3RD-PARTY DEVICE ATTESTATION FOR ACME

RIFAAT SHEKH-YUSEF

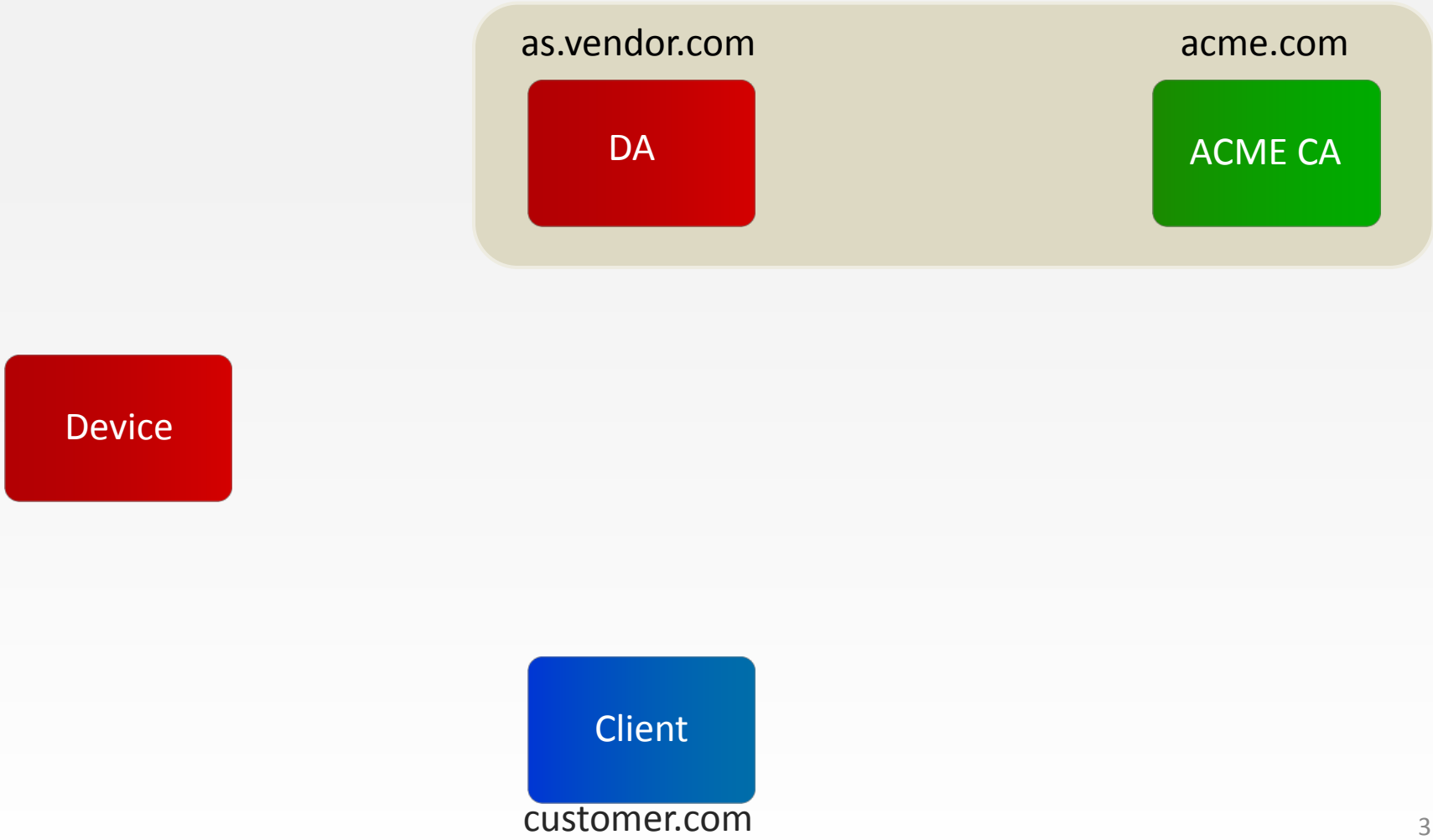
IETF104, ACME WG, Prague, Czech Republic

27 March 2019

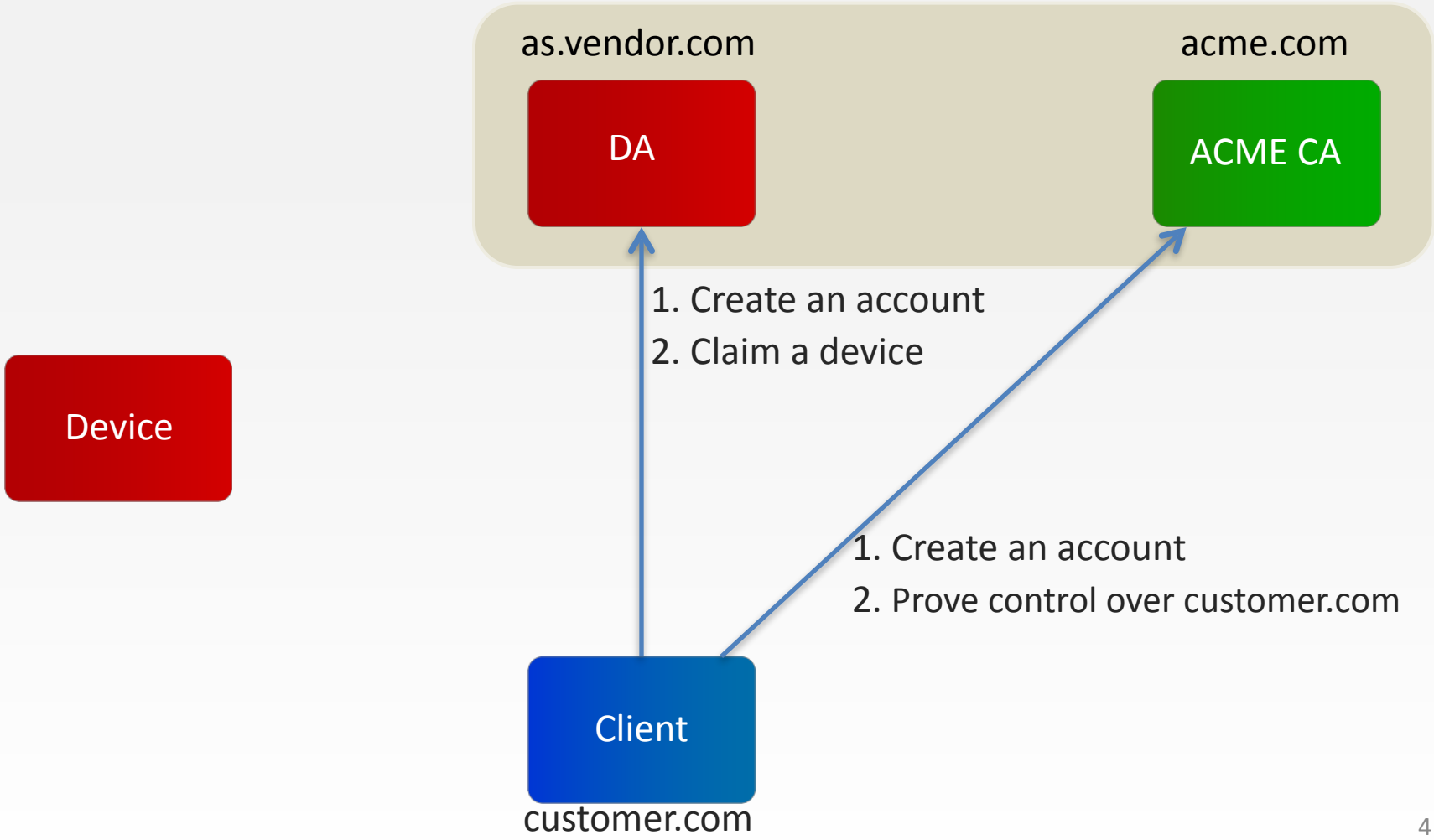
GOAL

- 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.

