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

Device

as.vendor.com
DA

acme.com
ACME CA

Client
customer.com
SETUP

1. Create an account
2. Claim a device

1. Create an account
2. Prove control over customer.com
FLOW OVERVIEW

Device

as.vendor.com
DA

acme.com
ACME CA

customer.com
Client
FLOW OVERVIEW

1. Auth

Device

as.vendor.com

DA

acme.com

ACME CA

Client
customer.com
FLOW OVERVIEW

1. Auth

2. JWT

Device

as.vendor.com
DA
acme.com
ACME CA

Client

customer.com
FLOW OVERVIEW

1. Auth
2. JWT
3. CSR, JWT
FLOW OVERVIEW

1. Auth
2. JWT
3. CSR, JWT
4. Apply for Cert [CSR, JWT]
FLOW OVERVIEW

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

Device
as.vendor.com
DA
ACME CA
acme.com
Client
customer.com
FLOW OVERVIEW

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

customer.com

Client

acme.com

ACME CA
CLIENT-CA INTERACTION

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

[02] 201 Created
final=customer.com/acme/order/asdf/
finalize
authorization=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
## CLIENT-CA INTERACTION

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[01]</strong> POST /new-order</td>
<td></td>
</tr>
<tr>
<td></td>
<td>kid=customer.com/acme/acct/&lt;acct&gt;</td>
</tr>
<tr>
<td></td>
<td>url=vendor.com/acme/new-order</td>
</tr>
<tr>
<td></td>
<td>identifier=&lt;mac&gt;</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[02]</strong> 201 Created</td>
<td></td>
</tr>
<tr>
<td></td>
<td>finalize=customer.com/acme/order/asdf/</td>
</tr>
<tr>
<td></td>
<td>finalize</td>
</tr>
<tr>
<td></td>
<td>authorizations=vendor.com/acme/authz/1234</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[03]</strong> POST /vendor.com/acme/authz/1234</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JWT</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[04]</strong> 200 OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>status=valid</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[05]</strong> POST /customer.com/acme/order/asdf/finalize</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSR</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[06]</strong> 200 OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>certificate=customer.com/acme/cert/asdf</td>
</tr>
</tbody>
</table>
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?