance of this field.
- s-uri-signing-deny-reason (optional):
  - format: QSTRING
  - field value: a string for providing further information in case the signed JWT was rejected, e.g., for debugging purposes.

* occurrence: there MUST be zero or exactly one instance of this field.

5. URI Signing Message Flow

URI Signing supports both HTTP-based and DNS-based request routing. JSON Web Token (JWT) [RFC7519] defines a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a signed JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

5.1. HTTP Redirection

For HTTP-based request routing, a set of information that is unique to a given end user content request is included in a signed JWT, using key information that is specific to a pair of adjacent CDNI hops (e.g., between the CSP and the uCDN or between the uCDN and a dCDN). This allows a CDNI hop to ascertain the authenticity of a given request received from a previous CDNI hop.

The URI signing method described below is based on the following steps (assuming HTTP redirection, iterative request routing, and a CDN path with two CDNs). Note that uCDN and uCDN are used exchangeably.

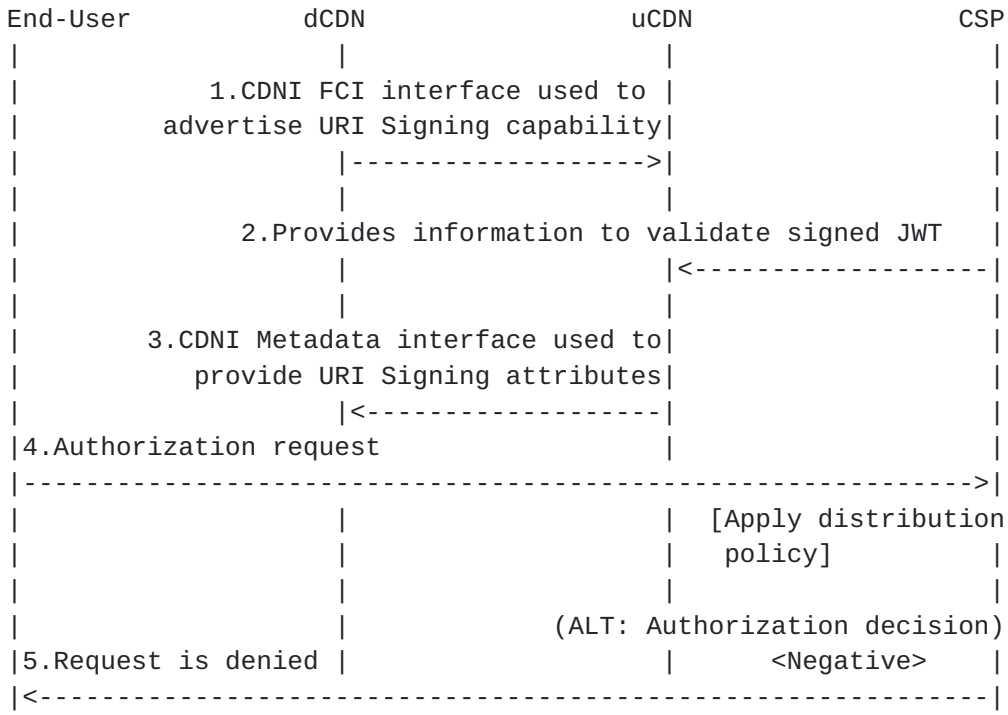




Figure 3: HTTP-based Request Routing with URI Signing

1. Using the CDNI Footprint & Capabilities Advertisement interface, the dCDN advertises its capabilities including URI Signing support to the uCDN.

2. CSP provides to the uCDN the information needed to validate signed JWTs from that CSP. For example, this information may include a key value.

3. Using the CDNI Metadata interface, the uCDN communicates to a dCDN the information needed to validate signed JWTs from the uCDN for the given CSP. For example, this information may include the URI query string parameter name for the URI Signing Package Attribute.

4. When a UA requests a piece of protected content from the CSP, the CSP makes a specific authorization decision for this unique request based on its personal distribution policy.

5. If the authorization decision is negative, the CSP rejects the request and sends an error code (e.g., 403 Forbidden) in the HTTP response.

