

ACME
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2018

Y. Sheffer
Intuit
D. Lopez
O. Gonzalez de Dios
A. Pastor Perales
Telefonica I+D
T. Fossati
Nokia
June 29, 2018

Generating Certificate Requests for Short-Term, Automatically-Renewed
(STAR) Certificates
draft-sheffer-acme-star-request-02

Abstract

This memo proposes a protocol that allows a domain name owner to delegate to a third party (such as a CDN) control over a certificate that bears one or more names in that domain. Specifically the third party creates a Certificate Signing Request for the domain, which can then be used by the domain owner to request a short term and automatically renewed (STAR) certificate.

This is a component in a solution where a third-party such as a CDN can terminate TLS sessions on behalf of a domain name owner (e.g., a content provider), and the domain owner can cancel this delegation at any time without having to rely on certificate revocation mechanisms.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 31, 2018.

Internet-Draft

ACME STAR Request

June 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 (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Terminology	3
1.2.	Conventions used in this document	4
2.	Protocol Flow	4
2.1.	Preconditions	4
2.2.	Bootstrap	4
2.3.	Refresh	6
2.4.	Termination	7
3.	Protocol Details	8
3.1.	STAR API	8
3.1.1.	Creating a Delegation Request	8
3.1.2.	Polling the Delegation Request	10
3.2.	Transport Security for the STAR Protocol	11
4.	CDNI Use Cases	11
4.1.	Multiple Parallel Delegates	11
4.2.	Chained Delegation	11
5.	Security Considerations	12
5.1.	STAR Protocol Authentication	12
6.	Acknowledgments	12
7.	References	12
7.1.	Normative References	12
7.2.	Informative References	13
Appendix A.	Document History	14
A.1.	draft-sheffer-acme-star-request-02	14
A.2.	draft-sheffer-acme-star-request-01	14
A.3.	draft-sheffer-acme-star-request-00	14

[1.](#) Introduction

This document is a companion document to [\[I-D.ietf-acme-star\]](#). To avoid duplication, we give here a bare-bones description of the motivation for this solution. For more details and further use cases, please refer to the introductory sections of [\[I-D.ietf-acme-star\]](#).

A content provider (referred to in this document as Domain Name Owner, DNO, or more generally as Identity Owner, IdO) has agreements in place with one or more Content Delivery Networks (CDNs) that are contracted to serve its content over HTTPS. The CDN terminates the HTTPS connection at one of its edge cache servers and needs to present its clients (browsers, set-top-boxes) a certificate whose name matches the authority of the URL that is requested, i.e. that of the DNO. However, many DNOs balk at sharing their long-term private keys with another organization and, equally, delegates (henceforth referred to as NDC, Name Delegation Consumer) would rather not have to handle other parties' long-term secrets.

This document describes a protocol where the IdO and the NDC agree on a CSR template and the NDC generates a CSR for a private key that it holds. The IdO then uses the ACME protocol (as extended in [\[I-D.ietf-acme-star\]](#)) to issue the STAR certificate.

The generated short-term certificate is automatically renewed by an ACME Certification Authority (CA) [\[I-D.ietf-acme-acme\]](#) and periodically fetched into the NDC and used for HTTPS connections. The IdO can end the delegation at any time by simply instructing the CA to stop the automatic renewal and letting the certificate expire shortly thereafter.

[1.1.](#) Terminology

IdO Identity Owner, the owner of an identity (e.g., a domain name) that needs to be delegated.

DNO Domain Name Owner, a specific kind of IdO whose identity is a domain name.

NDC Name Delegation Consumer, the entity to which the domain name is delegated for a limited time. This is often a CDN (in fact, readers may note the similarity of the two acronyms).

CDN Content Delivery Network, a widely distributed network that serves the domain's web content to a wide audience at high performance.

STAR Short-Term, Automatically Renewed X.509 certificates.

ACME The IETF Automated Certificate Management Environment, a certificate management protocol.