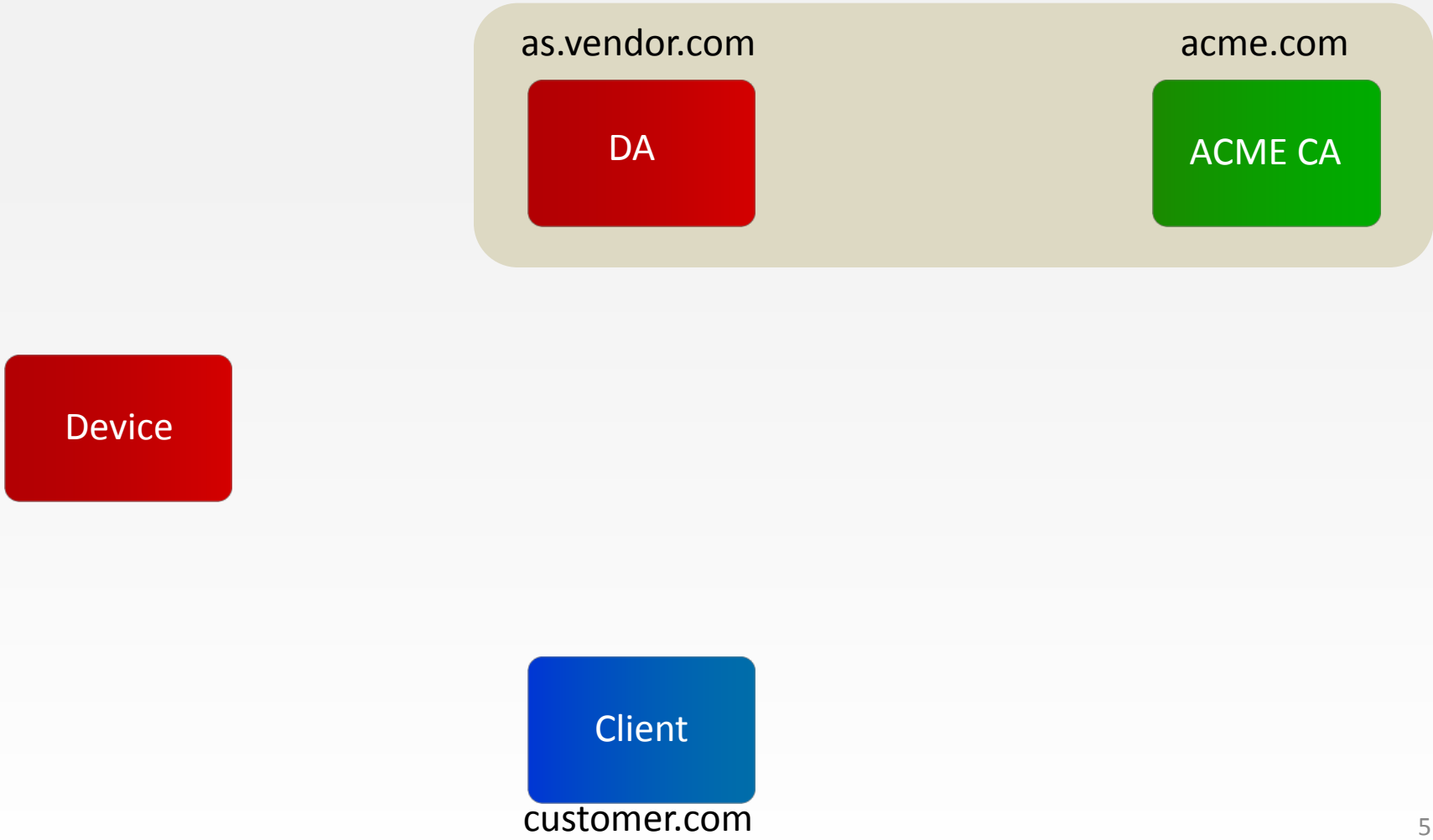
INITIAL TRUST



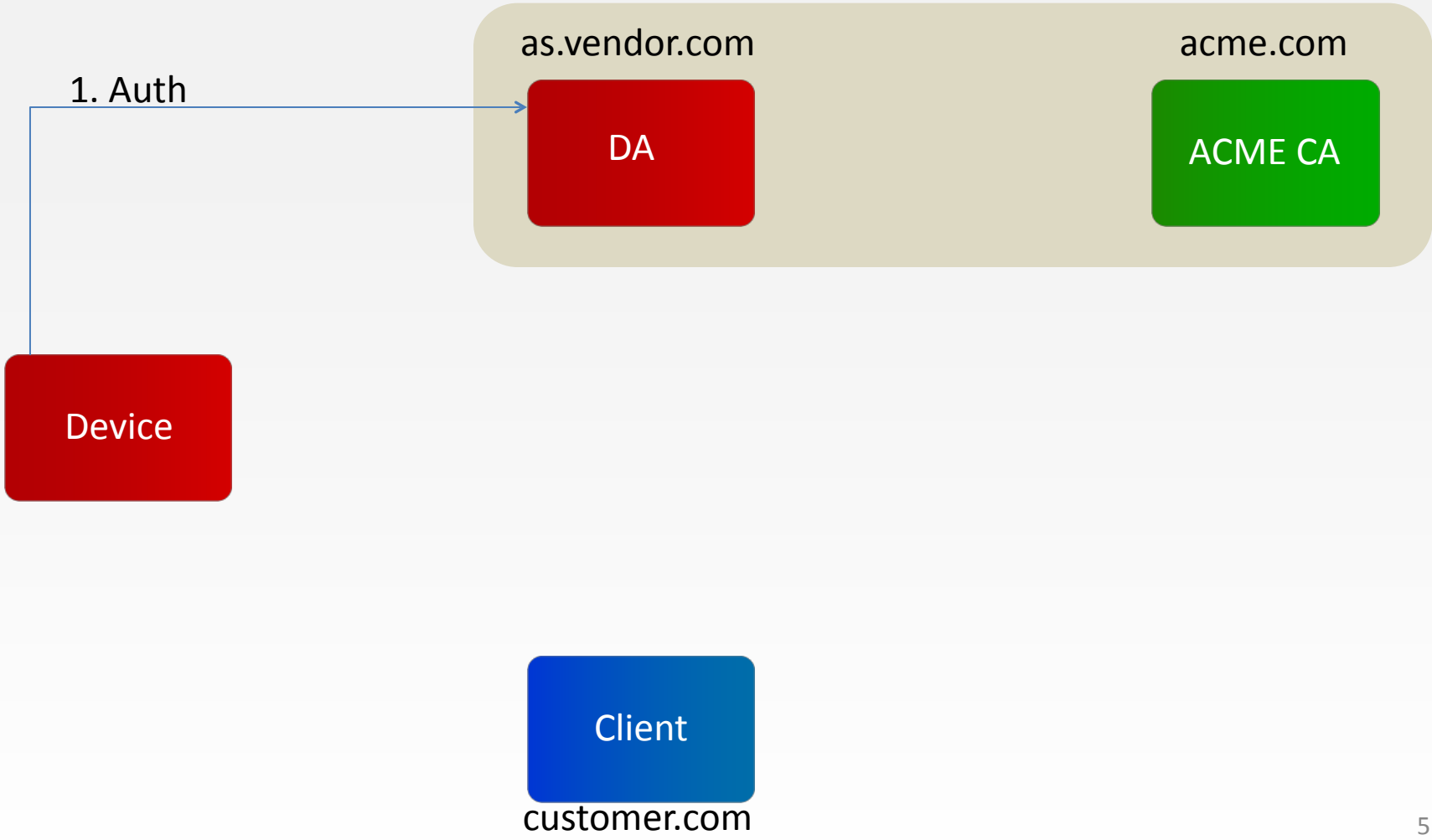
SETUP


as.vendor.com
acme.com
DA
ACME CA
1. Create an account
2. Claim a device
Device
1. Create an account
2. Prove control over customer.com
Client
customer.com

