TNAuthList profile of ACME Authority Token

draft-ietf-acme-authority-token-tnauthlist-00

ACME Working Group

IETF102

Overview

- Moved document to WG document
- Updated to incorporate the suggested ASN.1 object in the token/challenge vs JSON representation
- Updated to explicitly support fingerprint including examples

TNAuthList Identifier

- type = “TNAuthList”
- value = Base64 encoded ASN.1 TNAuthList Object

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

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/1",
    "nonce": "5XJ1L3lEkMG7tR6pA00clA",
    "url": "https://example.com/acme/new-order"
  }),
  "payload": base64url({
    "identifiers": [{"type:"TNAuthList","value":"F83n2a...avn27DN3=="}],
    "notBefore": "2018-01-01T00:00:00Z",
    "notAfter": "2018-01-08T00:00:00Z"
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

Challenge/challenge response per ATC

```
HTTP/1.1 200 OK
Content-Type: application/json
Link: <https://example.com/acme/some-directory>;rel="index"

{
  "status": "pending",
  "expires": "2018-03-03T14:09:00Z",

  "identifier": {
    "type:"TNAuthList",
    "value":"F83n2a...avn27DN3=="
  },

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

```
POST /acme/authz/asdf/0 HTTP/1.1
Host: sti-ca.com
Content-Type: application/jose+json

{
 "protected": base64url({
 "alg": "ES256",
 "kid": "https://sti-ca.com/acme/reg/asdf",
 "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
 "url": "https://sti-ca.com/acme/authz/asdf/0"
}),
 "payload": base64url({
 "ATC": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"
}),
 "signature": "9cbg5JO1Gf5YLjjz...SpkUfcdPai9uVYYQ"
}
```

ATC token/“atc” claim

- all claims are per ATC, except “atc” as defined by this draft
- ATC claim contains key of “TNAuthList” and value
- Incorporates the fingerprint of the ACME client account key

```
{ "typ":"JWT",
  "alg":"ES256",
  "x5u":https://authority.example.org/cert
}

{
 "iss":"https://authority.example.org/authz",
 "exp":1300819380,
 "jti":"id6098364921",
 "atc":["TnAuthList","F83n2a...avn27DN3==",
   "SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3:BA:B9:19:81:F8:50:
    9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"]
}
```

Next Steps

- Comments?

- We think we are pretty complete for STIR/industry requirements and TNAuthList