CA A Certificate Authority that implements the ACME protocol.

[1.2.](#) Conventions used in this document

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 [\[RFC2119\]](#).

[2.](#) Protocol Flow

This section presents the protocol flow. For completeness, we include the STAR Interface proposed in this draft, as well as the extended ACME protocol as described in [\[I-D.ietf-acme-star\]](#).

[2.1.](#) Preconditions

The protocol assumes the following preconditions are met:

- o A mutually authenticated channel between NDC and IdO pre-exists. This is called "STAR channel" and all STAR protocol exchanges between NDC and IdO are run over it. It provides the guarantee that requests and responses are authentic.
- o NDC and IdO have agreed on a "CSR template" to use, including at a minimum:
 - Subject name (e.g., "somesite.example.com"),
 - Requested algorithms,
 - Key length,
 - Key usage.

The NDC is required to use this template for every CSR created under the same delegation.

- o IdO has registered through the ACME interface exposed by the Certificate Authority (CA) using the usual ACME registration procedure. In ACME terms, the IdO has an Account on the server and is ready to issue Orders.

2.2. Bootstrap

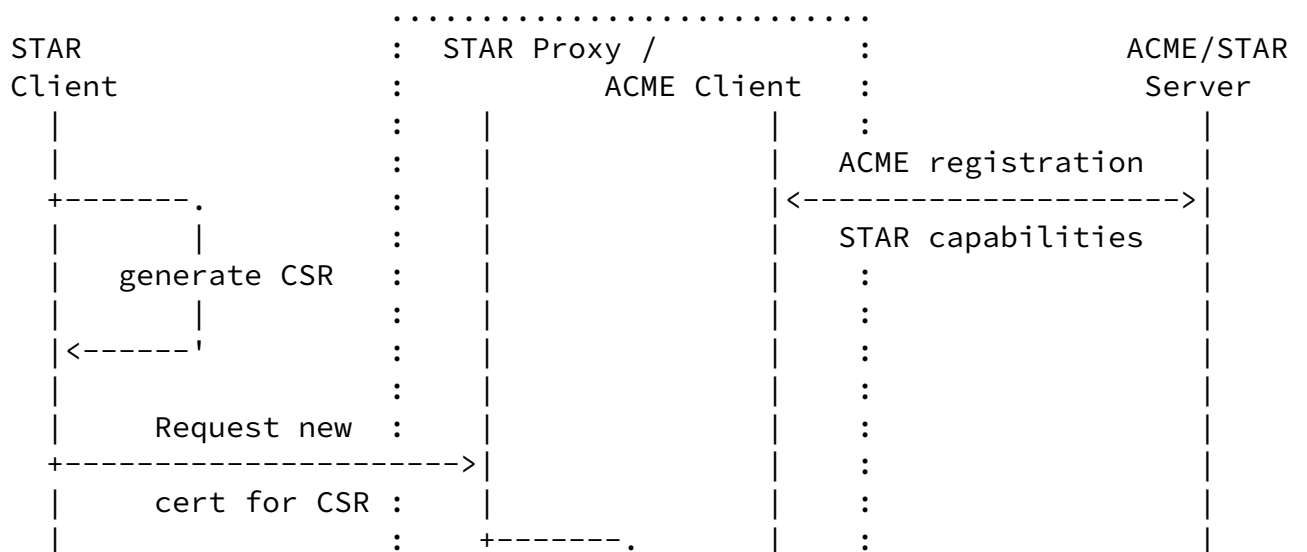
The NDC (STAR Client) generates a key-pair, wraps it into a Certificate Signing Request (CSR) according to the agreed upon CSR template, and sends it to the IdO (STAR Proxy) over the pre-established STAR channel. The IdO uses the NDC identity provided on the STAR channel to look up the CSR template that applies to the requesting NDC and decides whether or not to accept the request. Assuming everything is in order, it then "forwards" the NDC request to the ACME CA by means of the usual ACME application procedure. Specifically, the IdO, in its role as an ACME client, requests the CA to issue a STAR certificate, i.e., one that:

- o Has a short validity (e.g., 24 to 72 hours);
- o Is automatically renewed by the CA for a certain period of time;
- o Is downloadable from a (highly available) public link without requiring any special authorization.