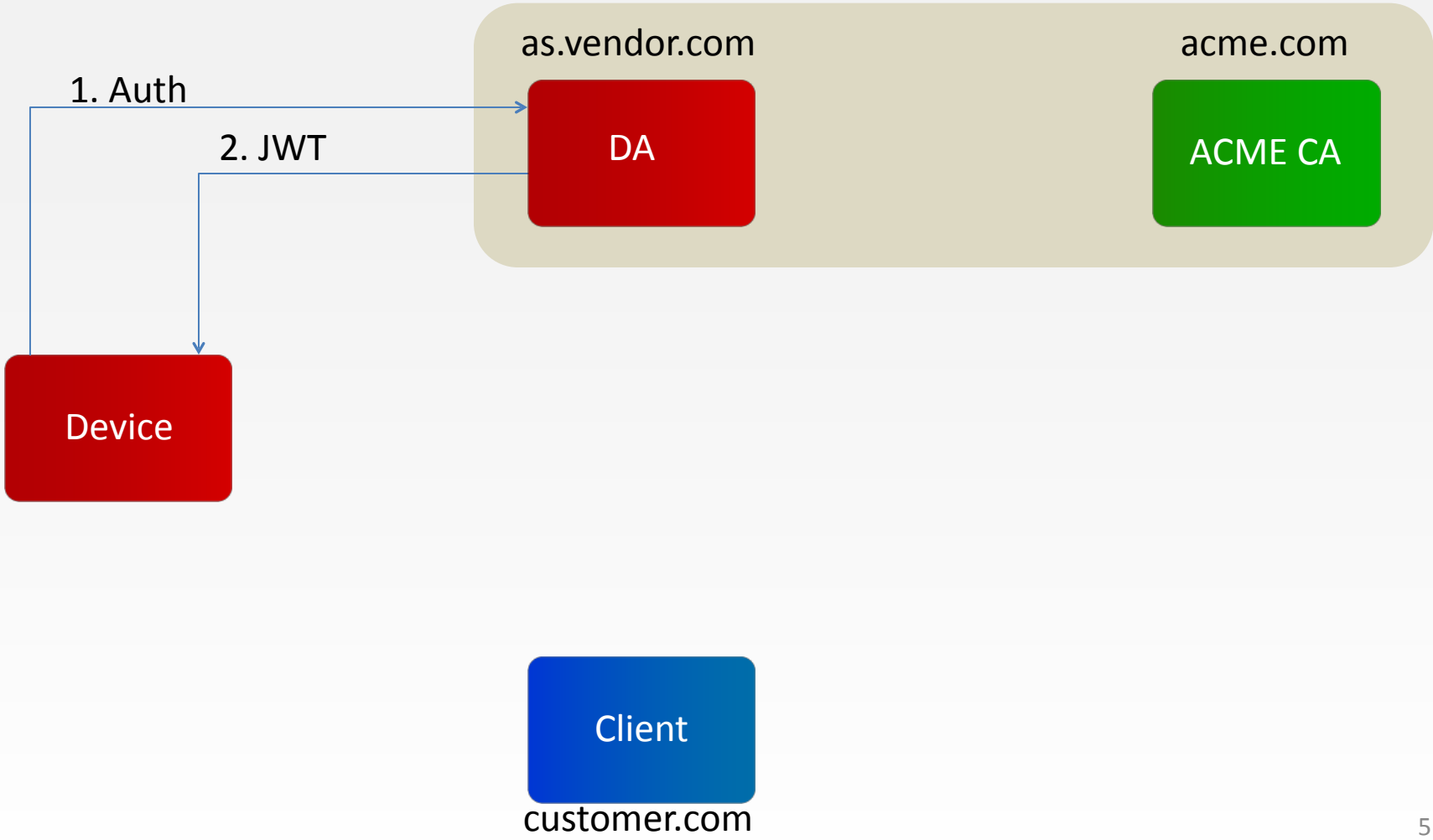
FLOW OVERVIEW



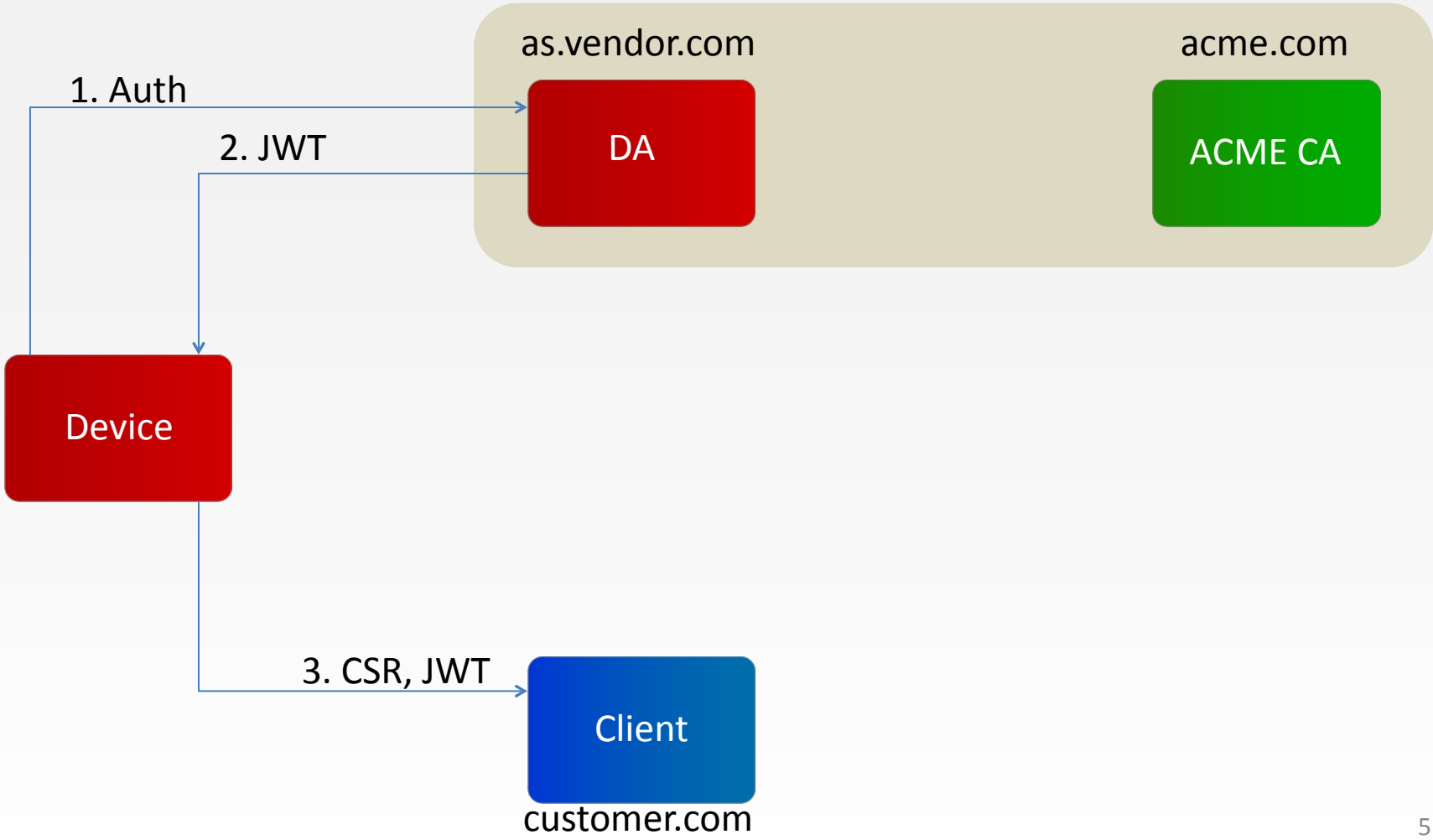
FLOW OVERVIEW



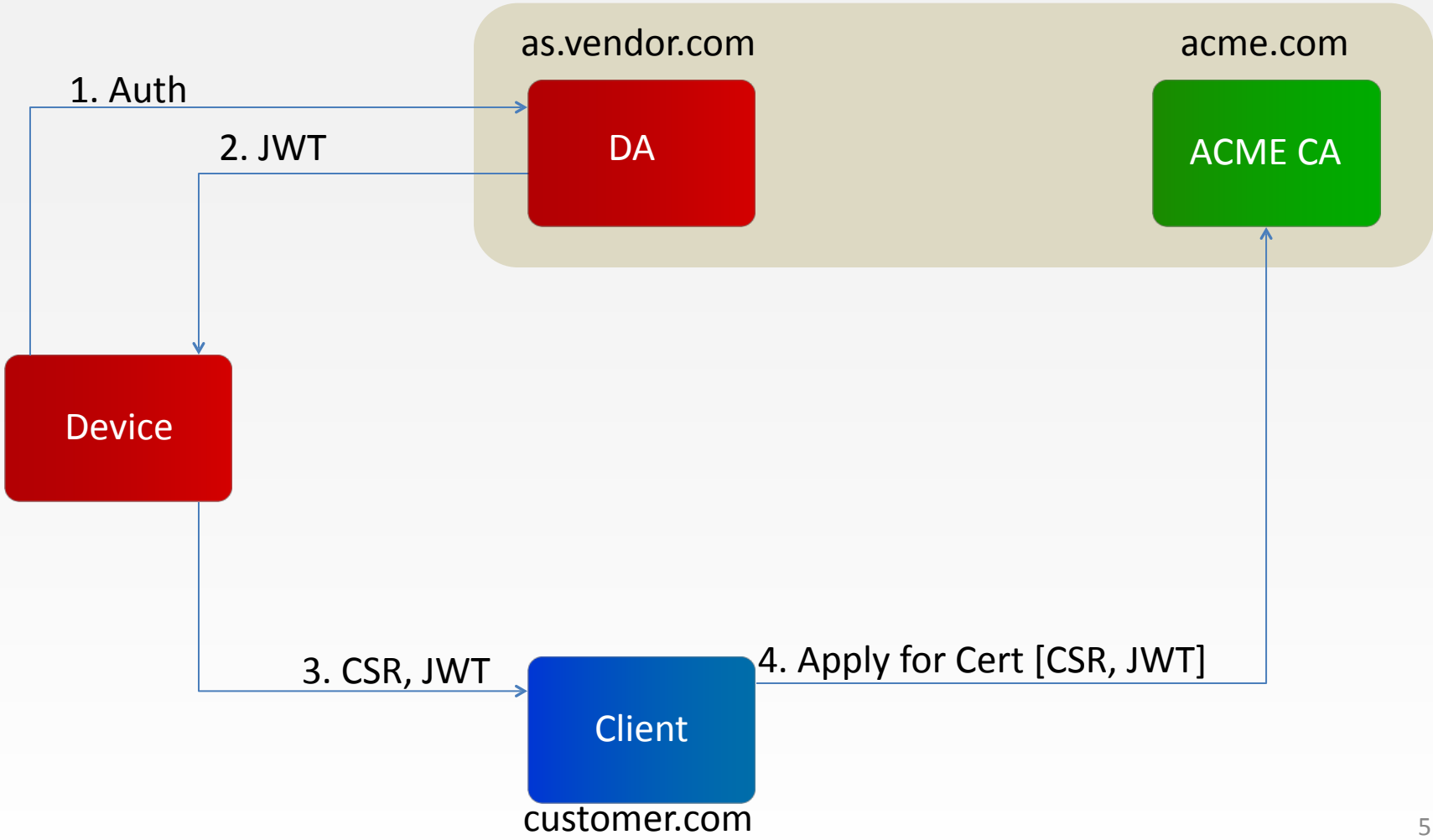
