

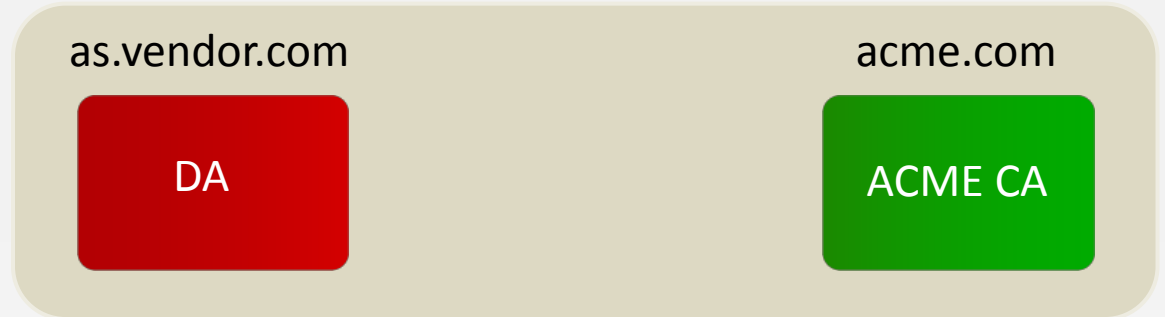
# **3<sup>RD</sup>-PARTY DEVICE ATTESTATION FOR ACME**

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

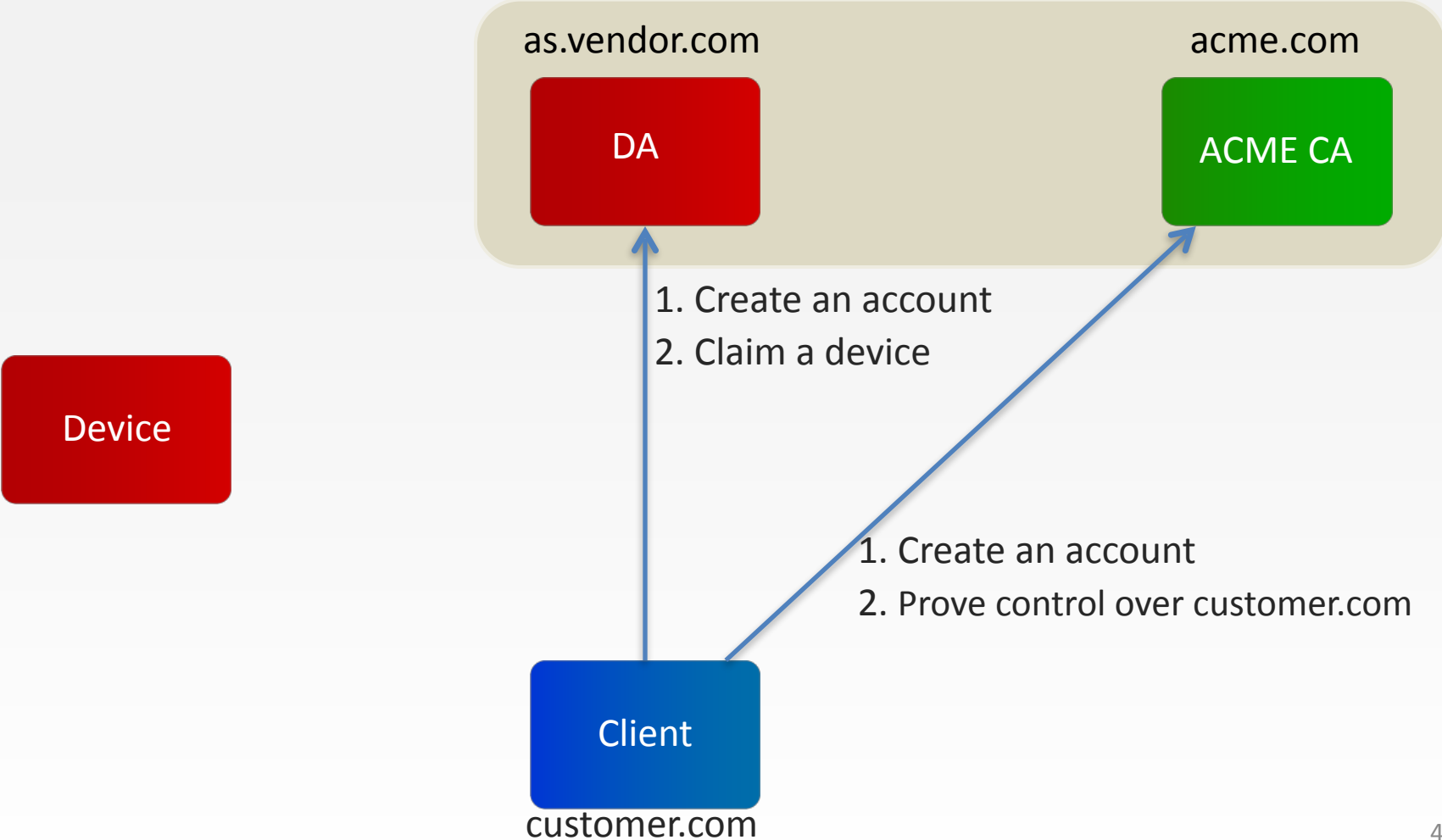
# GOAL

- 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.