Other than that, the ACME protocol flows as normal between IdO and CA, in particular IdO is responsible for satisfying the requested ACME challenges until the CA is willing to issue the requested certificate. Per normal ACME processing, the IdO is given back an Order ID for the issued STAR certificate to be used in subsequent interaction with the CA (e.g., if the certificate needs to be terminated.)

Concurrently, a response is sent back to the NDC with an endpoint to poll for completion of the certificate generation process.

The bootstrap phase ends when the IdO obtains the OK from the ACME CA and posts the certificate's URL to the "completion endpoint" where the NDC can retrieve it.



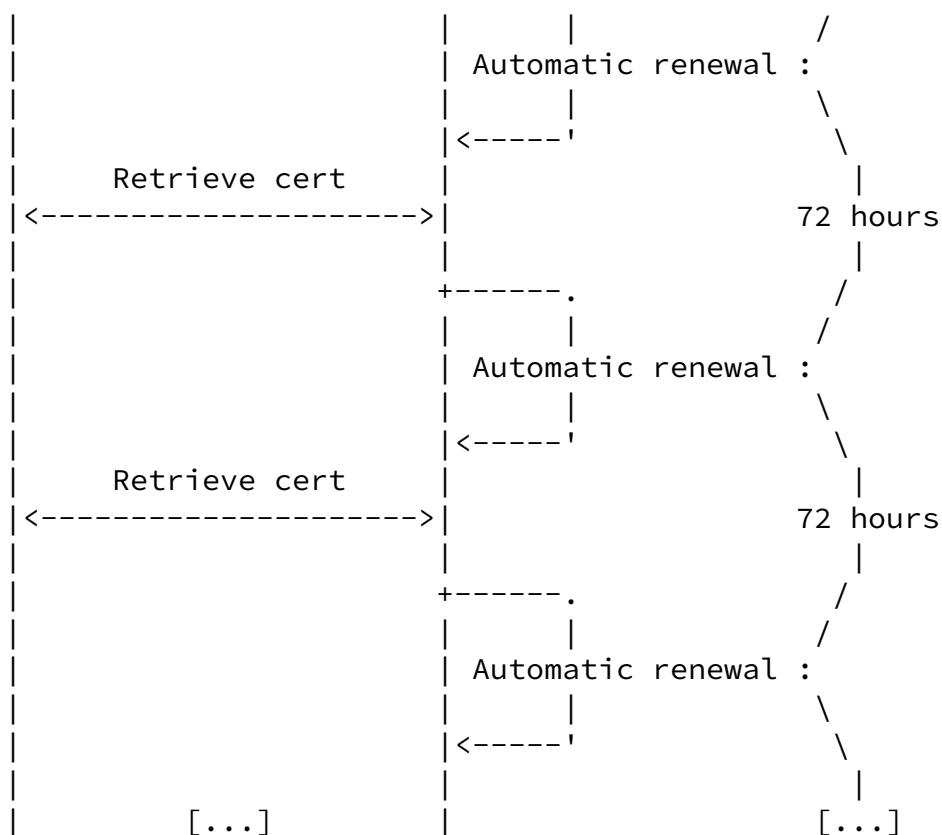


Figure 2: Auto renewal

[2.4.](#) Termination

The IdO may request early termination of the STAR certificate by including the Order ID in a certificate termination request to the ACME interface, defined below. After the CA receives and verifies the request, it shall:

- o Cancel the automatic renewal process for the STAR certificate;
- o Change the certificate publication resource to return an error indicating the termination of the delegation to external clients, including the NDC.

Note that it is not necessary to explicitly revoke the short-term certificate.