FLOW OVERVIEW



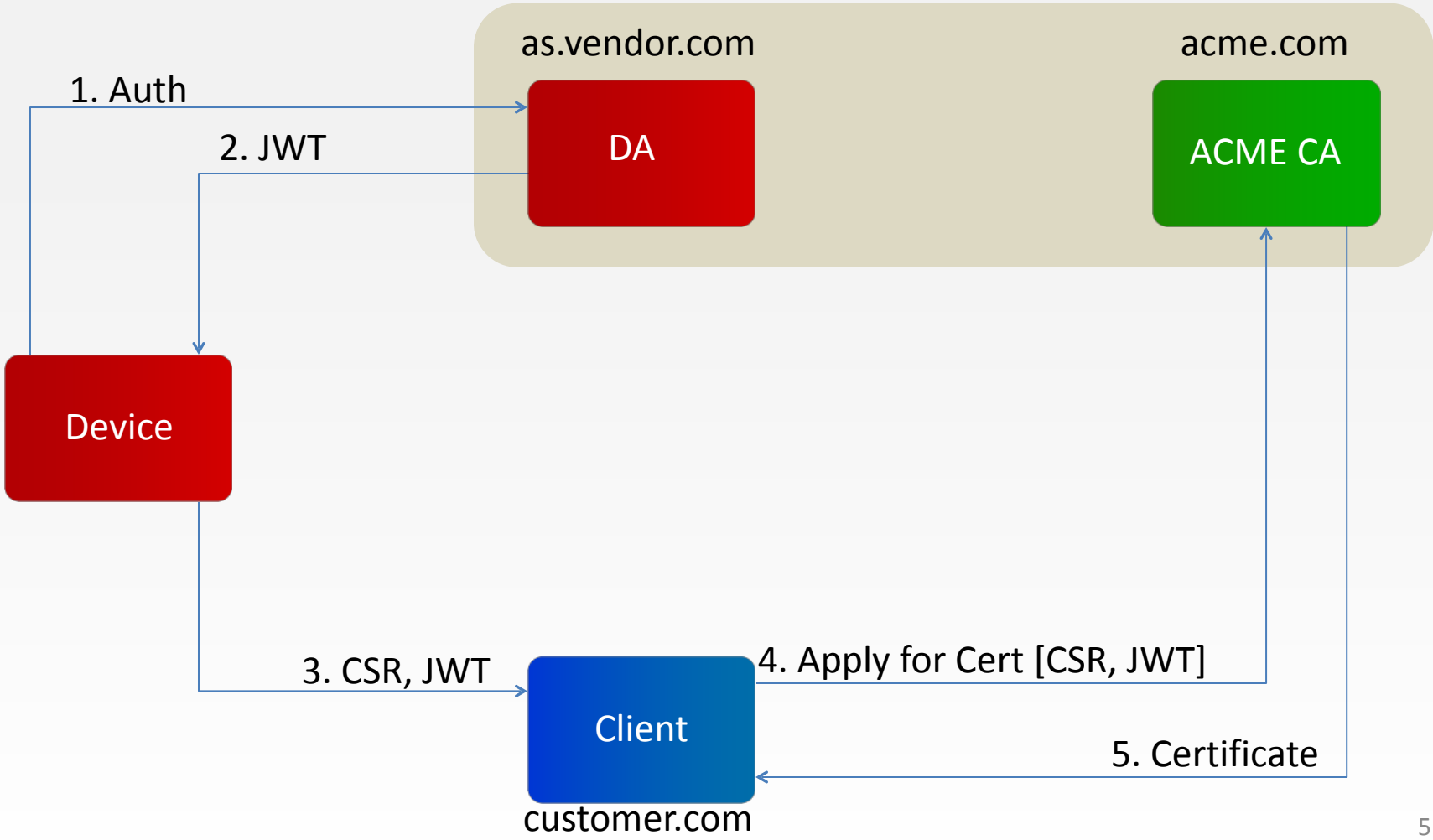
FLOW OVERVIEW



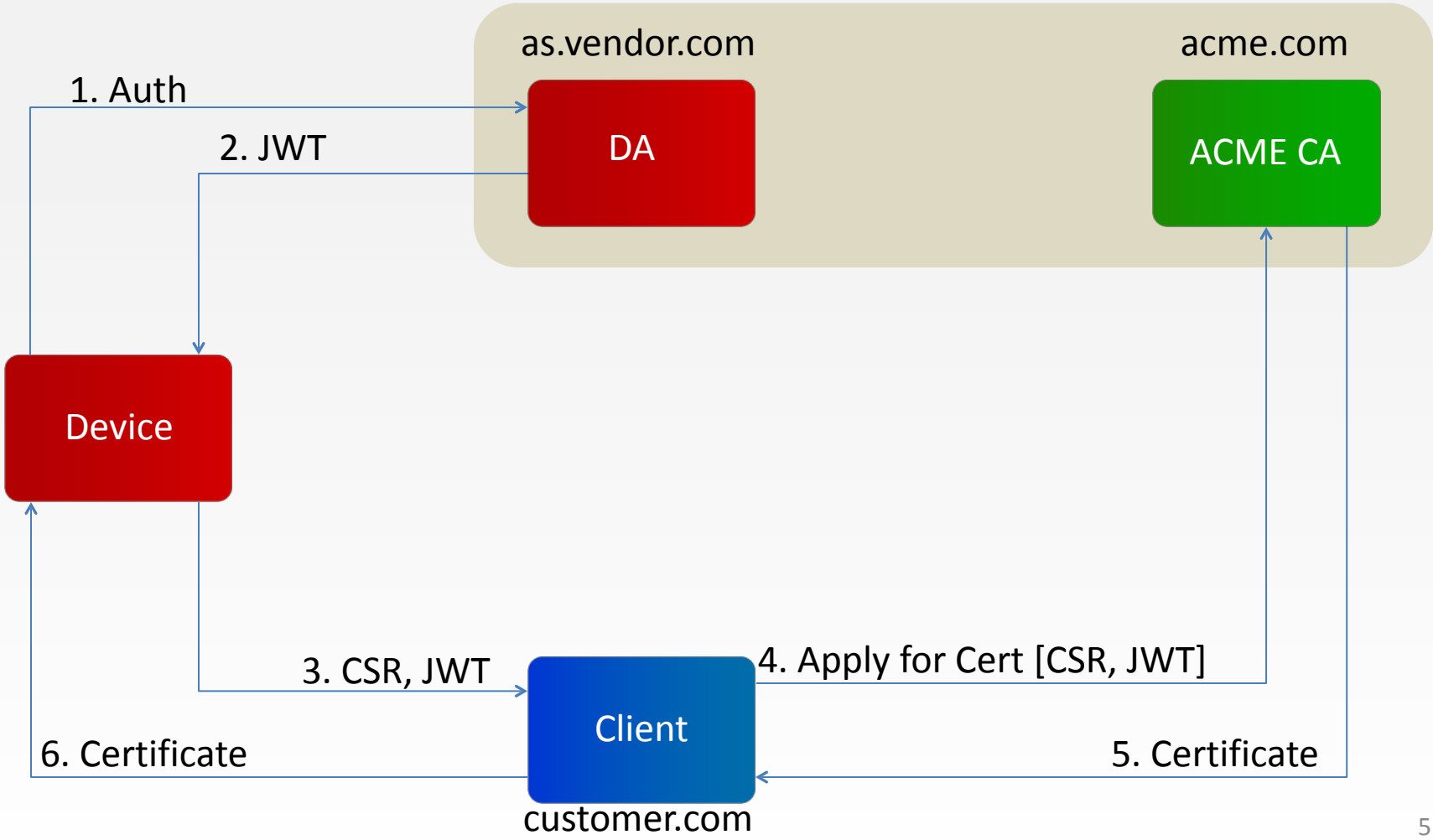
FLOW OVERVIEW



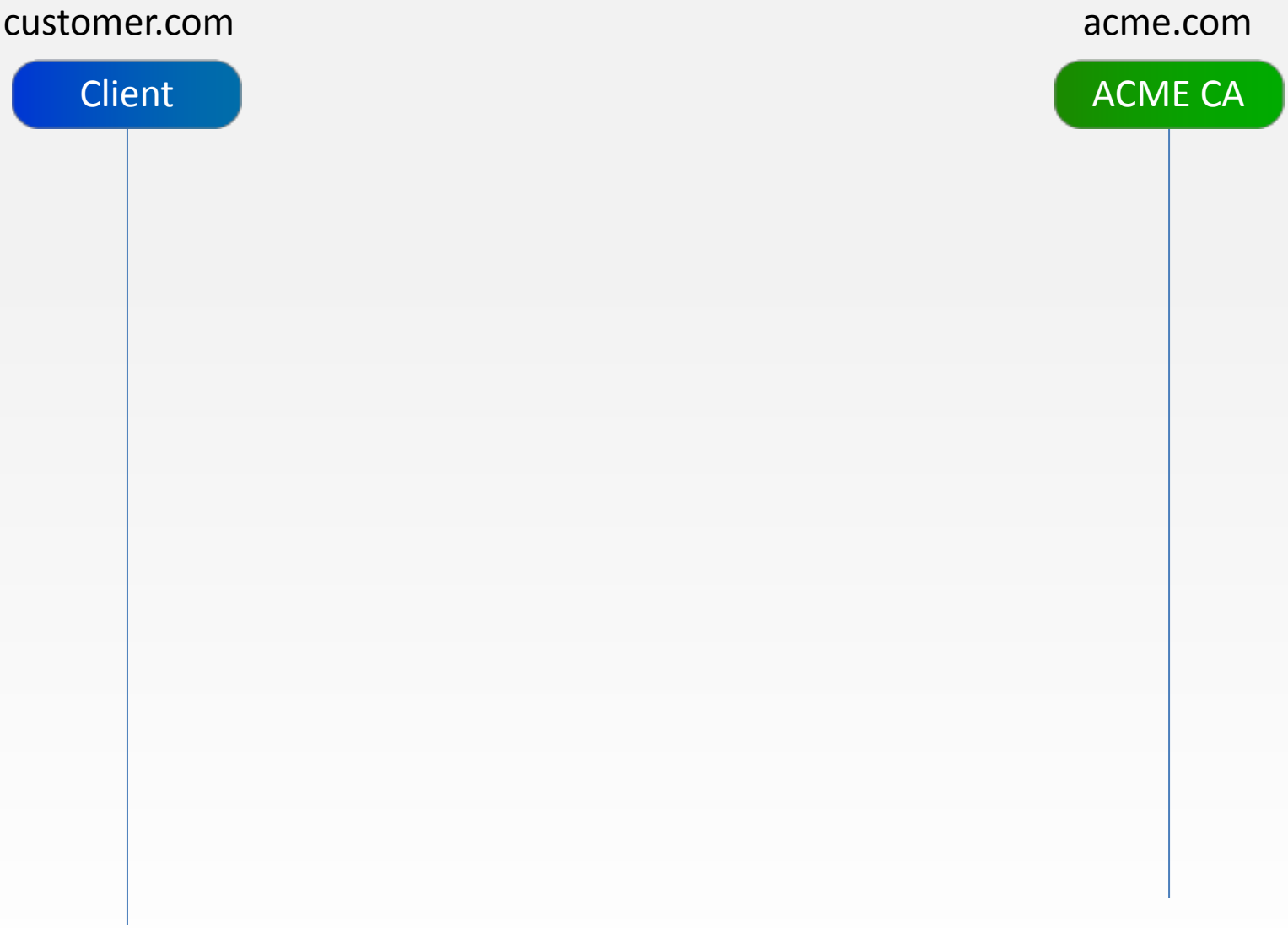
