ACME
Internet-Draft
Intended status: Standards Track
Expires: December 18, 2017

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

June 16, 2017

Generating Certificate Requests for Short-Term, Automatically-Renewed (STAR) Certificates
draft-sheffer-acme-star-request-01

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 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 December 18, 2017.

Table of Contents

1. Introduction

This document is a companion document to [I-D.ietf-acme-star]. To avoid duplication, we give here a barebones 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) 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 DNO and the NDC agree on a CSR template and the NDC generates a CSR for a private key that it holds. The DNO 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 routinely fetched into the NDC and used for HTTPS connections. The DNO 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

DNO Domain Name Owner, the owner of a domain that needs to be delegated.

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:

- A mutually authenticated channel between NDC and DNO pre-exists. This is called "STAR channel" and all STAR protocol exchanges between NDC and DNO are run over it. It provides the guarantee that requests and responses are authentic.
- NDC and DNO 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.
- DNO has registered through the ACME interface exposed by the Certificate Authority (CA) using the usual ACME registration procedure. In ACME terms, the DNO 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 DNO (STAR Proxy) over the pre-established STAR channel. The DNO 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 DNO, in its role as an ACME client, requests the CA to issue a STAR certificate, i.e., one that:

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

Other than that, the ACME protocol flows as normal between DNO and CA, in particular DNO is responsible for satisfying the requested ACME challenges until the CA is willing to issue the requested certificate. Per normal ACME processing, the DNO 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 DNO obtains the OK from the ACME CA and posts the certificate's URL to the "completion endpoint" where the NDC can retrieve it.