6. If the authorization decision is positive, the CSP computes a Signed URI that is based on unique parameters of that request and conveys it to the end user as the URI to use to request the content.

7. On receipt of the corresponding content request, the uCDN validates the signed JWT in the URI using the information provided by the CSP.

8. If the validation is negative, the uCDN rejects the request and sends an error code (e.g., 403 Forbidden) in the HTTP response.

9. If the validation is positive, the uCDN computes a Signed URI that is based on unique parameters of that request and provides it to the end user as the URI to use to further request the content from the dCDN.

10. On receipt of the corresponding content request, the dCDN validates the signed JWT in the Signed URI using the information provided by the uCDN in the CDNI Metadata.

11. If the validation is negative, the dCDN rejects the request and sends an error code (e.g., 403 Forbidden) in the HTTP response.

12. If the validation is positive, the dCDN serves the request and delivers the content.

13. At a later time, the dCDN reports logging events that include URI signing information.

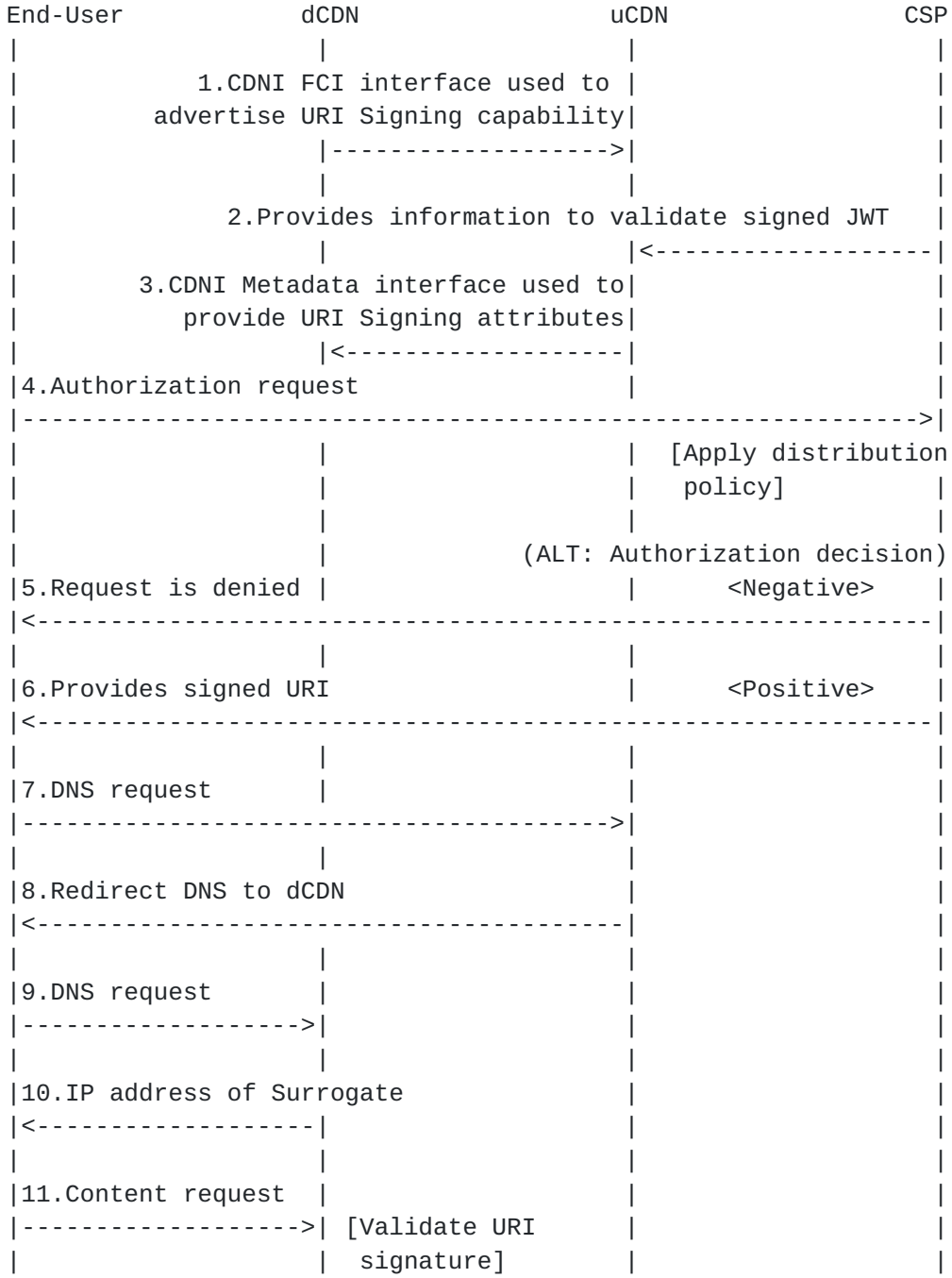
With HTTP-based request routing, URI Signing matches well the general chain of trust model of CDNI both with symmetric and asymmetric keys because the key information only needs to be specific to a pair of adjacent CDNI hops.