FLOW OVERVIEW



FLOW OVERVIEW

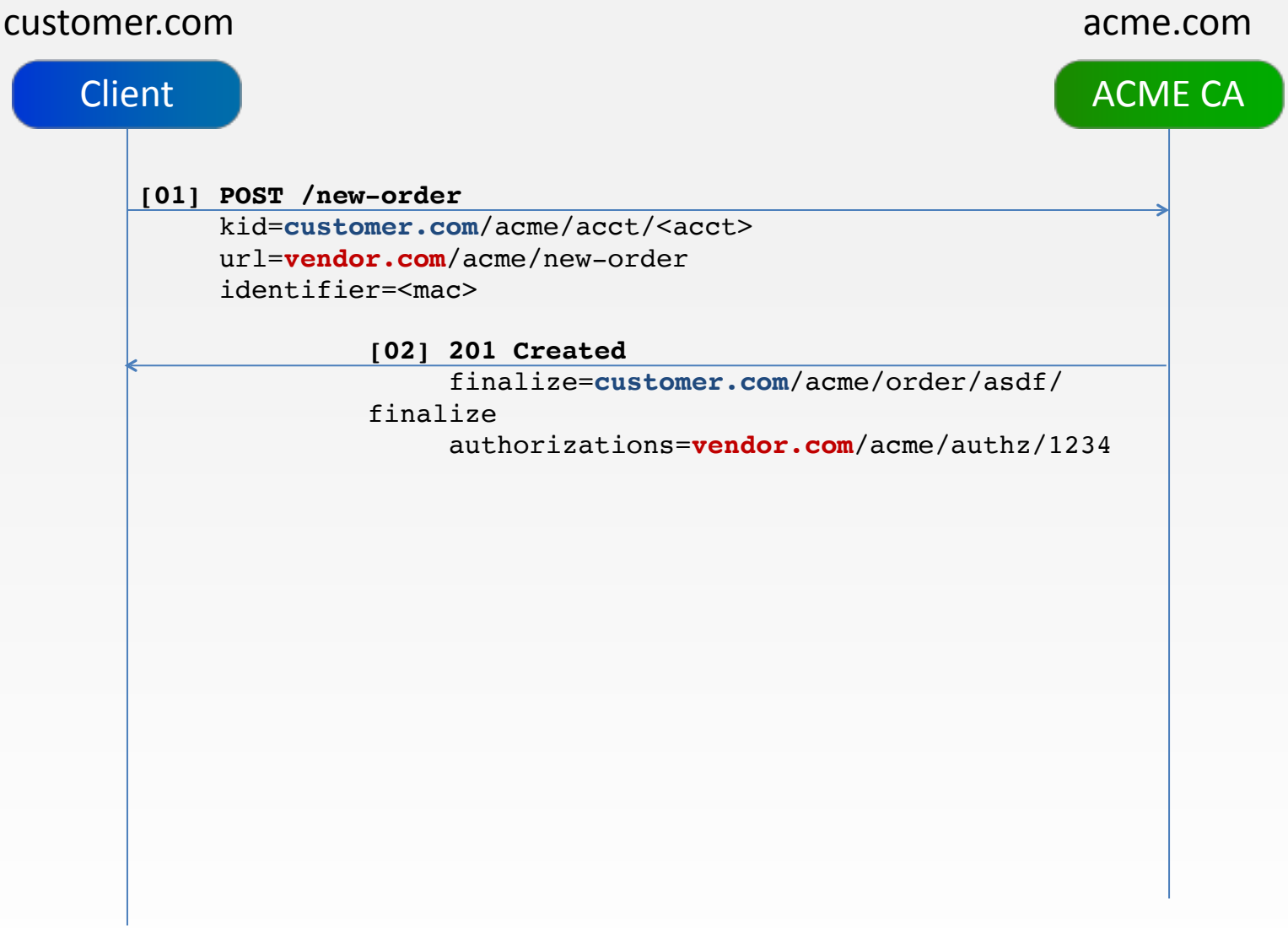


CLIENT-CA INTERACTION

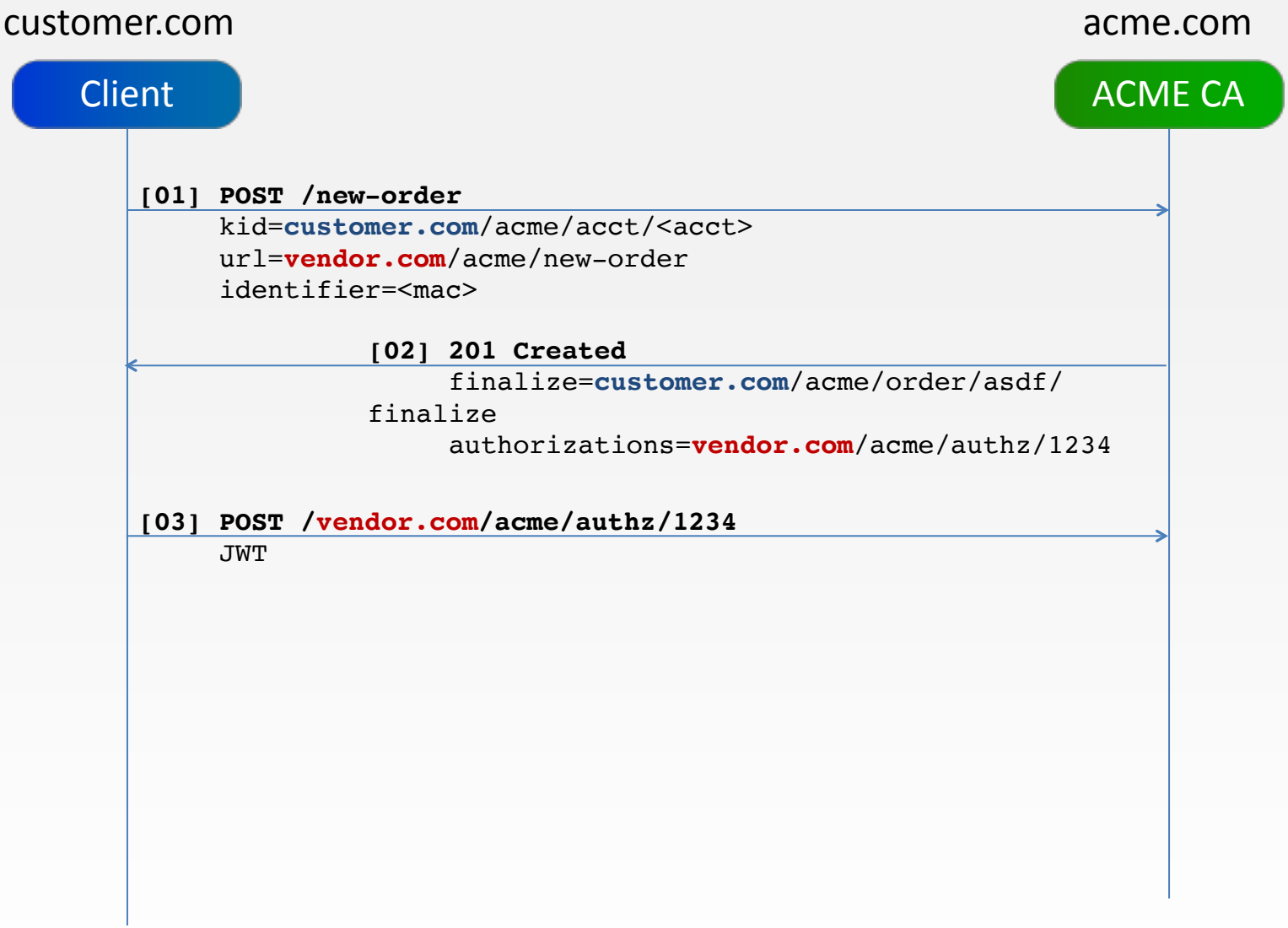