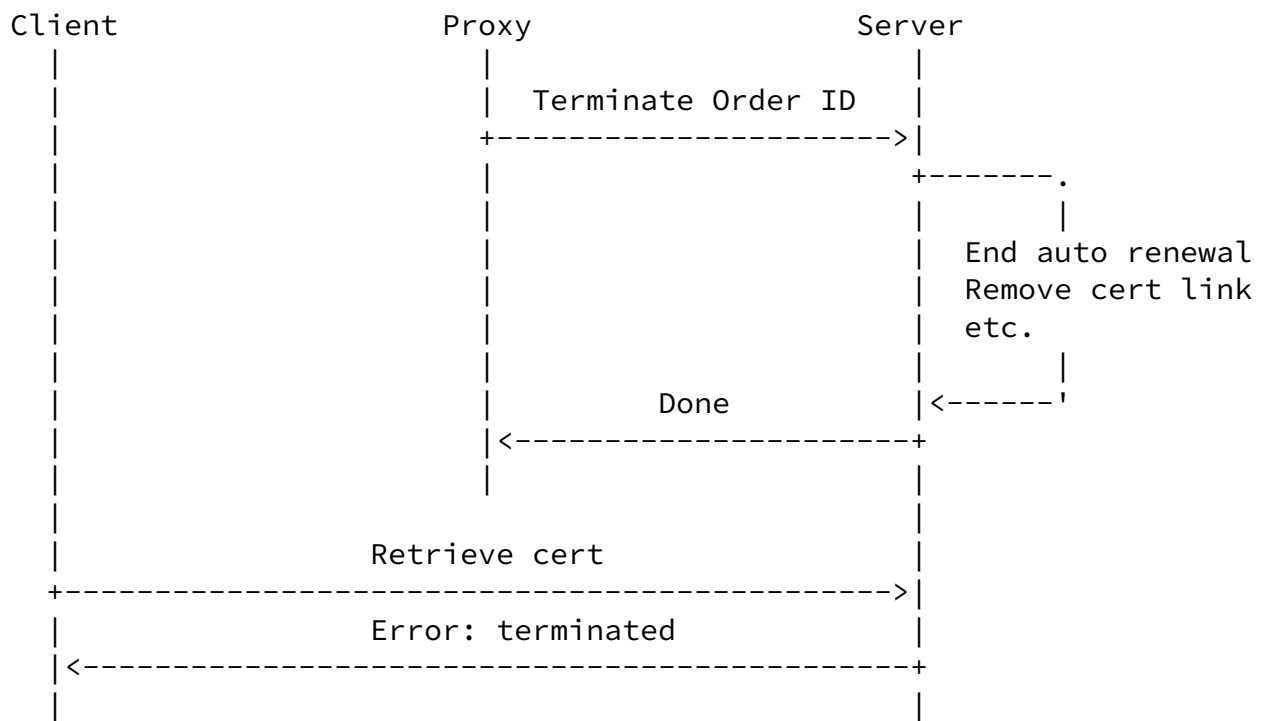


Figure 3: Termination

No facility is provided for the NDC to directly initiate the termination of a STAR certificate.

[3. Protocol Details](#)

This section describes the STAR API between the STAR Client and the STAR Proxy.

[3.1. STAR API](#)

This API allows an IdO (STAR Proxy) to control the long-term delegation of one of its names to an authorized third-party (STAR Client).

[3.1.1. Creating a Delegation Request](#)

To create a new delegation request, the client wraps the following parameters in a POST to the '/star/delegation' path:

- o `csr` (required, string): A CSR encoding the parameters for the certificate being requested [[RFC2986](#)]. The CSR is sent in the base64url-encoded version of the DER format. (Note: Because this field uses base64url, and does not include headers, it is different from PEM.)

- o duration (optional, integer): How long the delegation should last (in seconds). If not specified, a local default applies.
- o certificate-lifetime (optional, integer): How long each short-term certificate should last (in seconds). If not specified, a local default applies.

