Delegated Voucher: problem statement

- RFC8366 vouchers require a MASA (manufacturer) to provide a voucher for each device.
  - the manufacture can block secondary sales
  - a failed manufacturer’s device may become landfill
- BRSKI (mostly) requires this to be an online service.
- SZTP (RFC8572) works better for offline uses, but still has difficulties
Applicability

- second sale from willing seller
- second sale via creditor/bankruptcy, etc.
- manufacturer of assembly of composite devices, e.g.
  - a passenger rail car
  - transparent factory/plant machine with many sensors/actuators
- disconnected owner (military base example)
- owner that uses cloud/public PKI for registrar
  - each time the CA changes, it’s a “resale”
Shape of proposed solution

```json
{
    "ietf-voucher:voucher": {
        "created-on": "2016-10-07T19:31:42Z",
        "assertion": "logged",
        "serial-number": "JADA123456789",
        "idevid-issuer": "base64encodedvalue==",
        "pinned-domain-cert": "base64encodedvalue==",
        "nonce": "base64encodedvalue=="
    }
}

{
    "ietf-voucher:voucher": {
        "created-on": "2020-03-14T06:28:31Z",
        "expire-on": "2039-12-31T01:61:80Z",
        "assertion": "logged",
        "serial-number": ["JADA123456789", "SKU338327950", "NPU2884197169"],
        "pinned-intermediate-cert": ["reseller1base64cert=="],
        "delegate-limit": 3,
    }
}
```
Proposed structure

MASA

Delegated Voucher (DV1)

OWNER 1

EPHERMERAL VOUCHER+ DV1

OWNER 2
Proposed structure

MASA

Delegated Voucher (DV1)

OWNER 1 (DV2)

Delegated Voucher

OWNER 1

OWNER 2

EPHERMERAL VOUCHER + DV1 + DV2

OWNER 3
Proposed structure: reseller

MASA

Long-period Voucher Set (VS)

INTERMEDIARY

OWNER 1

EPHERMERAL VOUCHER + VS

OWNER 2

EPHERMERAL VOUCHER + VS