ACME FOR ONIONS

draft-ietf-acme-onion

Q MISELL, GLAUCA DIGITAL

IETF 117, Monday 24th of July 2023

Fedi: @q@glauca.space
Email: q@as207960.net
SINCE IETF 116

- Adopted 🎉
- Reference CA implementation acmeforonions.org
- Certbot plugin for onion-csr-01 certbot-onion
- Tor Spec Proposal 343-rend-caa
WHY EVEN HAVE X.509 CERTIFICATES FOR TOR HIDDEN SERVICES?

- Secure cookies
- Content Security Policy
- HTTP/2
- PCI DSS
- Security-in-depth
GOALS
Define extensions to ACME to automate the issuance of X.509 certificates for Tor hidden services in line with the accepted methods in the CA/BF BR.

NON-GOALS
Any method not accepted by the CA/BF.
CURRENT STATE OF THINGS

- DigiCert (EV only)
- HARICA
CA/BF BR APPENDIX B

- § 3.2.2.4.18 - Agreed-Upon Change to Website v2
- § 3.2.2.4.19 - Agreed-Upon Change to Website - ACME
- § 3.2.2.4.20 - TLS Using ALPN
- § B.2.b - Special CSR
Clients can be oblivious to the fact that the identifier is a Tor hidden service with "http-01" or "tls-alpn-01" validation methods.

```json
{
    "type": "dns",
    "value": "bbcweb3hytmz...rad.onion"
}
```
NEW onion-csr-01 VALIDATION METHOD

Implements CA/BF BR § B.2.b

Clients prove control over the .onion domain by signing a CSR with the private key of the .onion domain.
OVERVIEW OF THE TOR HIDDEN SERVICE DESCRIPTOR
OUTER LAYER

Fetched with the service's blinded public key

hs-descriptor 3
descriptor-lifetime ...
descriptor-signing-key-cert
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
revision-counter ...
superencrypted
-----BEGIN MESSAGE-----
...
-----END MESSAGE-----
FIRST LAYER ENCRYPTED DATA

Encrypted with the service's (non-blinded) public key

desc-auth-type x25519
desc-auth-ephemeral-key ...
auth-client ...
auth-client ...
auth-client ...
encrypted
-----BEGIN MESSAGE-----
...
-----END MESSAGE-----
SECOND LAYER ENCRYPTED DATA

Encrypted with data from auth-client

create2-formats 2
introduction-point ...
onion-key ntor ...
auth-key
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
enc-key ntor ...
enc-key-cert
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
introduction-point ...
CLIENT AUTHENTICATION

Tor allows hidden services to restrict which clients can connect using client authentication.

New authKey field to allow hidden service operators to allow the CA's Tor client to read their hidden service descriptor to issue certificates.
CAA RECORDS

.onion domains aren't in the DNS, so standard CAA records can't be used. Instead, CAA records are encoded in the BIND zone file format the second layer hidden service descriptor.

```plaintext
1 create2-formats 2
2 single-onion-service
3 caa 128 issue "test.acmeforonions.org;validationmethods=onio"
4 caa 0 iodef "mailto:security@example.com"
5 introduction-point AwAGsAk5n...
```
CAA INTERACTION WITH CLIENT AUTHENTICATION

New field in the first layer hidden service descriptor to signal that there are CAA records in the second layer descriptor.

```
1 desc-auth-type x25519
2 caa-critical
3 auth-client ...
```
QUESTIONS?

Q MISSELL, GLAUCA DIGITAL

Slide deck available at magicalcodewit.ch/ietf117-slides/

Fedi: @q@glauca.space
Email: q@as207960.net