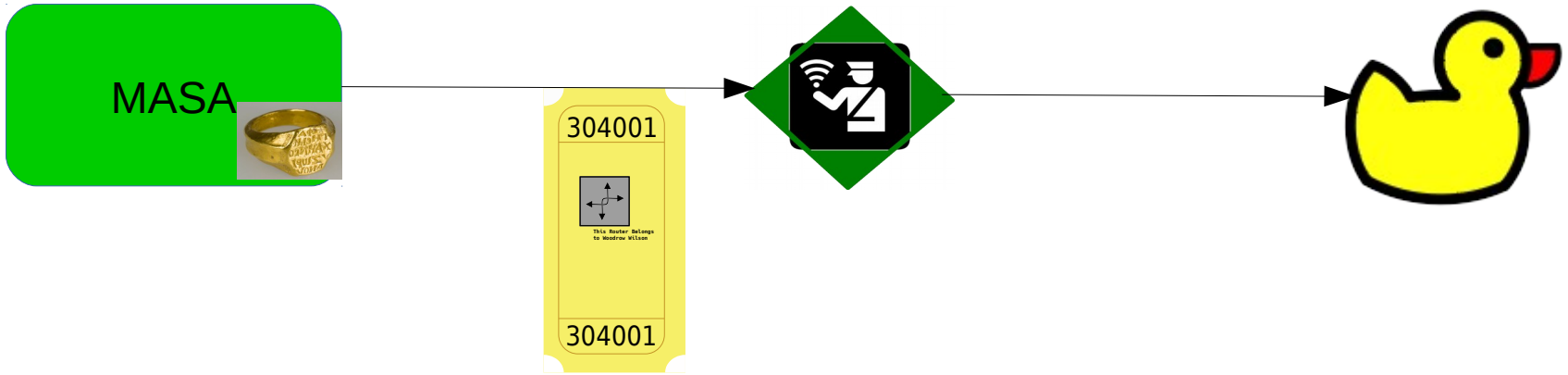
Delegated Authority for Bootstrap Voucher Artifacts

draft-richardson-anima-voucher-delegation

M. Richardson
Liang Xia
Jie Yang(presenting)

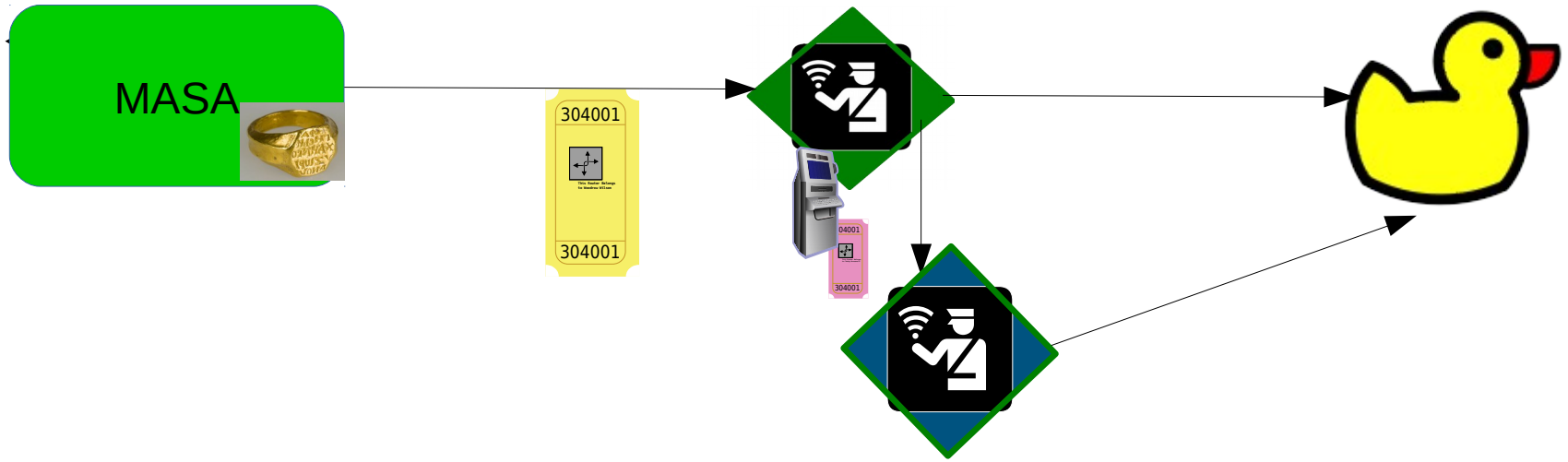
IETF 107, ANIMA
April 9, 2020

The problem with Manufacturer Issued (RFC8366) Vouchers



- 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.
  - MASA must be reachable to the Registrar during on-boarding
  - Device owner is always strongly dependent on the MASA service
- SZTP (RFC8572) works better for some offline uses, but has same resale issue