CLIENT-CA INTERACTION

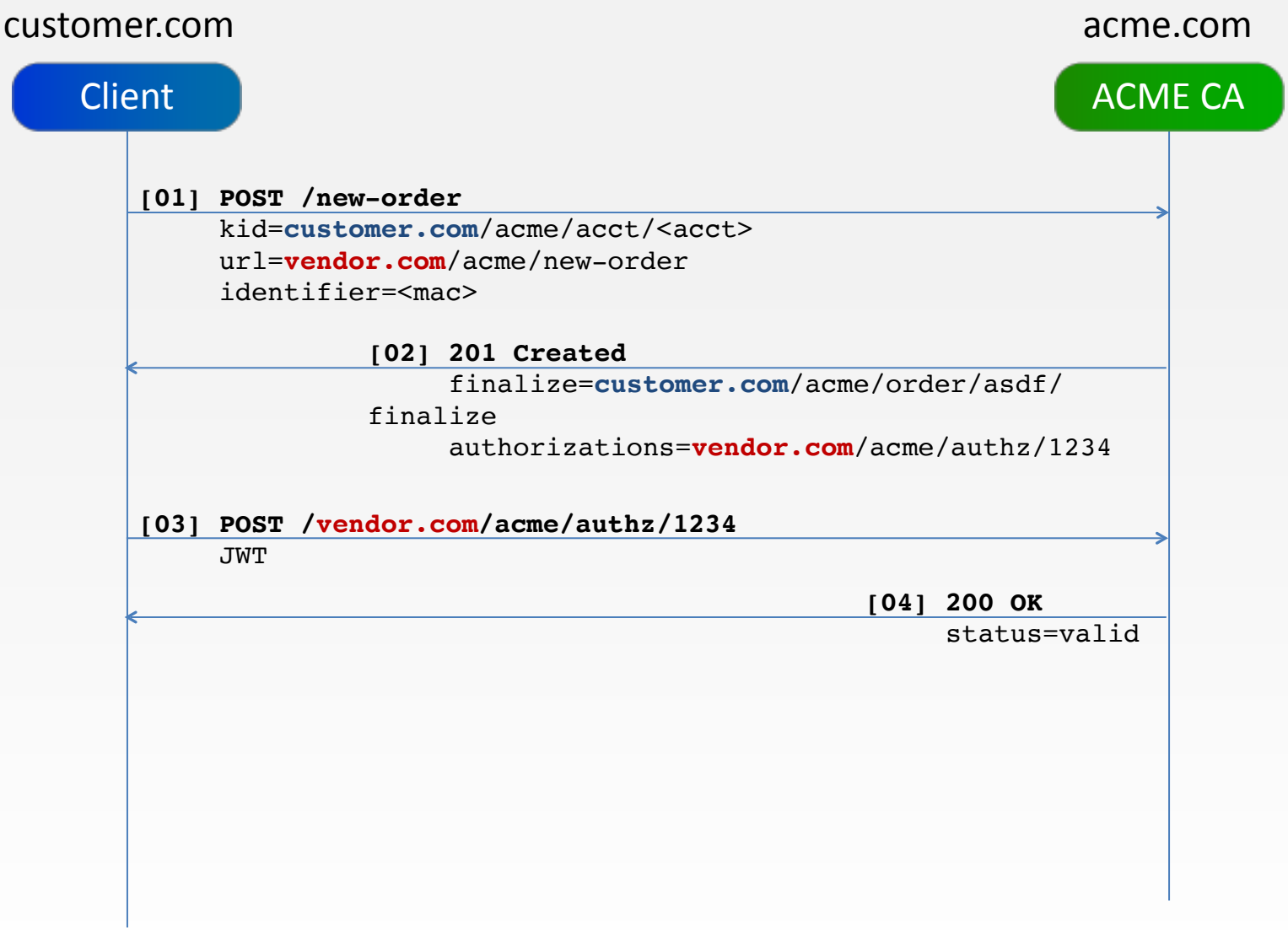
CLIENT-CA INTERACTION



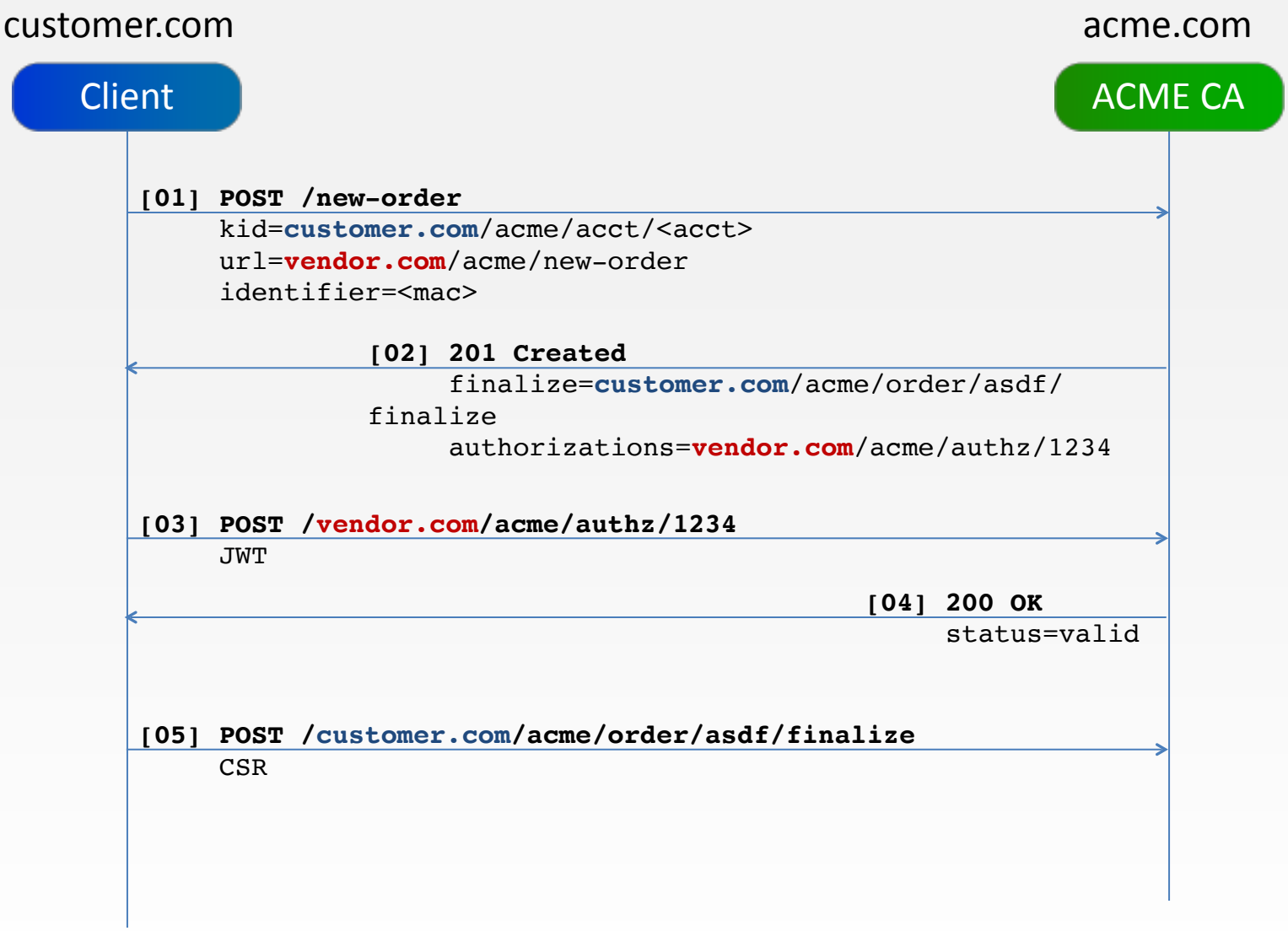
CLIENT-CA INTERACTION



