Short-Term Certificates

DRAFT-IETF-ACME-STAR-00

YARON SHEFFER, DIEGO LOPEZ, THOMAS FOSSATI, OSCAR GONZALEZ DE DIOS, ANTONIO PASTOR PERALES

IETF-99, PRAGUE

Motivation

Delegate the authorization to publish a web site

Securely: owner can revoke the authorization at any time

And with no change to the client side (browser)

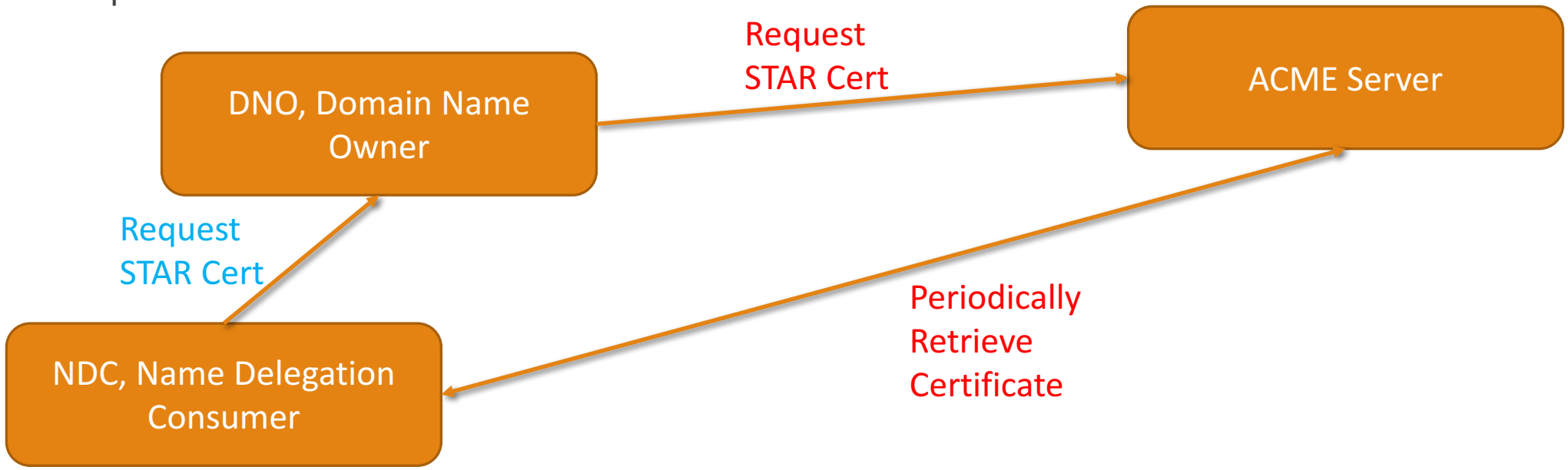
Initial use case: CDN

Also identified Public Cloud and IOT use cases

Document Status

Split the draft in two:

- **draft-ietf-acme-star-00**: adopted by this group, an ACME extension for short-term renewable certs
- **draft-sheffer-acme-star-request-00**: non-WG document, protocol for the NDC to create the initial request



The ACME Extension

We are adding a few attributes to the Order resource:

```
{
    "recurrent": true,
    "recurrent-total-lifetime": 365,
    "recurrent-certificate-validity": 7
}
```

A server that doesn't implement the extension returns a normal unextended Order object, and the client will likely abort

Open: days? Minutes? Picoseconds?

Fetching the STAR Certificates

All are dispensed from the single certificate endpoint

Lifetime indicated by an `Expires` header

- Apparently incorrect; use a private header?
- Or have the DNC parse the cert to extract the expiry?

Revocation

Adding Order cancellation to ACME

```
DELETE /acme/order/1 HTTP/1.1
Host: acme-server.example.org
```

How to authenticate this request?

Martin proposed to replace with a POST, and have the JWS signature take care of that

- But semantics is iffy

TODO

More cleanup to remove remnants of the NDC-to-DNO part

Discussion of Certificate Transparency

Additional comments from the list

Simple enough to go to WGLC after -01

Creating the Certificate Request: draft-sheffer-acme-star-request-00

We propose to adopt it as a WG draft, as a second step

It provides context to the WG draft: why are we doing what we're doing

It is **not** restricted to CDNs

It absolutely needs to be interoperable, because there are different entities involved

The draft includes security guidance, and without it there are multiple ways to do it wrong

Thank You!