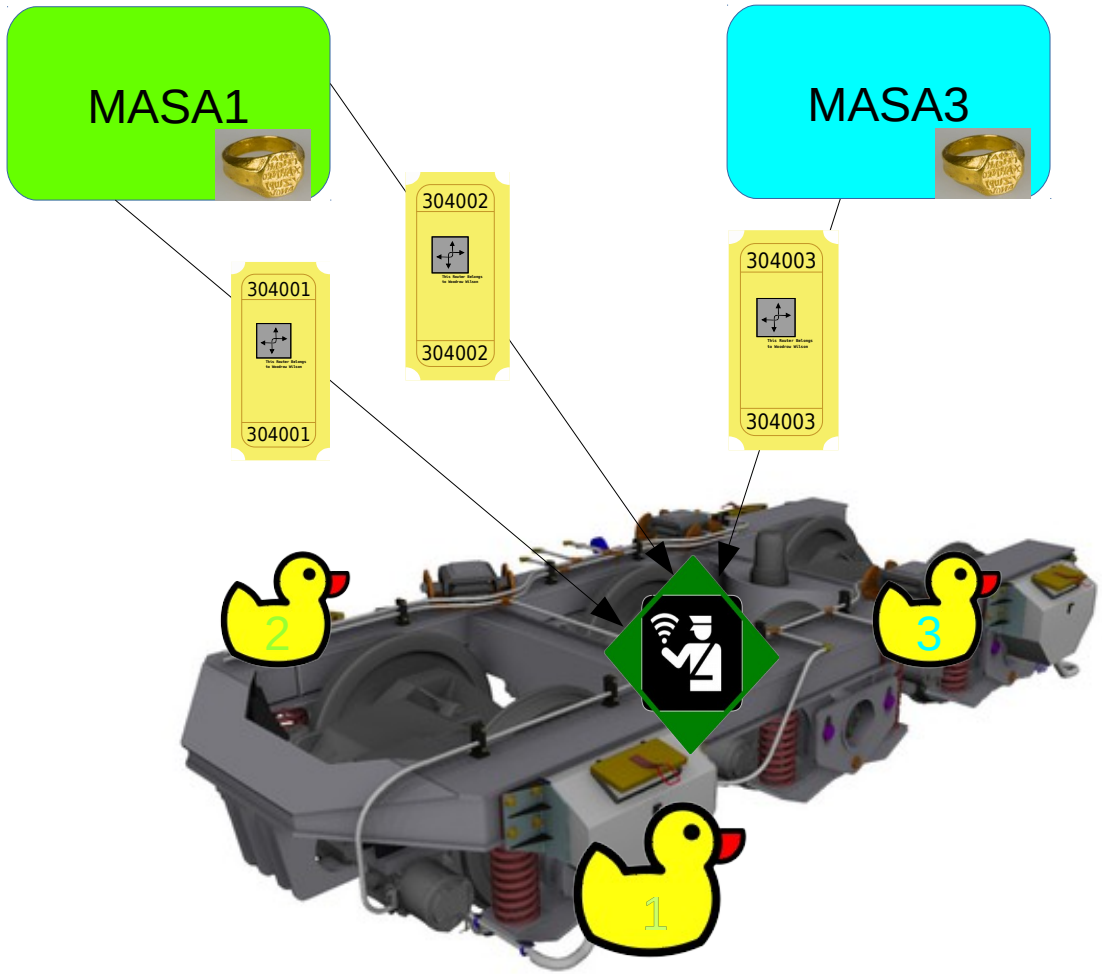
Applicability of Delegated Voucher



- Second sale
  - From willing seller
  - Via creditor/bankruptcy, etc.
- With a cloud/public PKI, if the Registrar wishes to change it's CA, then it is effectively a "resale"

