Authority Tokens for ACME

IETF 104
ACME WG
Jon & Chris - Praha - Mar 2019
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-03
  – 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": "example-01",  
    "tkauth-type": "ex",  
    "token-authority": "https://authority.example.org/authz",  
    "url": "https://boulder.example.com/authz/asdf/0"  
    "token": "IlirfxKXXAsHtmzK29Pj8A"  
  }  
]

• The tkauth-type is governed by a registry  
  – Specifies the syntax of the token  
    • Today we only specify one initial registration, for JWT  
    • 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 ACME TNAuthlist document
- Example ACME response with a JWT
  - The JWT itself is the “ATC” payload in bold

```json
{
  "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": { "tktype":... } }),
  "signature": "5wUrDI3eAaV4wl2Rfj3aC0Pp--XB3t4YYuNgacv_D3U"
}
```
What’s New in AT -03 (and -02)

• Fleshed out the REST interface for token acquisition
  – Cribbed from the ATIS specification
• Better ATC structure
• Introduced the concept of asking for a particular authority scope
  – Basically, you post the ATC object you will want the Token Authority to issue, scope is “tkvalue”
• So, can you ask for a CA cert in ACME?
  – Why not? CSR with CA boolean set to true
  – We have a optional flag for that boolean in ATC
• Added some minimal IANA Considerations
ATC Structure

"atc":{
"tktype":"TnAuthList",
"tkvalue":"F83n2a...avn27DN3==",
"fingerprint":"SHA256 56:...8:E3"
}

• Optional element

"ca":true
Updates & To Do

• To Do
  – Housekeeping in both drafts (Sec Cons, etc.)

• Should be ready for review and last call after another rev of each draft