Authority Tokens for ACME & TNAuthlist

IETF 103

ACME WG

Jon & Chris - กรุงเทพฯ - Nov 2018

Authority Token Challenge

- Identified a generic need for authorities to provide tokens to a CA to respond to challenges
  - Surely any number of namespaces have authorities who could generate tokens
    - Inspired by the STIR case, but this could work for domains even
  - Requires the ACME server has some trust relationship with the authority
- draft-ietf-acme-authority-token-01
  - Framework for tokens that allow authorities trusted by the CA to attest client ownership of names
    - CA can then issue certs via ACME for particular names
  - Need some sort of typing mechanism for tokens, and a means to contact authorities

Example challenge

```
"challenges": [
        {
          "type": "tkauth-01",
          "tkauth-type": “ATC",
          "token-authority": "https://authority.example.org/authz",
          "url": "https://boulder.example.com/authz/asdf/0"
          "token": "IlirfxKKXAsHtmzK29Pj8A" }
        ]
```

- The tkauth-type is governed by a registry
  - Specifies the syntax of the token
    - Today we only specify one initial registration, for JWT (do we need more?)
  - It is the identifier type in the challenge that tells you what you are asking the authority to attest
- The token-authority contains an optional URL
  - A hint for where clients can get a token
  - Not mandatory to follow, clients may already know where to get tokens from some out-of-band source

The “ATC” tkauth-type

- “ATC” tkauth-type based on JWT
  - Described in the TNAuthlist document
- Example ACME response with a JWT
  - The JWT itself is the “ATC” payload in **bold**

```
{ "protected": base64url({
  "alg": "ES256",
  "kid": "https://boulder.example.com/acme/reg/asdf",
  "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
  "url": "https://boulder.example.com/acme/authz/asdf/0" }),
  "payload": base64url({ "ATC": "evaGxfADs...62jcerQ" }),
  "signature": "5wUrDI3eAaV4wl2Rfj3aC0Pp--XB3t4YYuNgacv_D3U" }
```

Updates & To Do

- Editorial fixes
- Updated the examples in the TNAuthlist draft to the latest version of ACME
- Patched SHAKEN errata, reviewed over at ATIS

- To Do
  - Patch in example of a ReSTful interface for token acquisition draft
    - Thinking is it will be an example rather than mandatory to implement – potentially several ways to acquire a token
  - Other housekeeping in both drafts (Sec Cons, etc.)
  - Should be ready for review and last call after another rev of each