5.2. DNS Redirection

For DNS-based request routing, the CSP and uCDN must agree on a trust model appropriate to the security requirements of the CSP's particular content. Use of asymmetric public/private keys allows for

unlimited distribution of the public key to dCDNs. However, if a shared secret key is preferred, then the CSP may want to restrict the distribution of the key to a (possibly empty) subset of trusted dCDNs. Authorized Delivery CDNs need to obtain the key information to validate the Signed URI.

The URI signing method described below is based on the following steps (assuming iterative DNS request routing and a CDN path with two CDNs).



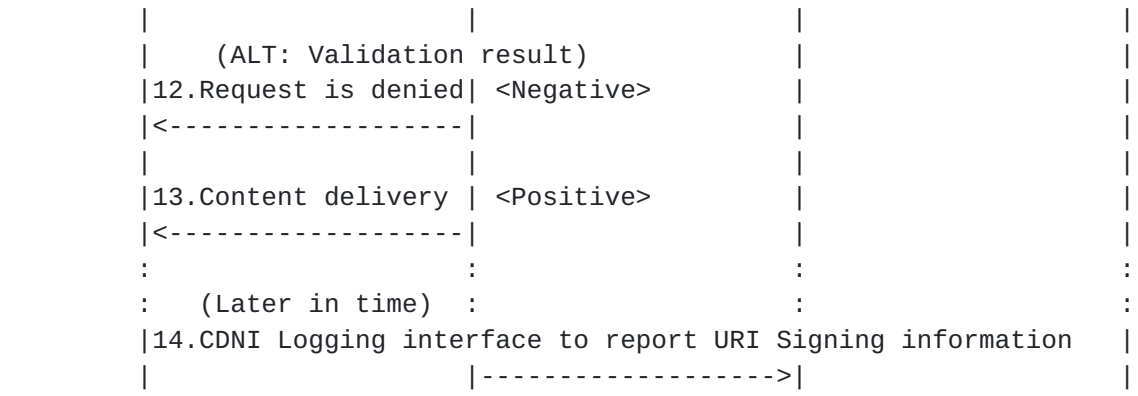


Figure 4: DNS-based Request Routing with URI Signing

1. Using the CDNI Footprint & Capabilities Advertisement interface, the dCDN advertises its capabilities including URI Signing support to the uCDN.

2. CSP provides to the uCDN the information needed to validate cryptographic signatures from that CSP. For example, this information may include a key.

3. Using the CDNI Metadata interface, the uCDN communicates to a dCDN the information needed to validate cryptographic signatures from the CSP (e.g., the URI query string parameter name for the URI Signing Package Attribute). In the case of symmetric key, the uCDN checks if the dCDN is allowed by CSP to obtain the shared secret key.

4. When a UA requests a piece of protected content from the CSP, the CSP makes a specific authorization decision for this unique request based on its arbitrary distribution policy.