Note that the STAR Proxy MAY treat both "duration" and "certificate-lifetime" as hints, and MAY update any of them due to local policy decisions or as a result of the interaction with the ACME server.

```
POST /star/delegation
Host: star-proxy.example.net
Content-Type: application/json
```

```
{
  "csr": "jcRf4uXra7FGYW5ZMewvV...rhlnznwy8YbpMGqwidEXfE",
  "duration": 31536000,
  "certificate-lifetime": 604800
}
```

On success, the service returns a 201 Created status with the URL of the newly generated delegation order in the Location header field. The current state of the delegation order is returned in the body of the response in JSON format:

```
HTTP/1.1 201 Created
Content-Type: application/json
Location: http://example.net/star/delegation/567
```

```
{
  "id": "567",
  "certificate-lifetime": 604800,
  "duration": 31536000,
  "status": "new"
}
```

If an error occurs, an error response (4XX or 5XX) is generated with an appropriate problem detail [[RFC7807](#)] body, e.g.:

HTTP/1.1 400 Bad Request

Content-Type: application/problem+json

```
{
  "type": "https://example.net/validation-error",
  "title": "Your request parameters didn't validate.",
  "invalid-params": [ {
    "name": "csr",
    "reason": "missing mandatory parameter"
  } ]
}
```

[3.1.2.](#) Polling the Delegation Request

The returned delegation order URL can be polled until the dialog between the STAR Proxy and the ACME server is complete (i.e., the "status" attribute changes from "new" or "pending" to one of "failed" or "success"):

```
GET /star/delegation/567
Host: star-proxy.example.net
```

In responding to poll requests while the validation is still in progress, the server **MUST** return a 200 (OK) response and **MAY** include a Retry-After header field to suggest a polling interval to the client. The Retry-After value **MUST** be expressed in seconds. If the Retry-After header is present, in order to avoid surprising interactions with heuristic expiration times, a max-age Cache-Control **SHOULD** also be present and set to a value slightly smaller than the Retry-After value:

```
HTTP/1.1 200 OK
Content-Type: application/json
Retry-After: 10
Cache-Control: max-age=9
```

```
{
  "id": "5",
  "certificate-lifetime": 604800,
```

```
"creation-date": "2017-11-12T01:38:09Z",
"duration": 31536000,
"status": "pending"
}
```

When the operation is successfully completed, the ACME Proxy returns:

```
HTTP/1.1 200 OK
```

```
{
  "status": "success", // or "failed"
  "lifetime": 365,      // lifetime of the registration in days,
                        // possibly less than requested
  "certificates": "https://ca.example.org/certificates/A51A3"
}
```

The "certificates" attribute contains a URL of the certificate pull endpoint, received from the ACME Server.

If the registration fails for any reason, the server returns a "200 OK" response, with the status as "failed" and a "reason" attribute containing a human readable error message.

[3.2.](#) Transport Security for the STAR Protocol

Traffic between the STAR Client and the STAR Proxy MUST be protected with HTTPS. For interoperability, all implementations MUST support HTTP Basic Authentication [[RFC7617](#)]. However some deployments MAY prefer mutually-authenticated HTTPS or two-legged OAUTH.

[4.](#) CDNI Use Cases

Members of the IETF CDNI (Content Delivery Network Interconnection) working group are interested in delegating authority over web content to CDNs. Their requirements are described in a draft [[I-D.fieau-cdni-https-delegation](#)] that compares several solutions. This section discusses two particular requirements in the context of the STAR protocol.

[4.1.](#) Multiple Parallel Delegates

In some cases the DNO would like to delegate authority over a web site to multiple CDNs. This could happen if the DNO has agreements in place with different regional CDNs for different geographical regions. STAR enables this use case naturally, since each CDN can authenticate separately to the DNO specifying its CSR, and the DNO is free to allow or deny each certificate request according to its own policy.

