THIRD-PARTY DEVICE
ATTESTATION FOR ACME

RIFAAT SHEKH-YUSEF
IETF104, ACME WG, Prague, Czech Republic
27 March 2019
GOAL

• Automate the issuance of ACME certificate to a specific device with a specific Service URI, where the device and the Service URI are controlled by different entities.
INITIAL TRUST

Device

Client

customer.com

as.vendor.com

DA

acme.com

ACME CA
1. Create an account
2. Claim a device

1. Create an account
2. Prove control over customer.com
**Flow Overview**

1. Auth
2. JWT
3. CSR, JWT
4. Apply for Cert [CSR, JWT]
5. Certificate
6. Certificate

Device → as.vendor.com (DA) → acme.com (ACME CA) → Client (customer.com)

- Device
- as.vendor.com (DA)
- acme.com (ACME CA)
- Client (customer.com)
**CLIENT-CA INTERACTION**

[01] POST /new-order
    kid=customer.com/acme/acct/<acct>
    url=vendor.com/acme/new-order
    identifier=<mac>

[02] 201 Created
    finalize=customer.com/acme/order/asdf/finalize
    authorizations=vendor.com/acme/authz/1234

[03] POST /vendor.com/acme/authz/1234
    JWT

[04] 200 OK
    status=valid

[05] POST /customer.com/acme/order/asdf/finalize
    CSR

[06] 200 OK
    certificate=customer.com/acme/cert/asdf
DEVICE IDENTIFIER

{
  "type": "mac",
  "value": "<mac>"
}

JWT EXAMPLE

Header:
{
    "alg": "ES256",
    "typ": "JWT"
}

Body:
{
    "iss": "as.vendor.com",
    "sub": "<mac>",
    "aud": ["customer.com", "acme.com"]
}
The issued certificate must include the following identifiers:

- MAC Address
- Service URI
QUESTIONS?