5. If the authorization decision is negative, the CSP rejects the request.

6. If the authorization decision is positive, the CSP computes a cryptographic signature that is based on unique parameters of that request and includes it in the URI provided to the end user to request the content.

7. End user sends DNS request to the uCDN.

8. On receipt of the DNS request, the uCDN redirects the request to the dCDN.

9. End user sends DNS request to the dCDN.

10. On receipt of the DNS request, the dCDN responds with IP address of one of its Surrogates.

11. On receipt of the corresponding content request, the dCDN validates the cryptographic signature in the URI using the information provided by the uCDN in the CDNI Metadata.

12. If the validation is negative, the dCDN rejects the request and sends an error code (e.g., 403) in the HTTP response.

13. If the validation is positive, the dCDN serves the request and delivers the content.

14. At a later time, dCDN reports logging events that includes URI signing information.

With DNS-based request routing, URI Signing matches well the general chain of trust model of CDNI when used with asymmetric keys because the only key information that needs to be distributed across multiple, possibly untrusted, CDNI hops is the public key, which is generally not confidential.

With DNS-based request routing, URI Signing does not match well the general chain of trust model of CDNI when used with symmetric keys because the symmetric key information needs to be distributed across multiple CDNI hops, to CDNs with which the CSP may not have a trust relationship. This raises a security concern for applicability of URI Signing with symmetric keys in case of DNS-based inter-CDN request routing.

6. IANA Considerations

6.1. CDNI Payload Type

This document requests the registration of the following CDNI Payload Type under the IANA "CDNI Payload Type" registry:

Payload Type	Specification
MI.UriSigning	RFCthis

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

6.1.1. CDNI UriSigning Payload Type

Purpose: The purpose of this payload type is to distinguish UriSigning MI objects (and any associated capability advertisement).

Interface: MI/FCI

Encoding: see Section 4.4

6.2. CDNI Logging Record Type

This document requests the registration of the following CDNI Logging record-type under the IANA "CDNI Logging record-types" registry:

record-types	Reference	Description
cdni_http_request_v2	RFCthis	Extension to CDNI Logging Record version 1 for content delivery using HTTP, to include URI Signing logging fields

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

6.2.1. CDNI Logging Record Version 2 for HTTP

The "cdni_http_request_v2" record-type supports all of the fields supported by the "cdni_http_request_v1" record-type [RFC7937] plus the two additional fields "s-uri-signing" and "s-uri-signing-deny-reason", registered by this document in Section 6.3. The name, format, field value, and occurence information for the two new fields can be found in Section 4.5 of this document.

6.3. CDNI Logging Field Names

This document requests the registration of the following CDNI Logging fields under the IANA "CDNI Logging Field Names" registry:

Field Name	Reference
s-uri-signing	RFCthis
s-uri-signing-deny-reason	RFCthis

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

6.4. CDNI URI Signing Signed Token Transport

The IANA is requested to create a new "CDNI URI Signing Signed Token Transport" subregistry in the "Content Delivery Networks Interconnection (CDNI) Parameters" registry. The "CDNI URI Signing Signed Token Transport" namespace defines the valid values that may be in the Signed Token Transport (cdnistt) JWT claim. Additions to the Signed Token Transport namespace conform to the "Specification Required" policy as defined in [RFC5226].

The following table defines the initial Enforcement Information Elements:

Value	Description	RFC
0	Designates token transport is not enabled	RFCthis
1	Designates token transport via cookie	RFCthis

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

[Ed Note: are there any special instructions to the designated expert reviewer?]

6.5. JSON Web Token Claims Registration

This specification registers the following Claims in the IANA "JSON Web Token Claims" registry [IANA.JWT.Claims] established by [RFC7519].