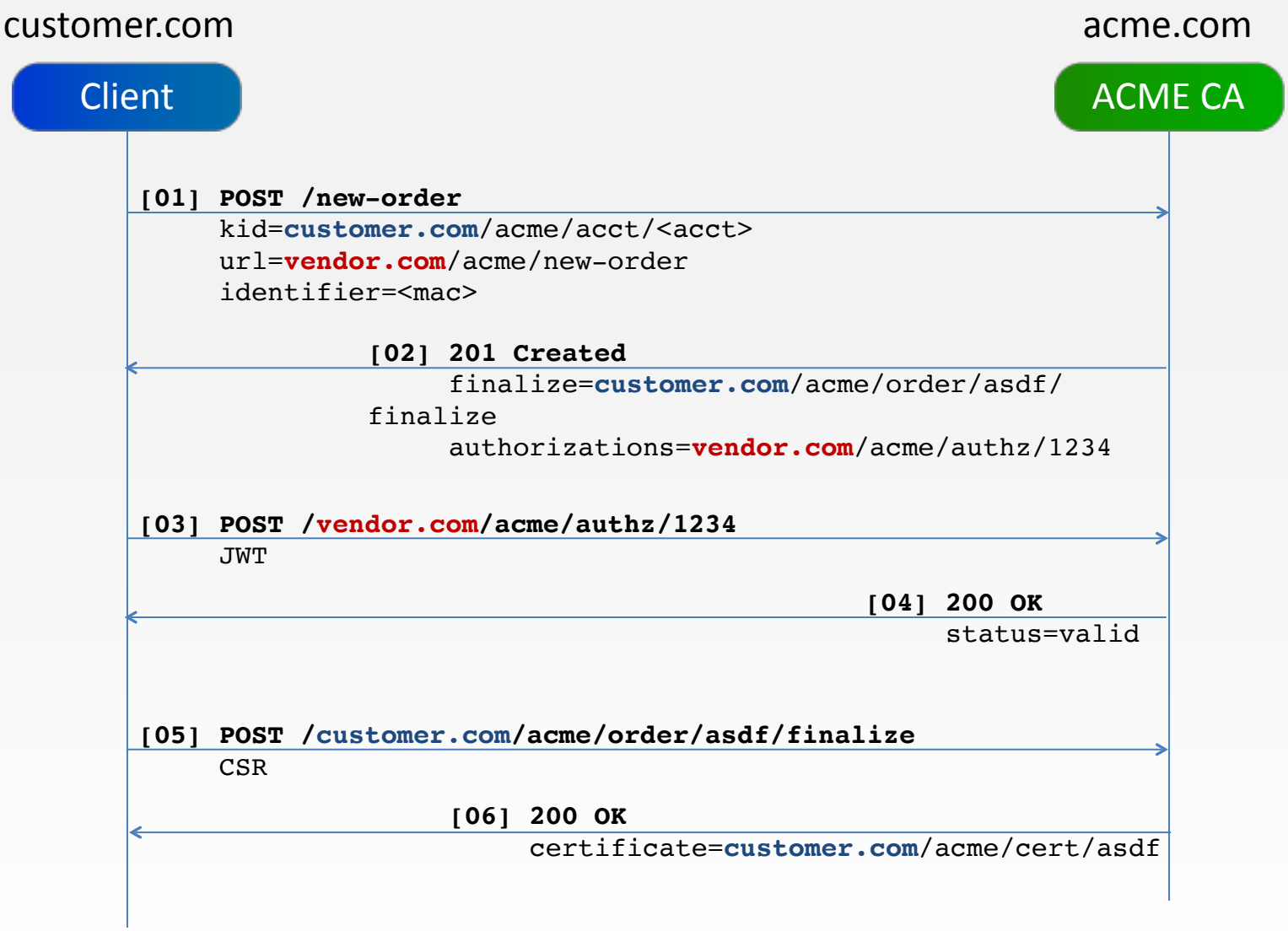
CLIENT-CA INTERACTION



CLIENT-CA INTERACTION



CLIENT-CA INTERACTION



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"]
}
```

CERTIFICATE IDENTIFIERS

The issued certificate must include the following identifiers:

- MAC Address
- Service URI

QUESTIONS?