- Blue Registrar must override MASA URL, contacting Green Registrar for voucher

Applicability of Delegated Voucher: Assembly

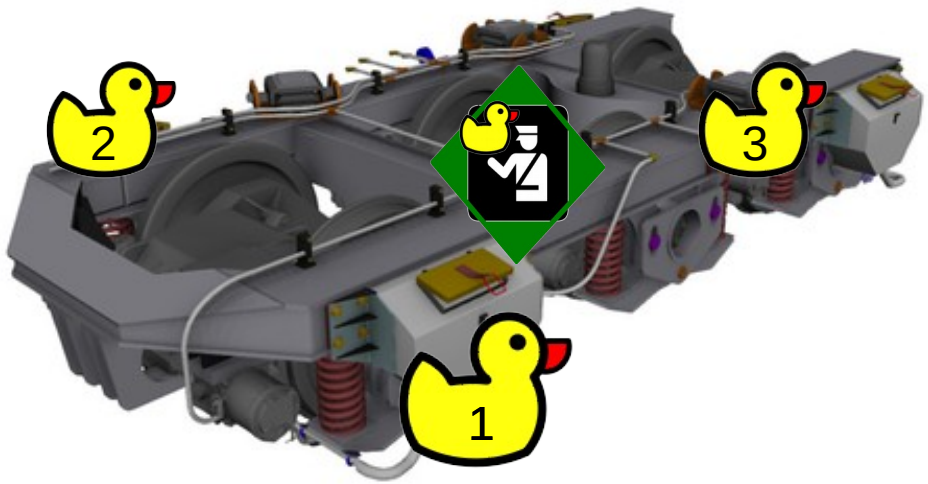


- First sale is from component manufacturer
  - owner is assembly controller
  - voucher includes delegation options