6.5.1. Registry Contents

- Claim Name: "cdniv"
- Claim Description: CDNI Claim Set Version
- Change Controller: IESG
- Specification Document(s): Section 2.1.8 of [[this specification]]

- Claim Name: "cdniip"
- Claim Description: CDNI IP Address
- Change Controller: IESG
- Specification Document(s): Section 2.1.9 of [[this specification]]

- Claim Name: "cdniuc"
- Claim Description: CDNI URI Container
- Change Controller: IESG
- Specification Document(s): Section 2.1.10 of [[this specification]]

- Claim Name: "cdniets"
- Claim Description: CDNI Expiration Time Setting for Signed Token Renewal
- Change Controller: IESG
- Specification Document(s): Section 2.1.11 of [[this specification]]

- Claim Name: "cdnistt"
- Claim Description: CDNI Signed Token Transport Method for Signed Token Renewal
- Change Controller: IESG
- Specification Document(s): Section 2.1.12 of [[this specification]]

7. Security Considerations

This document describes the concept of URI Signing and how it can be used to provide access authorization in the case of CDNI. The primary goal of URI Signing is to make sure that only authorized UAs are able to access the content, with a CSP being able to authorize every individual request. It should be noted that URI Signing is not a content protection scheme; if a CSP wants to protect the content itself, other mechanisms, such as DRM, are more appropriate.

In general, it holds that the level of protection against illegitimate access can be increased by including more claims in the signed JWT. The current version of this document includes claims for enforcing Issuer, Client IP Address, Not Before time, and Expiration Time, however this list can be extended with other, more complex, attributes that are able to provide some form of protection against some of the vulnerabilities highlighted below.

That said, there are a number of aspects that limit the level of security offered by URI Signing and that anybody implementing URI Signing should be aware of.

- Replay attacks: A (valid) Signed URI may be used to perform replay attacks. The vulnerability to replay attacks can be reduced by picking a relatively short window between the Not Before time and Expiration Time attributes, although this is limited by the fact that any HTTP-based request needs a window of at least a couple of seconds to prevent a sudden network issues from preventing

legitimate UAs access to the content. One may also reduce exposure to replay attacks by including a unique one-time access ID via the Nonce attribute (jti claim). Whenever the dCDN receives a request with a given unique ID, it adds that ID to the list of 'used' IDs. In the case an illegitimate UA tries to use the same URI through a replay attack, the dCDN can deny the request based on the already-used access ID.

- Illegitimate clients behind a NAT: In cases where there are multiple users behind the same NAT, all users will have the same IP address from the point of view of the dCDN. This results in the dCDN not being able to distinguish between the different users based on Client IP Address and illegitimate users being able to access the content. One way to reduce exposure to this kind of attack is to not only check for Client IP but also for other attributes, e.g., attributes that can be found in HTTP headers.

The shared key between CSP and uCDN may be distributed to dCDNs - including cascaded CDNs. Since this key can be used to legitimately sign a URL for content access authorization, it is important to know the implications of a compromised shared key.

If a shared key usable for signing is compromised, an attacker can use it to perform a denial-of-service attack by forcing the CDN to evaluate prohibitively expensive regular expressions embedded in a cdniuc claim. As a result, compromised keys should be timely revoked in order to prevent exploitation.

8. Privacy

The privacy protection concerns described in CDNI Logging Interface [RFC7937] apply when the client's IP address (cdniip) is embedded in the Signed URI. For this reason, the mechanism described in Section 2 encrypts the Client IP before including it in the URI Signing Package (and thus the URL itself).

9. Acknowledgements

The authors would like to thank the following people for their contributions in reviewing this document and providing feedback: Scott Leibrand, Kevin Ma, Ben Niven-Jenkins, Thierry Magnien, Dan York, Bhaskar Bhupalam, Matt Caulfield, Samuel Rajakumar, Iuniana Oprescu, Leif Hedstrom, Gancho Tenev, Brian Campbell, and Chris Lemmons.

10. Contributors

In addition, the authors would also like to make special mentions for certain people who contributed significant sections to this document.

- Matt Caulfield provided content for the CDNI Metadata Interface section.
- Emmanuel Thomas provided content for HTTP Adaptive Streaming.
- Matt Miller provided consultation on JWT usage as well as code to generate working JWT examples.

11. References

11.1. 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>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

[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>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[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>.

[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>.

11.2. Informative References

[IANA.JWT.Claims]
IANA, "JSON Web Token Claims", <http://www.iana.org/assignments/jwt>.