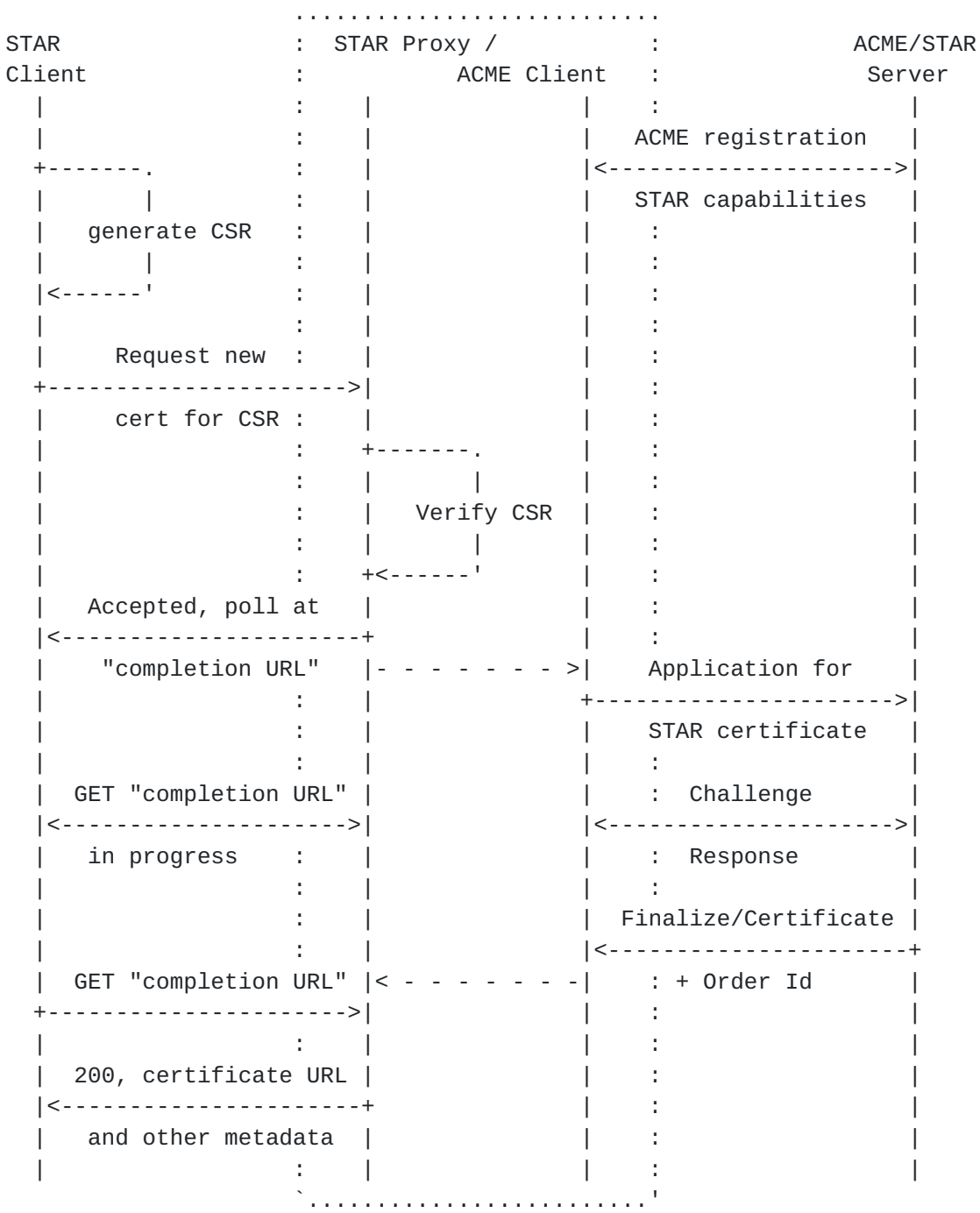

Figure 1: Bootstrap

2.3. Refresh

The CA automatically re-issues the certificate (using the same CSR) before it expires and publishes it to the URL that the NDC has come to know at the end of the bootstrap phase. The NDC downloads and installs it. This process goes on until either:

- DNO terminates the delegation, or
- Automatic renewal expires.

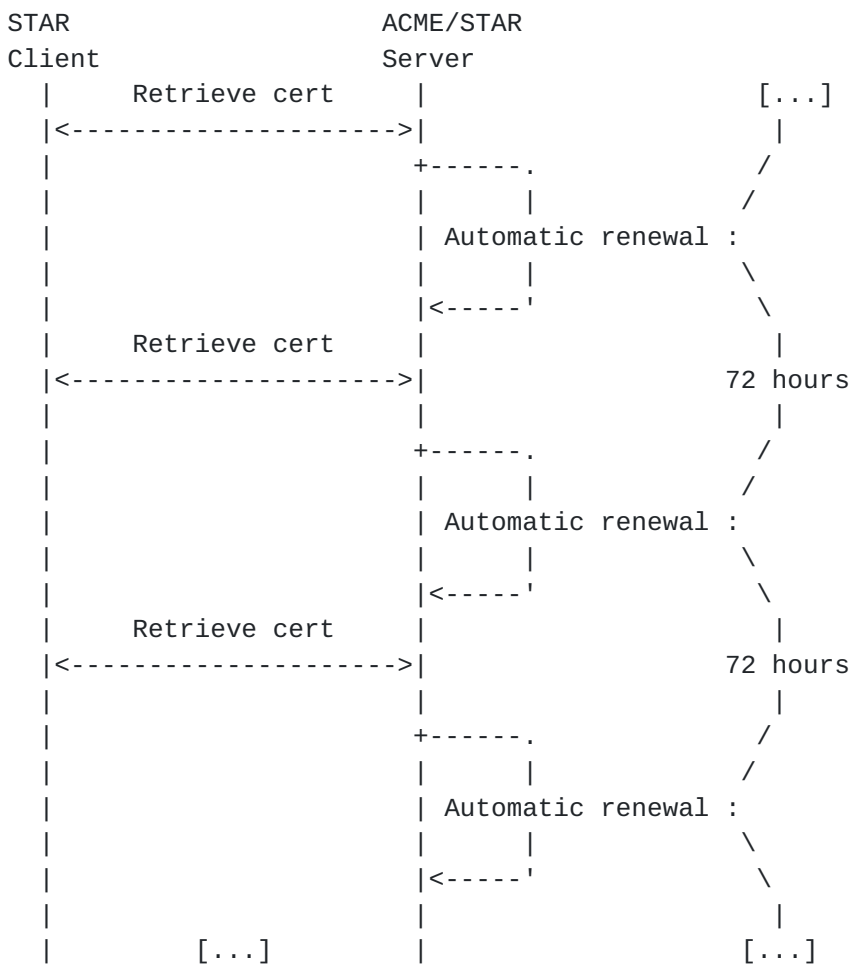

Figure 2: Auto renewal

2.4. Termination

The DNO 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:

- Cancel the automatic renewal process for the STAR certificate;
- 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.