[4.2.](#) Chained Delegation

In other cases, a content owner (DNO) delegates some domains to a large CDN (CDN1), which in turn delegates to a smaller regional CDN, CDN2. The DNO has a contractual relationship with CDN1, and CDN1 has

Sheffer, et al.

Expires December 31, 2018

[Page 11]

Internet-Draft

ACME STAR Request

June 2018

a similar relationship with CDN2. However DNO may not even know about CDN2.

The STAR protocol does not prevent this use case, although there is no special support for it. CDN1 can forward requests from CDN2 to DNO, and forward responses back to CDN2. Whether such proxying is allowed is governed by policy and contracts between the parties.

[5.](#) Security Considerations

[5.1.](#) STAR Protocol Authentication

The STAR protocol allows its client to obtain certificates bearing the IdO's identity. Therefore strong client authentication is mandatory.

When multiple NDCs may connect to the same IdO, the STAR protocol's authentication MUST allow the IdO to distinguish between different NDCs, and the IdO MUST associate different Registration objects to different clients. Among other benefits, this allows the IdO to cancel a STAR registration for one of its clients instead of all of them.

[6.](#) Acknowledgments

This work is partially supported by the European Commission under Horizon 2020 grant agreement no. 688421 Measurement and Architecture for a Middleboxed Internet (MAMI). This support does not imply endorsement.

[7.](#) References

[7.1.](#) Normative References

[I-D.ietf-acme-acme]

Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", [draft-ietf-acme-acme-12](#) (work in progress), April 2018.

[I-D.ietf-acme-star]

Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Support for Short-Term, Automatically-Renewed (STAR) Certificates in Automated Certificate Management Environment (ACME)", [draft-ietf-acme-star-03](#) (work in progress), March 2018.

Sheffer, et al.

Expires December 31, 2018

[Page 12]

Internet-Draft

ACME STAR Request

June 2018

[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>>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", [RFC 2986](#), DOI 10.17487/RFC2986, November 2000, <<https://www.rfc-editor.org/info/rfc2986>>.

[RFC7617] Reschke, J., "The 'Basic' HTTP Authentication Scheme", [RFC 7617](#), DOI 10.17487/RFC7617, September 2015, <<https://www.rfc-editor.org/info/rfc7617>>.

[RFC7807] Nottingham, M. and E. Wilde, "Problem Details for HTTP APIs", [RFC 7807](#), DOI 10.17487/RFC7807, March 2016, <<https://www.rfc-editor.org/info/rfc7807>>.

[7.2.](#) Informative References

[I-D.fieau-cdni-https-delegation]

Fieau, F., Emile, S., and S. Mishra, "HTTPS delegation in CDNI", [draft-fieau-cdni-https-delegation-02](#) (work in progress), July 2017.

Sheffer, et al.	Expires December 31, 2018	[Page 13]
-----------------	---------------------------	-----------

Internet-Draft	ACME STAR Request	June 2018
----------------	-------------------	-----------

[Appendix A.](#) Document History

[[Note to RFC Editor: please remove before publication.]]

[A.1.](#) [draft-sheffer-acme-star-request-02](#)

- o Clarifications and minor changes based on implementation experience.
- o More detail on error cases.

[A.2.](#) [draft-sheffer-acme-star-request-01](#)

- o Correct reference to WG draft.

A.3. [draft-sheffer-acme-star-request-00](#)

- o Initial version, the STAR API extracted from [draft-sheffer-acme-star-02](#).

Authors' Addresses

Yaron Sheffer
Intuit

EMail: aronf.ietf@gmail.com

Diego Lopez
Telefonica I+D

EMail: diego.r.lopez@telefonica.com

Oscar Gonzalez de Dios
Telefonica I+D

EMail: oscar.gonzalezdedios@telefonica.com

Antonio Agustin Pastor Perales
Telefonica I+D

EMail: antonio.pastorperales@telefonica.com

Thomas Fossati
Nokia

EMail: thomas.fossati@nokia.com