[MPEG-DASH]
ISO, "Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment format", ISO/IEC 23009-1:2014, Edition 2, 05 2014, <http://www.iso.org/standard/65274.html>.

[PCRE839] Hazel, P., "Perl Compatible Regular Expressions", Version 8.39, June 2016, <http://www.pcre.org/>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6707] Niven-Jenkins, B., Le Faucheur, F., and N. Bitar, "Content Distribution Network Interconnection (CDNI) Problem Statement", RFC 6707, DOI 10.17487/RFC6707, September 2012, <https://www.rfc-editor.org/info/rfc6707>.

[RFC6983] van Brandenburg, R., van Deventer, O., Le Faucheur, F., and K. Leung, "Models for HTTP-Adaptive-Streaming-Aware Content Distribution Network Interconnection (CDNI)", RFC 6983, DOI 10.17487/RFC6983, July 2013, <https://www.rfc-editor.org/info/rfc6983>.

[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>.

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

[RFC7975] Niven-Jenkins, B., Ed. and R. van Brandenburg, Ed., "Request Routing Redirection Interface for Content Delivery Network (CDN) Interconnection", RFC 7975, DOI 10.17487/RFC7975, October 2016, <https://www.rfc-editor.org/info/rfc7975>.

[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>.

[RFC8216] Pantos, R., Ed. and W. May, "HTTP Live Streaming", RFC 8216, DOI 10.17487/RFC8216, August 2017, <https://www.rfc-editor.org/info/rfc8216>.

Appendix A. Signed URI Package Example

This section contains three examples of token usage: a simple example with only the required claim present, a complex example which demonstrates the full JWT claims set, including an encrypted Client IP (cdniip), and one that uses a Signed Token Renewal.

Note: All of the examples have whitespace added to improve formatting and readability, but are not present in the generated content.

All examples use the following JWK Set [RFC7517]:

```
{ "keys": [
  {
    "kty": "EC",
    "kid": "P5UpOv0eMq1wcxLf7WxIg09JdSYGYFDOWkldueaImf0",
    "use": "sig",
    "alg": "ES256",
    "crv": "P-256",
    "x": "be807S4O7dzB6I4hTiCUvmxCI6FuxWba1xYBlLSSsZ8",
    "y": "rOGC4vI69g-WF9AGEVI37sNNwbjIzBxSjLvIL7f3RBA"
  },
  {
    "kty": "EC",
    "kid": "P5UpOv0eMq1wcxLf7WxIg09JdSYGYFDOWkldueaImf0",
    "use": "sig",
    "alg": "ES256",
    "crv": "P-256",
    "x": "be807S4O7dzB6I4hTiCUvmxCI6FuxWba1xYBlLSSsZ8",
    "y": "rOGC4vI69g-WF9AGEVI37sNNwbjIzBxSjLvIL7f3RBA",
    "d": "yaowezrCLTU6yIwUL5RQw67cHgvZeMTLVZXjUGb1A1M"
  },
  {
    "kty": "oct",
    "kid": "f-WbjxBC3dPuI3d24kP2hfvos7Qz688UTi6aB0hN998",
    "use": "enc",
    "alg": "A128GCM",
    "k": "4uFxxV7fhNmrtiah2d1fFg"
  }
]}
```

Note: They are the public signing key, the private signing key, and the shared secret enctyption key, respectively. The public and private signing keys have the same fingerprint and only vary by the 'd' parameter that is missing from the public signing key.

A.1. Simple Example

This example is a simple common usage example containing a minimal subset of claims that the authors find most useful.