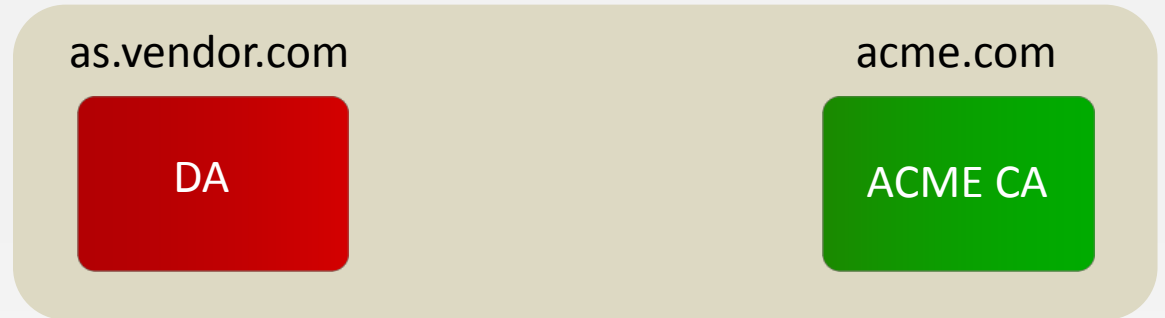
# INITIAL TRUST



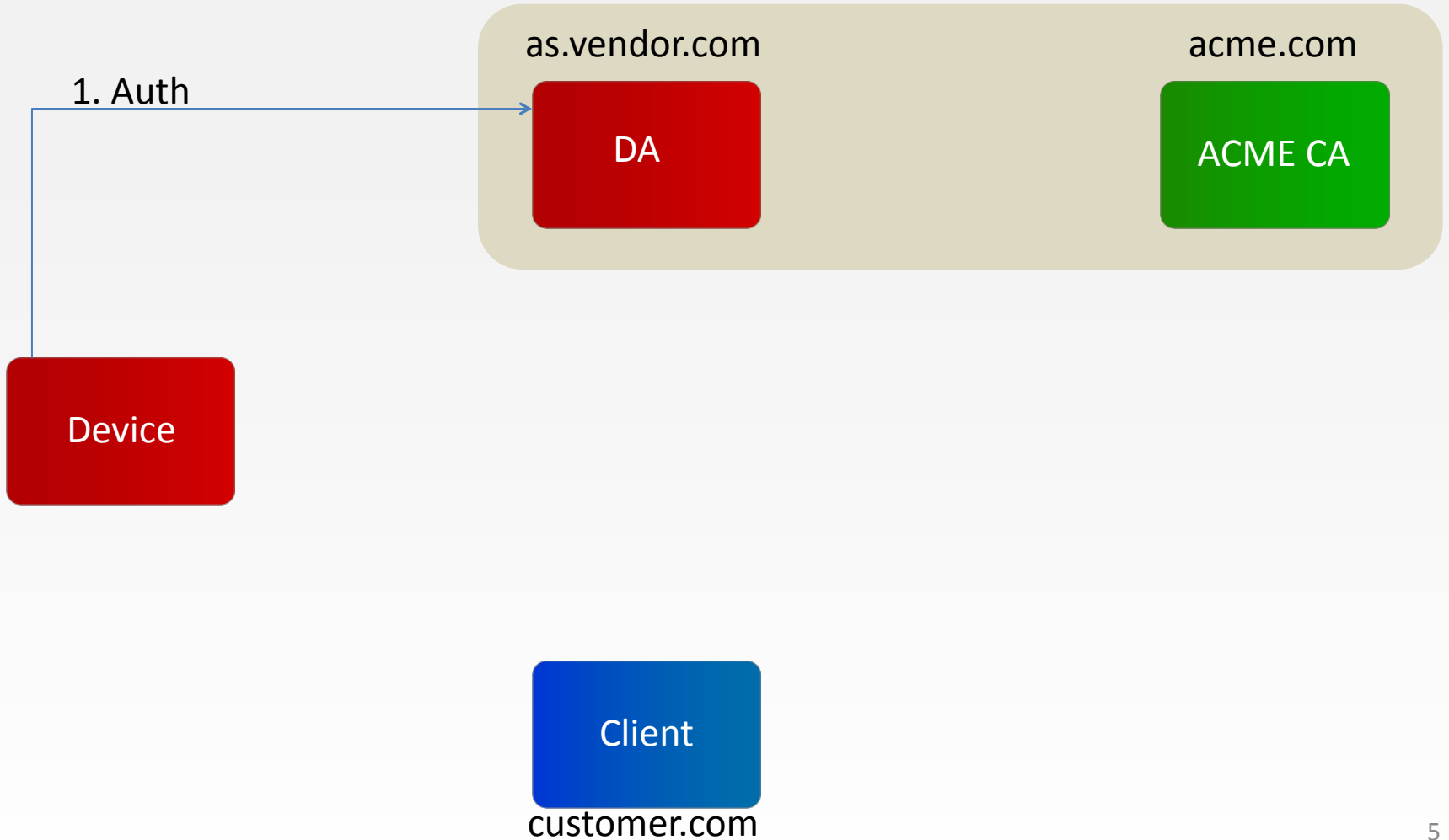
# SETUP



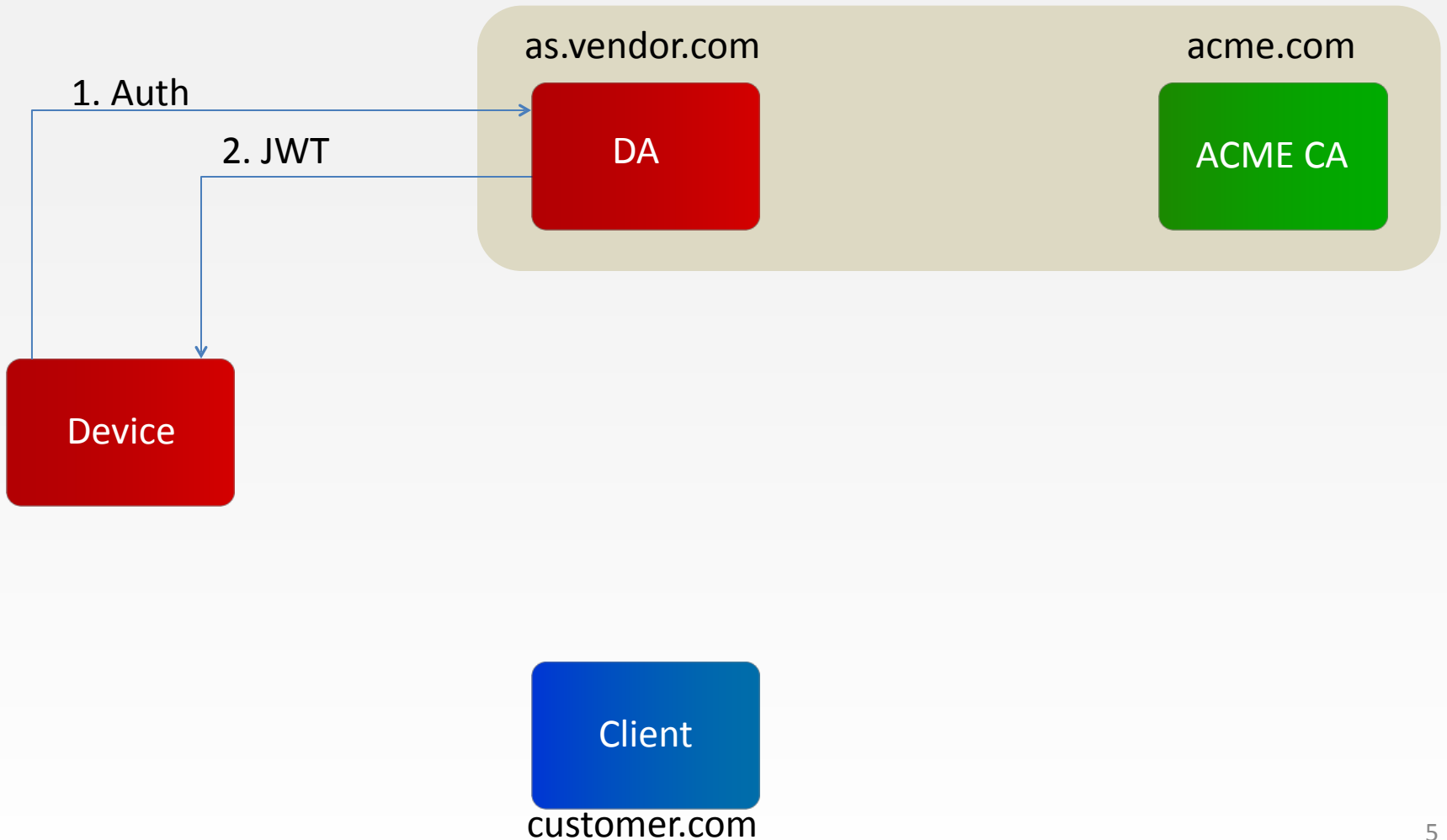
# FLOW OVERVIEW



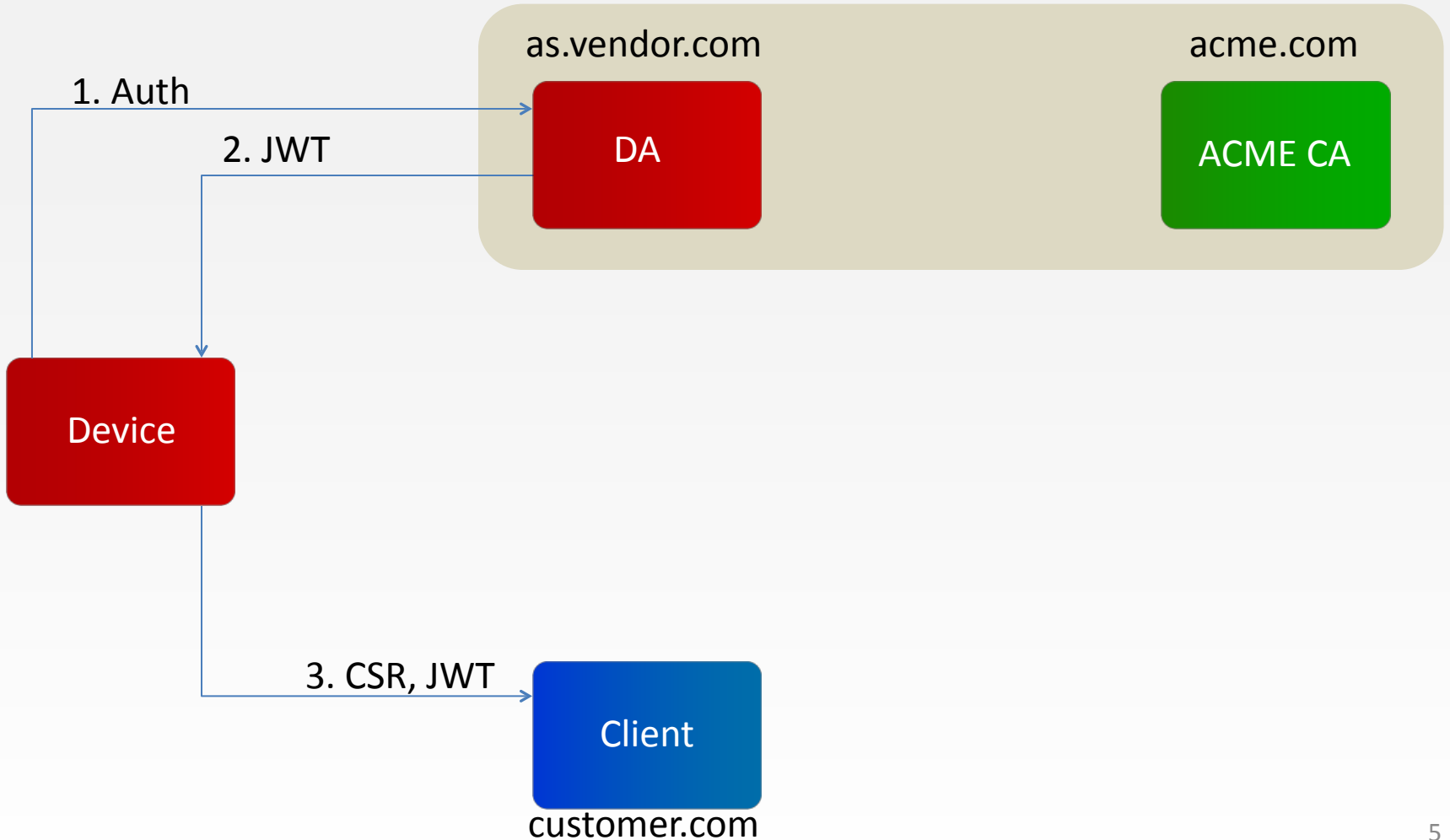
