ACME                                                         Y. Sheffer
Internet-Draft                                                   Intuit
Intended status: Standards Track                               D. Lopez
Expires: April 22, 2019                                A. Pastor Perales
                                                         Telefonica I+D
                                                             T. Fossati
                                                                  Nokia
                                                       October 19, 2018

### An ACME Profile for Generating Delegated STAR Certificates
### draft-sheffer-acme-star-delegation-00

Abstract

   This memo proposes a profile of the ACME protocol that allows the
   owner of an identifier (e.g., a domain name) to delegate to a third
   party access to a certificate associated with said identifier.  A
   primary use case is that of a CDN (the third party) terminating TLS
   sessions on behalf of a content provider (the owner of a domain
   name).  The presented mechanism allows the owner of the identifier to
   retain control over the delegation and revoke it at any time by
   cancelling the associated STAR certificate renewal with the ACME CA.
   Another key property of this mechanism is it does not require any
   modification to the deployed TLS ecosystem.

Status of This Memo

Copyright Notice

Table of Contents

## 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].

An Identifier Owner (IdO), that we can associate in the primary use
case to a content provider (also referred to as Domain Name Owner,
DNO), has agreements in place with one or more NDC (Name Delegation

Consumer) to use and attest its identity.  In the primary use case,
we consider a CDN provider contracted to serve the IdO content over
HTTPS.  The CDN terminates the HTTPS connection at one of its edge
cache servers and needs to present its clients (browsers, mobile
apps, set-top-boxes) a certificate whose name matches the authority
of the URL that is requested, i.e., that of the IdO.  Understandably,
most IdOs balk at sharing their long-term private keys with another
organization and, equally, delegates would rather not have to handle
other parties' long-term secrets.

This document describes a profile of the ACME protocol
[I-D.ietf-acme-acme] that allows the NDC to request the IdO, acting
as a profiled ACME server, a certificate for a delegated identity -
i.e., one belonging to the IdO.  The IdO then uses the ACME protocol
(with the extensions described in [I-D.ietf-acme-star]) to request
issuance of a STAR certificate for the same delegated identity.  The
generated short-term certificate is automatically renewed by the ACME
Certification Authority (CA), periodically fetched by the NDC and
used to terminate HTTPS connections in lieu of the IdO.  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.

In case the delegated identity is a domain name, this document also
provides a way for the NDC to inform the IdO about the CNAME mappings
that need to be installed in the IdO's DNS zone to enable the
aliasing of the delegated name, thus allowing the complete name
delegation workflow to be handled using a single interface.

## 1.1.  Terminology

IdO  Identifier Owner, the owner of an identifier (e.g., a domain
   name) that needs to be delegated.
DNO  Domain Name Owner, a specific kind of IdO whose identifier is a
   domain name
NDC  Name Delegation Consumer, the entity to which the domain name is
   delegated for a limited time.  This is a CDN in the primary use
   case (in fact, readers may note the symmetry 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
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

## 2.  Protocol Flow

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

## 2.1.  Preconditions

The protocol assumes the following preconditions are met:

o  The IdO exposes an ACME server interface to the NDC(s) comprising
   the account management interface;
o  The NDC has registered an ACME account with the IdO;
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 an ACME account with the Certificate Authority
   (CA)

Note that even if the IdO implements the ACME server role, it is not
acting as a CA: in fact, from the point of view of the certificate
issuance process, the IdO only works as a "policing" forwarder of the
NDC's key-pair and is responsible for completing the identity
verification process towards the ACME CA.

## 2.2.  Overview

The interaction between the NDC and the IdO is governed by the
profiled ACME workflow detailed in Section 2.3.  The interaction
between the IdO and the CA is ruled by ACME STAR
[I-D.ietf-acme-star].

The outline of the combined protocol is as follow (Figure 1):

o  NDC sends an Order for the delegated identifier to IdO;
o  IdO creates an Order resource in state "ready" with a "finalize"
   URL;
o  NDC immediately sends a finalize request (which includes the CSR)
   to the IdO;

o  IdO verifies the CSR according to the agreed CSR template;

o  If the CSR verification fails, the Order is moved to an "invalid"
   state and everything stops;

o  If the CSR verification is successful, IdO moves the Order to
   state "processing", and sends an Order' (using its own account)
   for the delegated identifier to the ACME STAR CA;

o  If the ACME STAR protocol fails, Order' moves to "invalid" and the
   same state is reflected in the NDC Order;

o  If the ACME STAR run is successful (i.e., Order' is "valid"), IdO
   copies the "star-certificate" URL from Order' to Order and moves
   its state "valid".

The NDC can now download, install and use the certificate bearing the
name delegated by the IdO.