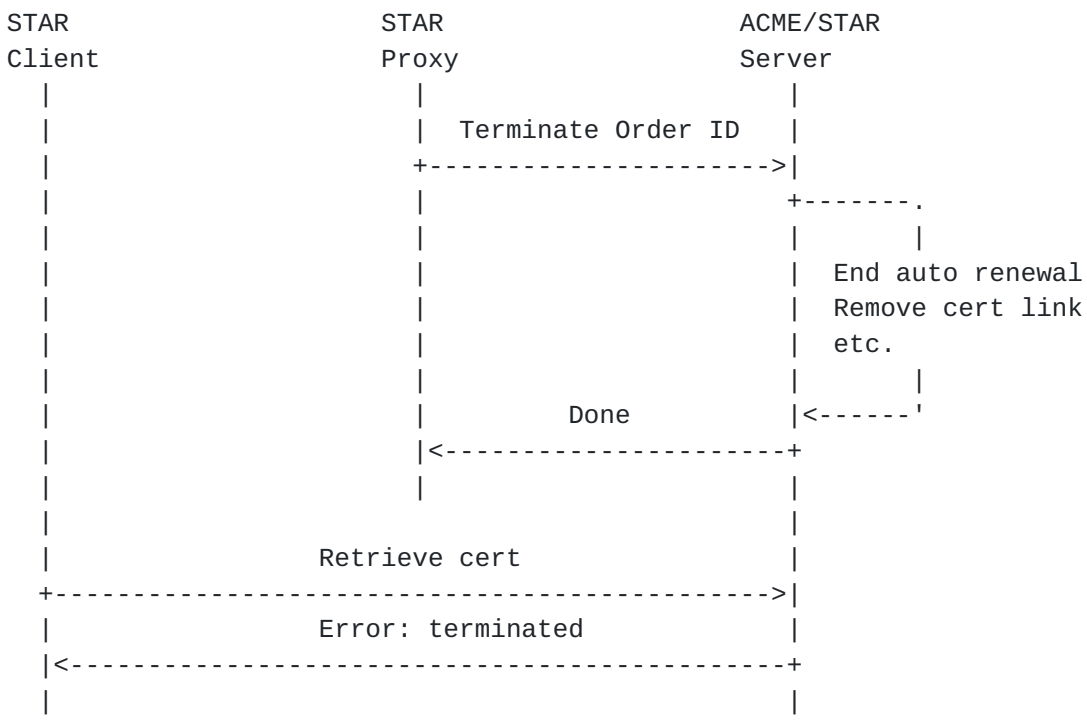

Figure 3: Termination

3. Protocol Details

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

3.1. STAR API

This API allows the STAR Client to request a STAR certificate via the STAR Proxy, using a previously agreed-upon CSR template.

The API consists of a single resource, "registration". A new Registration is created with a POST request, and the Registration instance is polled to obtain its details.

3.1.1. Creating a Registration

To create a registration, use:

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

{
    "csr": "...",    // CSR in PEM format
    "lifetime": 365, // requested registration lifetime in days,
                     // between 1 and 1095
    "validity": 7    // requested certificate validity in days
}
```

The STAR Proxy MAY treat both "lifetime" and "validity" periods as hints. Upon success, the call returns the new Registration resource.

```
HTTP/1.1 201 Created
Location: https://star-proxy.example.net/star/registration/567
```

3.1.2. Polling the Registration

The returned Registration can be polled until the information is available from the ACME server.

```
GET /star/registration/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
Retry-After: 10
Cache-Control: max-age=9

{
    "status": "pending"
}
```

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

```
HTTP/1.1 200 OK
Expires: Sun, 09 Sep 2018 14:09:00 GMT

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

The Expires header applies to the Registration resource itself, and may be as small as a few minutes. It is unrelated to the Order's lifetime which is measured in days or longer. 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 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 DNO's identity. Therefore strong client authentication is mandatory.

When multiple NDCs may connect to the same DNO, the STAR protocol's authentication MUST allow the DNO to distinguish between different NDCs, and the DNO MUST associate different Registration objects to different clients. Among other benefits, this allows the DNO 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., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-06 (work in progress), March 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.

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

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

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-01 (work in progress), March 2017.

Appendix A. Document History

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

A.1. draft-sheffer-acme-star-request-01

- Correct reference to WG draft.

A.2. draft-sheffer-acme-star-request-00

- Initial version, the STAR API extracted from draft-sheffer-acme-star-02.

Authors' Addresses

Yaron Sheffer
Intuit

EMail: yaronf.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