# FLOW OVERVIEW



# FLOW OVERVIEW

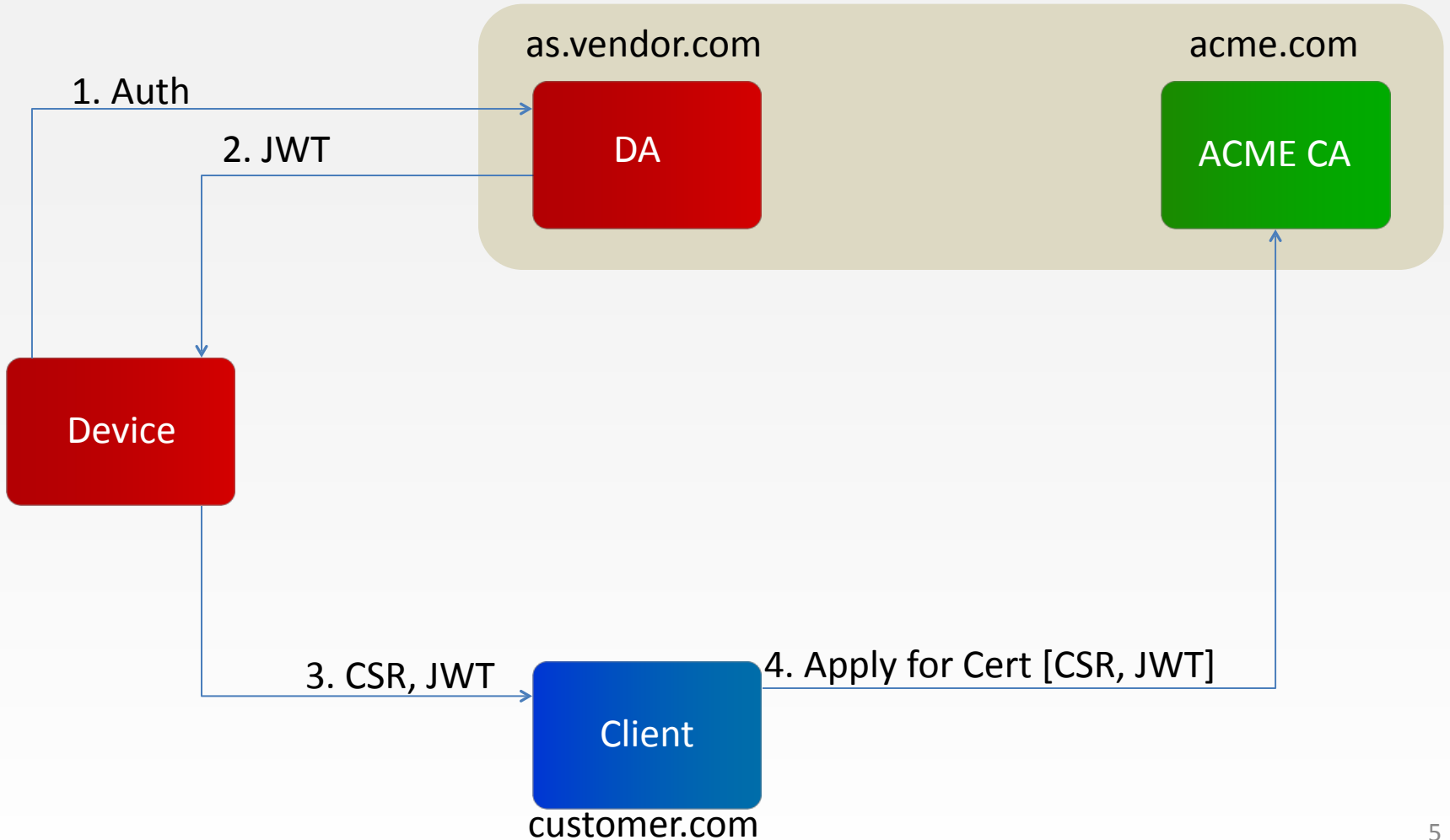


# FLOW OVERVIEW

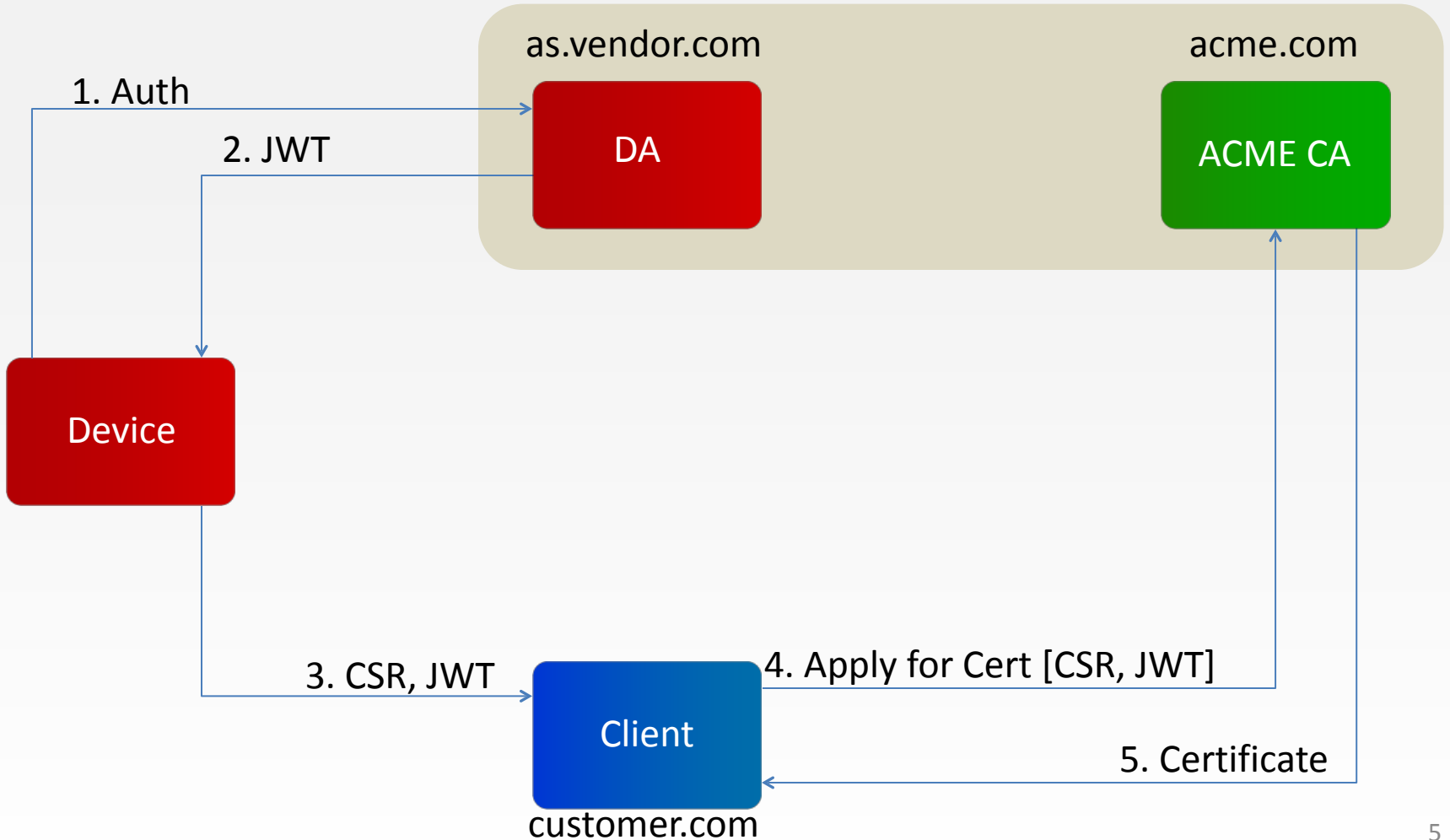




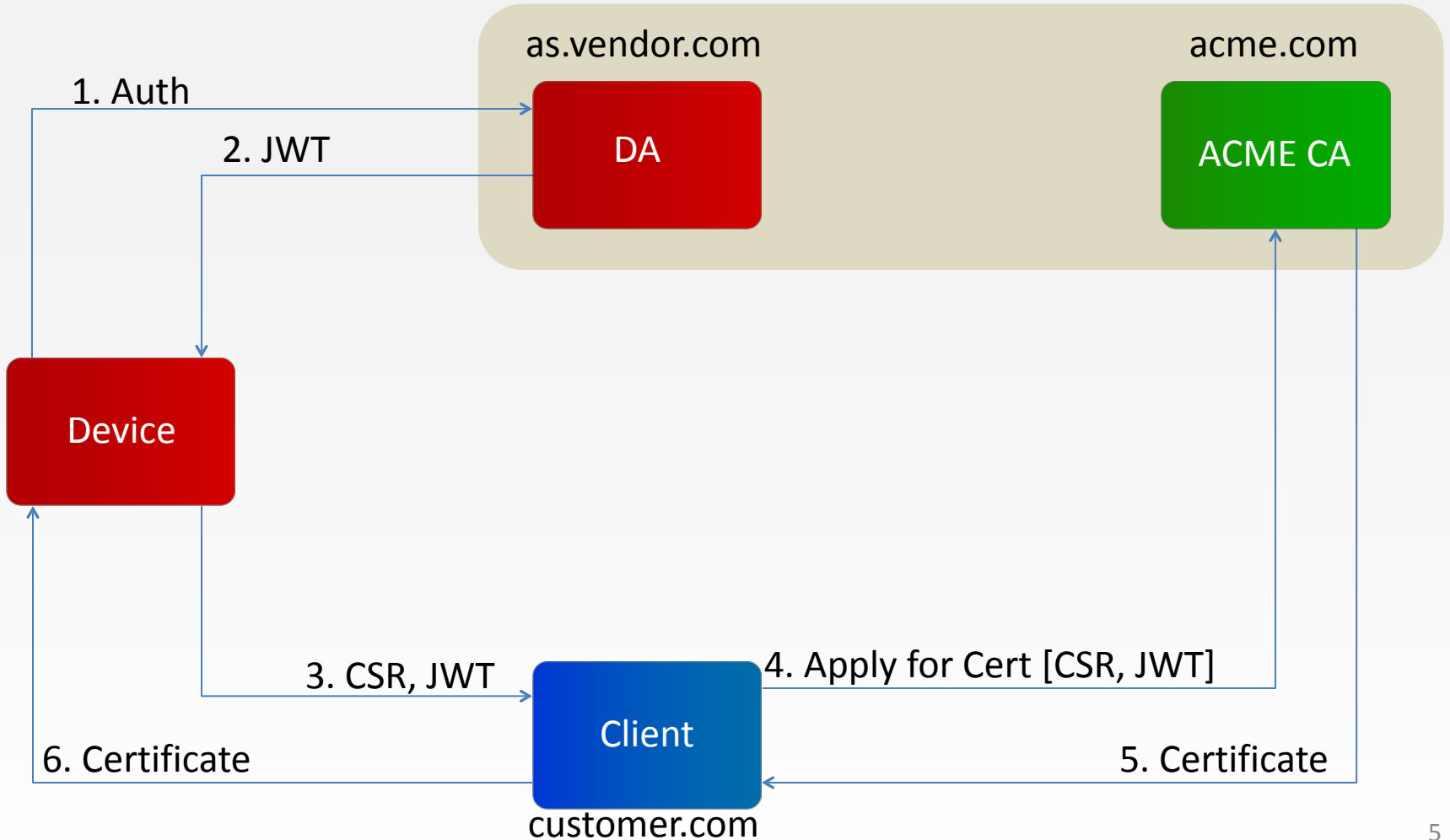
# FLOW OVERVIEW



# FLOW OVERVIEW



# FLOW OVERVIEW



# CLIENT-CA INTERACTION

customer.com

Client

acme.com

ACME CA

# CLIENT-CA INTERACTION

customer.com

Client

acme.com

ACME CA

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

```
sequenceDiagram
    participant Client as Client
    participant ACME_CA as ACME CA
    Client->>ACME_CA: [01] POST /new-order
    Note over Client, ACME_CA: kid=customer.com/acme/acct/<acct>
    Note over Client, ACME_CA: url=vendor.com/acme/new-order
    Note over Client, ACME_CA: identifier=<mac>
```