Note that, because the identity validation is suppressed, the NDC
sends the finalize request, including the CSR, to the IdO immediately
after the Order has been acknowledged.  The IdO must buffer a (valid)
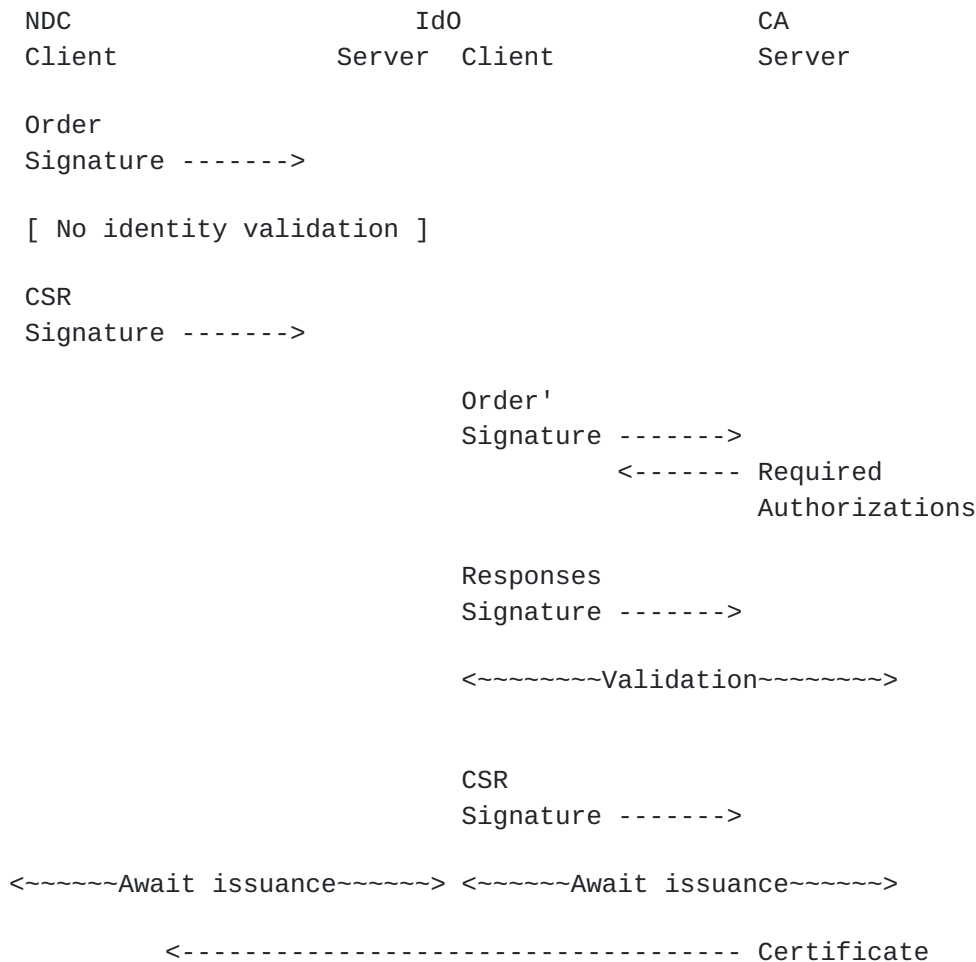CSR until the Validation phase completes successfully.

```
      NDC                    IdO                    CA
      Client              Server  Client            Server

      Order
      Signature ------->

      [ No identity validation ]

      CSR
      Signature ------->

                               Order'
                               Signature ------->
                                           <------- Required
                                                    Authorizations

                               Responses
                               Signature ------->

                               <~~~~~~~~Validation~~~~~~~~>


                               CSR
                               Signature ------->

      <~~~~~~Await issuance~~~~~~> <~~~~~~Await issuance~~~~~~>

              <-------------------------------- Certificate
```

                      Figure 1: End to end flow

## 2.3.  Delegated Identity Profile

## 2.3.1.  Order Object on the NDC-IdO side

   The Order object created by the NDC:

   o  MUST contain identifiers with the new "delegated" field set to
      true;
   o  MUST NOT contain the notBefore and notAfter fields;
   o  MAY contain any of the "recurrent-*" fields listed in
      Section 3.1.1 of [I-D.ietf-acme-star];
   o  In case the identifier type is "dns", it MAY contain a "cname"
      field with the alias of the identifier in the NDC domain.  This
      field is used by the IdO to create the DNS aliasing needed to
      redirect the resolvers to the delegated entity.

```
POST /acme/new-order HTTP/1.1
Host: acme.dno.example
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://acme.dno.example/acme/acct/evOfKhNU60wg",
    "nonce": "5XJ1L3lEkMG7tR6pA00clA",
    "url": "https://acme.dno.example/acme/new-order"
  }),
  "payload": base64url({
    "identifiers": [
      {
        "type": "dns",
        "value": "abc.ndc.dno.example.",
        "delegated": true,
        "cname": "abc.ndc.example."
      }
    ],
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

The Order object that is created on the IdO:

o  MUST start in the "ready" state;
o  MUST contain an "authorizations" array with zero elements;
o  MUST NOT contain the "notBefore" and "notAfter" fields.