The JWT Claim Set before signing:

```
{
  "exp": 1474243500,
  "iss": "uCDN Inc",
  "cdniuc": "uri:http://cdni.example/foo/bar"
}
```

The signed JWT:

```
eyJhbGciOiJFUzI1NiIsImtpZCI6IlA1VXBPdjBlTXExd2N4TGY3V3hJZzA5SmRTWU
dZRkRPV2tsZHVlYUltZjAifQ.eyJleHAiOjE0NzQyNDM1MDAsImlzcyI6InVDRE4gS
W5jIiwiY2RuaXVjIjoidXJpOmh0dHA6Ly9jZG5pLmV4YW1wbGUvZm9vL2JhciJ9.4W
xfA1ogQfeVLJYDtxrhilYctGR2KIIa1br5L6ZETTpn18_cNmsjQE4D7Cxs3tbbWAnI
gVSIdcNVwBneluta5g
```

A.2. Complex Example

This example uses all fields except for those dealing with Signed Token Renewal, including Client IP (cdniip) and Subject (sub) which are encrpyted. This significantly increases the size of the signed JWT token.

JWE for Client IP (cdniip) of [2001:db8::1/32]:

```
eyJhbGciOiJkaXIiLCJraWQiOiJmLVdianhCQzNkUHVJM2QyNGtQMmhmdm9zN1F6Nj
g4VVRpNmFCMGhOOTk4IiwiZW5jIjoiQTEyOEdDTSJ9..hHQn6LM8Km95O0IE.KgJiy
DRsW7QBQsDJrmS7Hg.cXRZ8sMJ8PKz3fnj6VXgvw
```

JWE for Subject (sub) of "UserToken":

```
eyJhbGciOiJkaXIiLCJraWQiOiJmLVdianhCQzNkUHVJM2QyNGtQMmhmdm9zN1F6Nj
g4VVRpNmFCMGhOOTk4IiwiZW5jIjoiQTEyOEdDTSJ9..ZH1hpBqhB8rgr3fD.3iEkR
iaFkgwG.nzyjp7bZ3SJlYcDWv9irrQ
```

The JWT Claim Set before signing:

```
{
  "aud": "dCDN LLC",
  "sub": "eyJhbGciOiJkaXIiLCJraWQiOiJmLVdianhCQzNkUHVJM2QyNGtQMmhm
dm9zN1F6Njg4VVRpNmFCMGhOOTk4IiwiZW5jIjoiQTEyOEdDTSJ9..ZH1hpBqhB8rg
r3fD.3iEkRiaFkgwG.nzyjp7bZ3SJlYcDWv9irrQ",
  "cdniip": "eyJhbGciOiJkaXIiLCJraWQiOiJmLVdianhCQzNkUHVJM2QyNGtQM
mhmdm9zN1F6Njg4VVRpNmFCMGhOOTk4IiwiZW5jIjoiQTEyOEdDTSJ9..hHQn6LM8K
m95O0IE.KgJiyDRsW7QBQsDJrmS7Hg.cXRZ8sMJ8PKz3fnj6VXgvw",
  "cdniv": 1,
  "exp": 1474243500,
  "iat": 1474243200,
  "iss": "uCDN Inc",
  "jti": "5DAafLhZAfhsbe",
  "nbf": 1474243200,
  "cdniuc": "uri-regex:http://cdni\\.example/foo/bar/[0-9]{3}\\.png"
}
```