# CLIENT-CA INTERACTION

customer.com

acme.com

Client

ACME CA

[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

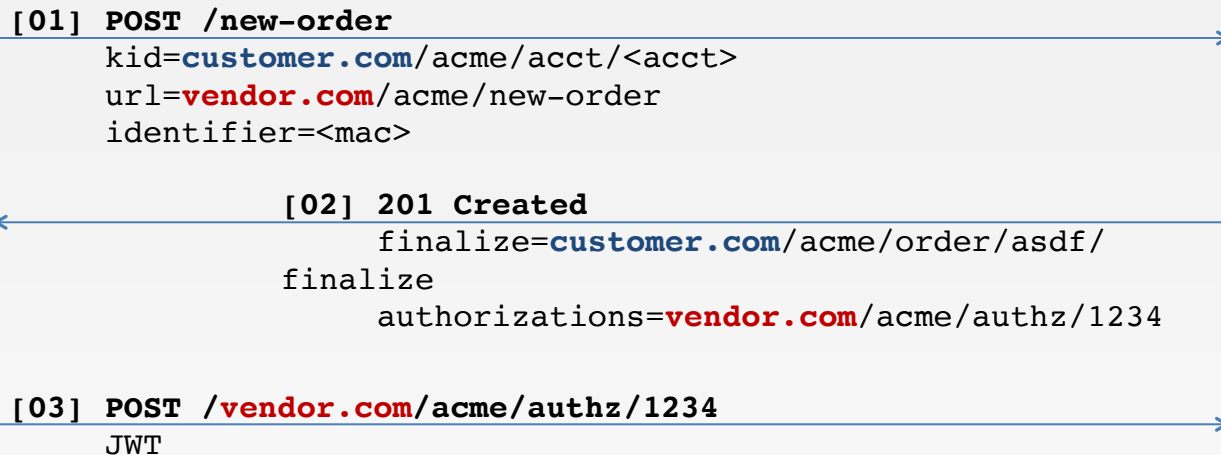
# CLIENT-CA INTERACTION

customer.com

acme.com

Client

ACME CA



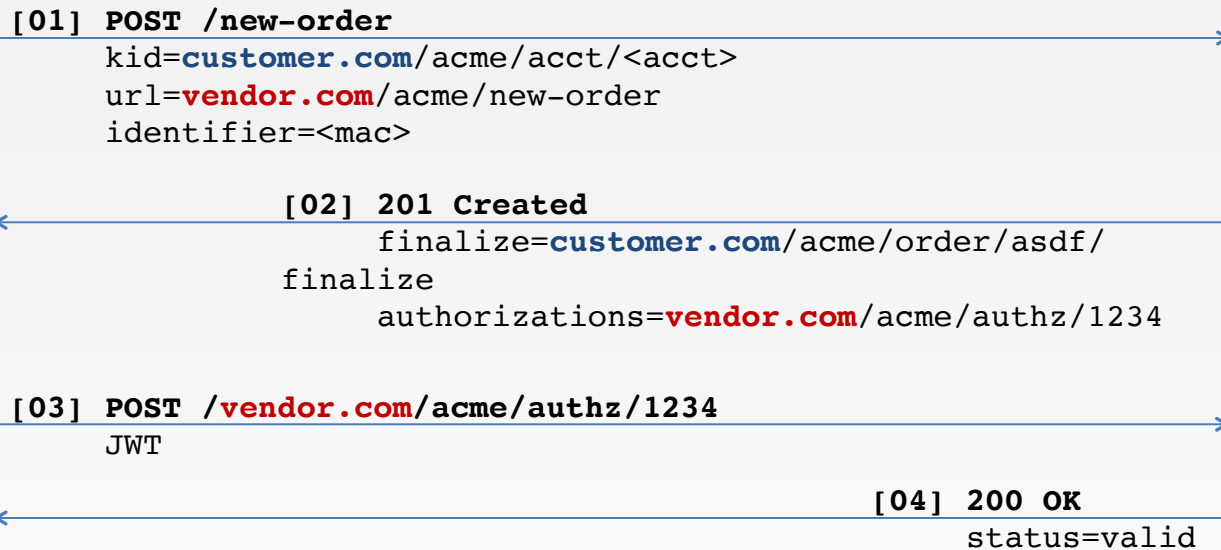
# CLIENT-CA INTERACTION

customer.com