```
 {
   "status": "ready",
   "expires": "2016-01-01T00:00:00Z",

   "identifiers": [
    {
      "type": "dns",
      "value": "abc.ndc.dno.example.",
      "delegated": true,
      "cname": "abc.ndc.example."
    }
   ],

   "authorizations": [],

   "finalize": "https://acme.dno.example/acme/order/TO8rfgo/finalize"
 }
```

The IdO SHOULD copy any "recurrent-*" field from the NDC request into
the related STAR request to the ACME CA.

When the validation of the identifiers has been successfully
completed and the certificate has been issued by the CA, the IdO:

o  MUST move its Order resource status to "valid";
o  MUST copy the "star-certificate" field from the STAR Order;

The latter indirectly includes (via the NotBefore and NotAfter HTTP
headers) the renewal timers needed by the NDC to inform its
certificate reload logic.

```
{
  "status": "valid",
  "expires": "2016-01-01T00:00:00Z",

  "identifiers": [
   {
     "type": "dns",
     "value": "abc.ndc.dno.example.",
     "delegated": true,
     "cname": "abc.ndc.example."
   }
  ],

  "authorizations": [],

  "finalize": "https://acme.dno.example/acme/order/TO8rfgo/finalize",

  "star-certificate": "https://acme.ca.example/acme/order/yTr23sSDg9"
}
```

If an "identifier" object of type "dns" was included, the IdO MUST
validate the specified CNAME at this point in the flow.  The NDC and
IdO may have a pre-established list of valid CNAME values.  At the
minimum, the IdO MUST verify that both DNS names are syntactically
valid.

Following this validation, the IdO can add the CNAME records to its
zone:

```
    abc.ndc.dno.example. CNAME abc.ndc.example.
```

### 2.3.2.  Order Object on the IdO-CA side

When sending the Order to the ACME CA, the IdO SHOULD strip the
"delegated" and "cname" attributes sent by the NDC (Section 2.3.1).
The IdO MUST add the necessary STAR extensions to the Order.  In
addition, to allow the NDC to download the certificate using
unauthenticated GET, the IdO MUST add the recurrent-certificate-get
attribute and set it to true.

### 2.3.3.  Capability Discovery

In order to help a client to discover support for this profile, the
directory object of an ACME server MUST contain the following
attribute inside the "meta" field:

o  star-delegation-enabled: boolean flag indicating support for the
   profile specified in this memo.  An ACME server that supports this
   delegation profile MUST include this key, and MUST set it to true.

### 2.3.4.  On Cancelation

It is worth noting that cancelation of the ACME STAR certificate is a
prerogative of the IdO.  The NDC does not own the relevant account
key on the ACME CA, therefore it can't issue a cancelation request
for the STAR cert.  Potentially, since it holds the STAR cert private
key, it could request the revocation of a single STAR certificate.
However, STAR explicitly disables the revokeCert interface.

### 3.  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 considers several solutions
addressing different delegation requirements.  This section discusses
two of these particular requirements in the context of the STAR
delegation workflow.

### 3.1.  Multiple Parallel Delegates

In some cases the content owner (IdO) would like to delegate
authority over a web site to multiple NDCs (CDNs).  This could happen
if the IdO has agreements in place with different regional CDNs for
different geographical regions, or if a "backup" CDN is used to
handle overflow traffic by temporarily altering some of the CNAME
mappings in place.  The STAR delegation flow enables this use case
naturally, since each CDN can authenticate separately to the IdO (via

   its own separate account) specifying its CSR, and the IdO is free to
   allow or deny each certificate request according to its own policy.

## 3.2.  Chained Delegation

   In other cases, a content owner (IdO) delegates some domains to a
   large CDN (uCDN), which in turn delegates to a smaller regional CDN,
   dCDN.  The DNO has a contractual relationship with uCDN, and uCDN has
   a similar relationship with dCDN.  However IdO may not even know
   about dCDN.

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

   One thing that might be necessary at the interface between uCDN and
   dCDN is a mechanism by which the uCDN can advertise:

   o  The namespace that is made available to the dCDN to mint its
      delegated names;
   o  The policy for creating the key material (allowed algorithms,
      minimum key lengths, key usage, etc.) that the dCDN needs to
      satisfy.

## 4.  IANA Considerations

   [[RFC Editor: please replace XXXX below by the RFC number.]]

## 4.1.  New fields in the "meta" Object within a Directory Object

   This document adds the following entries to the ACME Directory
   Metadata Fields:

```
         +-------------------------+------------+-----------+
         | Field Name              | Field Type | Reference |
         +-------------------------+------------+-----------+
         | star-delegation-enabled | boolean    | RCF XXXX  |
         +-------------------------+------------+-----------+
```

## 5.  Security Considerations

   TBD

## 6.  Acknowledgments

## 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-16 (work in progress),
          October 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.

[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>.

[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>.

### 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.

## Appendix A.  Document History

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

### A.1.  draft-sheffer-acme-star-delegation-00

o  Initial version, some text extracted from draft-sheffer-acme-star-requests-02

Authors' Addresses

Yaron Sheffer
Intuit

EMail: yaronf.ietf@gmail.com


Diego Lopez
Telefonica I+D

EMail: diego.r.lopez@telefonica.com


Antonio Agustin Pastor Perales
Telefonica I+D

EMail: antonio.pastorperales@telefonica.com


Thomas Fossati
Nokia

EMail: thomas.fossati@nokia.com