The signed JWT:

```
eyJhbGciOiJFUzI1NiIsImtpZCI6IlA1VXBPdjBlTXExd2N4TGY3V3hJZzA5SmRTWU
dZRkRPV2tsZHVlYUltZjAifQ.eyJhdWQiOiJkQ0ROIExMQyIsInN1YiI6ImV5SmhiR
2NpT2lKa2FYSWlMQ0pyYVdRaU9pSm1MVmRpYW5oQ1F6TmtVSFZKTTJReU5HdFFNbWh
tZG05ek4xRjZOamc0VlZScE5tRkNNR2hPT1RrNElpd2laVzVqSWpvaVFURXlPRWREV
FNKOS4uWkgxaHBCcWhCOHJncjNmRC4zaUVrUmlhRmtnd0cubnp5anA3YlozU0psWWN
EV3Y5aXJyUSIsImNkbmlpcCI6ImV5SmhiR2NpT2lKa2FYSWlMQ0pyYVdRaU9pSm1MV
mRpYW5oQ1F6TmtVSFZKTTJReU5HdFFNbWhtZG05ek4xRjZOamc0VlZScE5tRkNNR2h
PT1RrNElpd2laVzVqSWpvaVFURXlPRWREVFNKOS4uaEhRbjZMTThLbTk1TzBJRS5LZ
0ppeURSc1c3UUJRc0RKcm1TN0hnLmNYUlo4c01KOFBLejNmbmo2VlhndnciLCJjZG5
pdiI6MSwiZXhwIjoxNDc0MjQzNTAwLCJpYXQiOjE0NzQyNDMyMDAsImlzcyI6InVDR
E4gSW5jIiwianRpIjoiNURBYWZMaFpBZmhzYmUiLCJuYmYiOjE0NzQyNDMyMDAsImN
kbml1YyI6InVyaS1yZWdleDpodHRwOi8vY2RuaVxcLmV4YW1wbGUvZm9vL2Jhci9bM
C05XXszfVxcLnBuZyJ9.3sKwFFMy7Hlbur1RzkeI0wDKerYXcrmBdfwJG7NP3TWS7a
s52f8-F-wOFzFEIoX2UX3Z5Dinl6lbCQ__-pBgZw
```

A.3. Signed Token Renewal Example

This example uses fields for Signed Token Renewal.

The JWT Claim Set before signing:

```
{
  "cdniets": 30,
  "cdnistt": 1,
  "exp": 1474243500,
  "cdniuc": "uri-regex:http://cdni\\.example/foo/bar/[0-9]{3}\\.ts"
}
```

The signed JWT:

eyJhbGciOiJFUzI1NiIsImtpZCI6IlA1VXBPdjBlTXExd2N4TGY3V3hJZzA5SmRTWU
dZRkRPV2tsZHVlYUltZjAifQ.eyJjZG5pZXRzIjozMCwiY2RuaXN0dCI6MSwiZXhwI
joxNDc0MjQzNTAwLCJjZG5pdWMiOiJ1cmktcmVnZXg6aHR0cDovL2NkbmlcXC5leGF
tcGxlL2Zvby9iYXIvWzAtOV17M31cXC50cyJ9.fL4S6f4FovPls_N-JBap7CKGsQsi
Xhds2nFhz3EnIOVfDlrTt3mw6AA6SsHnc2fu6bqZP_3YOdwOYFYjDPTYfg

Once the server validates the signed JWT it will return a new signed JWT with an updated expiry time (exp) as shown below. Note the expiry time is increased by the expiration time setting (cdniets) value.

The JWT Claim Set before signing:

```
{
  "cdniets": 30,
  "cdnistt": 1,
  "exp": 1474243530,
  "cdniuc": "uri-regex:http://cdni\\.example/foo/bar/[0-9]{3}\\.ts"
}
```

The signed JWT:

eyJhbGciOiJFUzI1NiIsImtpZCI6IlA1VXBPdjBlTXExd2N4TGY3V3hJZzA5SmRTWU
dZRkRPV2tsZHVlYUltZjAifQ.eyJjZG5pZXRzIjozMCwiY2RuaXN0dCI6MSwiZXhwI
joxNDc0MjQzNTMwLCJjZG5pdWMiOiJ1cmktcmVnZXg6aHR0cDovL2NkbmlcXC5leGF
tcGxlL2Zvby9iYXIvWzAtOV17M31cXC50cyJ9.Zi-Xq-0ZrZ5uL2F5YCxZMXWWnaM6
wS9-x9eRu5UC6WgbMBQ0yH7lJNe7UG_5Ge-QPuRggm9tz1AF4S_Ty8H9Ig

Authors' Addresses

Ray van Brandenburg
Tiledmedia
Anna van Buerenplein 1
Den Haag 2595DA
The Netherlands

Phone: +31 88 866 7000
Email: ray@tiledmedia.com

Kent Leung
Cisco Systems, Inc.
3625 Cisco Way
San Jose, CA 95134
United States

Phone: +1 408 526 5030
Email: kleung@cisco.com

Phil Sorber

Email: sorber@apache.org