acme.com

Client

ACME CA





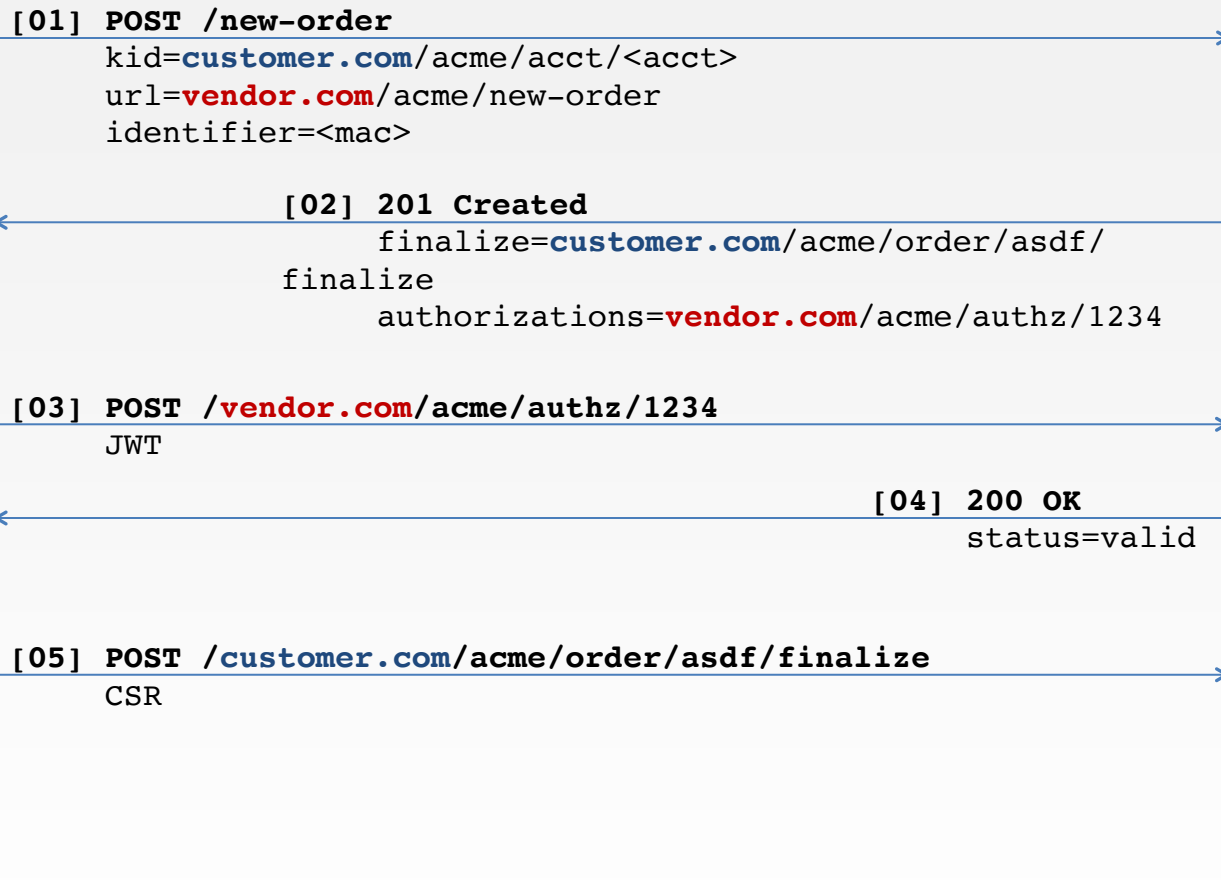
# CLIENT-CA INTERACTION

customer.com

acme.com

Client

ACME CA



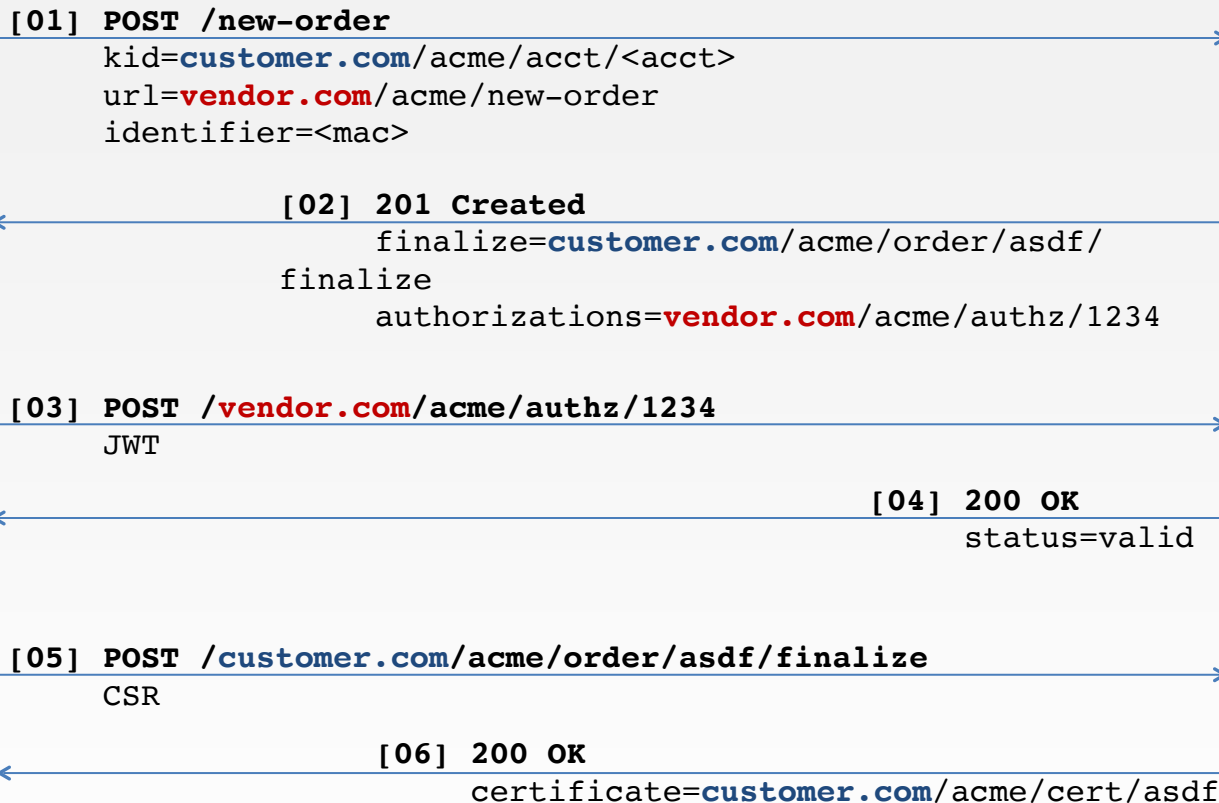
# CLIENT-CA INTERACTION

customer.com

acme.com

Client

ACME CA



# 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?

