ACME STAR

Yaron Sheffer, Thomas Fossati, Diego Lopez, Antonio Pastor Perales

IETF 103, Bangkok
Document Status

draft-ietf-acme-star already went through WGLC, but no request for publication yet
Numerous recent changes, but mostly to synchronize with base ACME

Also comments from Sean – thanks!
Changes in -04

Base doc moved to POST-as-GET, this doc makes “GET” great again
Details below

A few terminology changes
Identity Owner to Identifier Owner

Clarification about certificate validity time
Mandatory certificate predating to ensure client can always use fetched cert

Removed support for the revokeCert endpoint
Server must return 403 Forbidden
Using GET in ACME-STAR

Server advertises support in the directory object

Identifier Owner requests support with a new attribute in the Order object

  The Order object includes this attribute when successful

Now, the Client can use a GET to fetch the certificate

  Virtually unchanged from the previous version
Next Steps?
Doc was assigned to ACME by SecDispatch
ACME participants proposed to redo as an ACME profile
This profile now published as draft-sheffer-acme-star-delegation-00
Message Sequence

NDC                      IdO                   CA
Client              Server  Client             Server

Order
Signature -------->
[ No identity validation ]
CSR
Signature -------->

Order'
Signature -------->

Responses
Signature -------->

<~~~~~~~~Validation~~~~~~~~>
CSR
Signature -------->

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

<---------------------------- Certificate
Some Protocol Details

IdO has its own account management

The NDC-to-IdO protocol is somewhat restricted
   No authorizations, hence a simpler state machine

Added CNAME identity management

Next slide
CNAME Management

New *delegated* attribute to the *identifier* object of type DNS NDC indicates to IdO what name it will use locally for the delegated name

To close the delegation loop by including automated DNS provisioning

"identifiers": [

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

Open Issue: Restrict to STAR

We can envision cases where long term (normal) certs are delegated

Do we want to support them here?
Next Steps

We request adoption as a WG document