Applicability of Delegated Voucher: Transparent Assembly

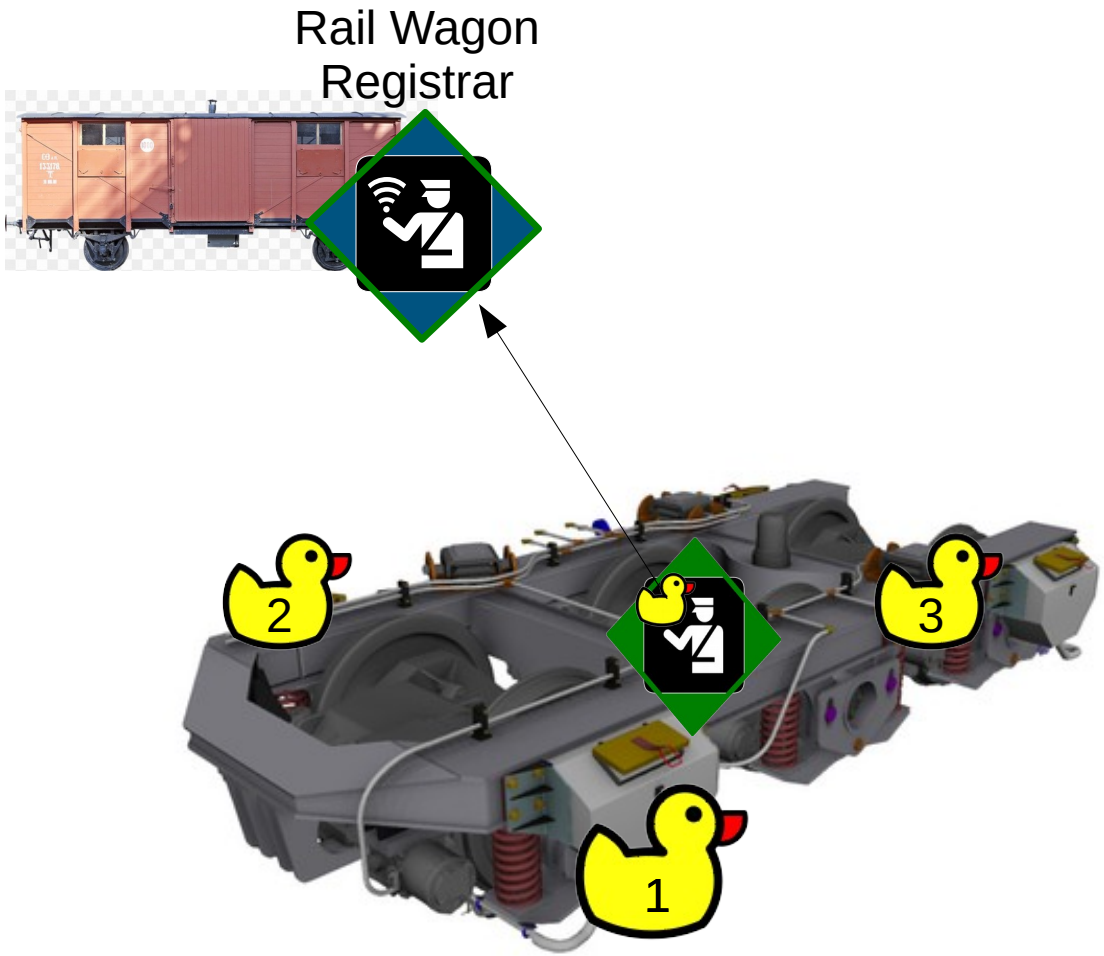
Rail Wagon Registrar

rail wagon assembly MASA4



- Assembly onboards as normal

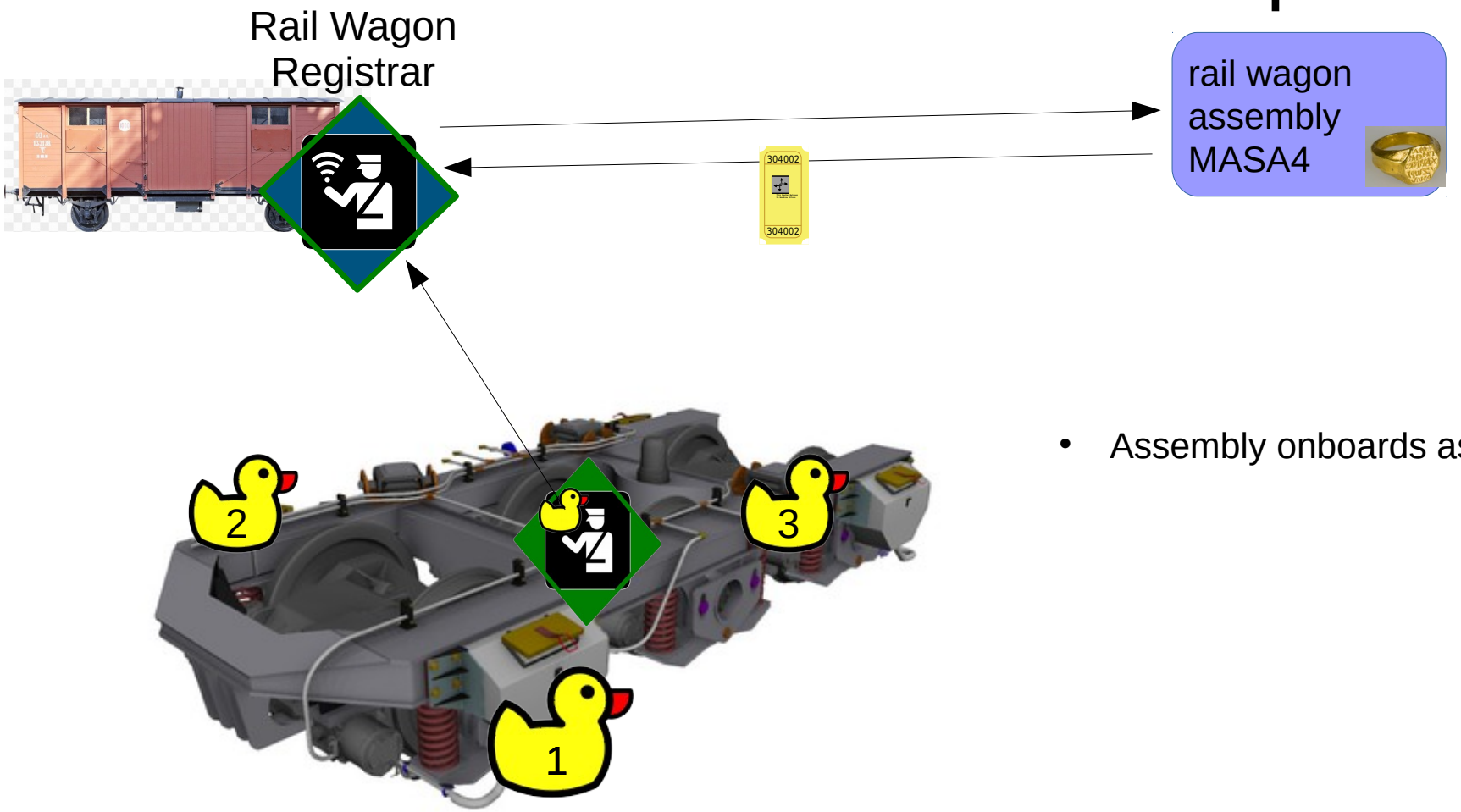
Applicability of Delegated Voucher: Transparent Assembly



rail wagon assembly MASA4

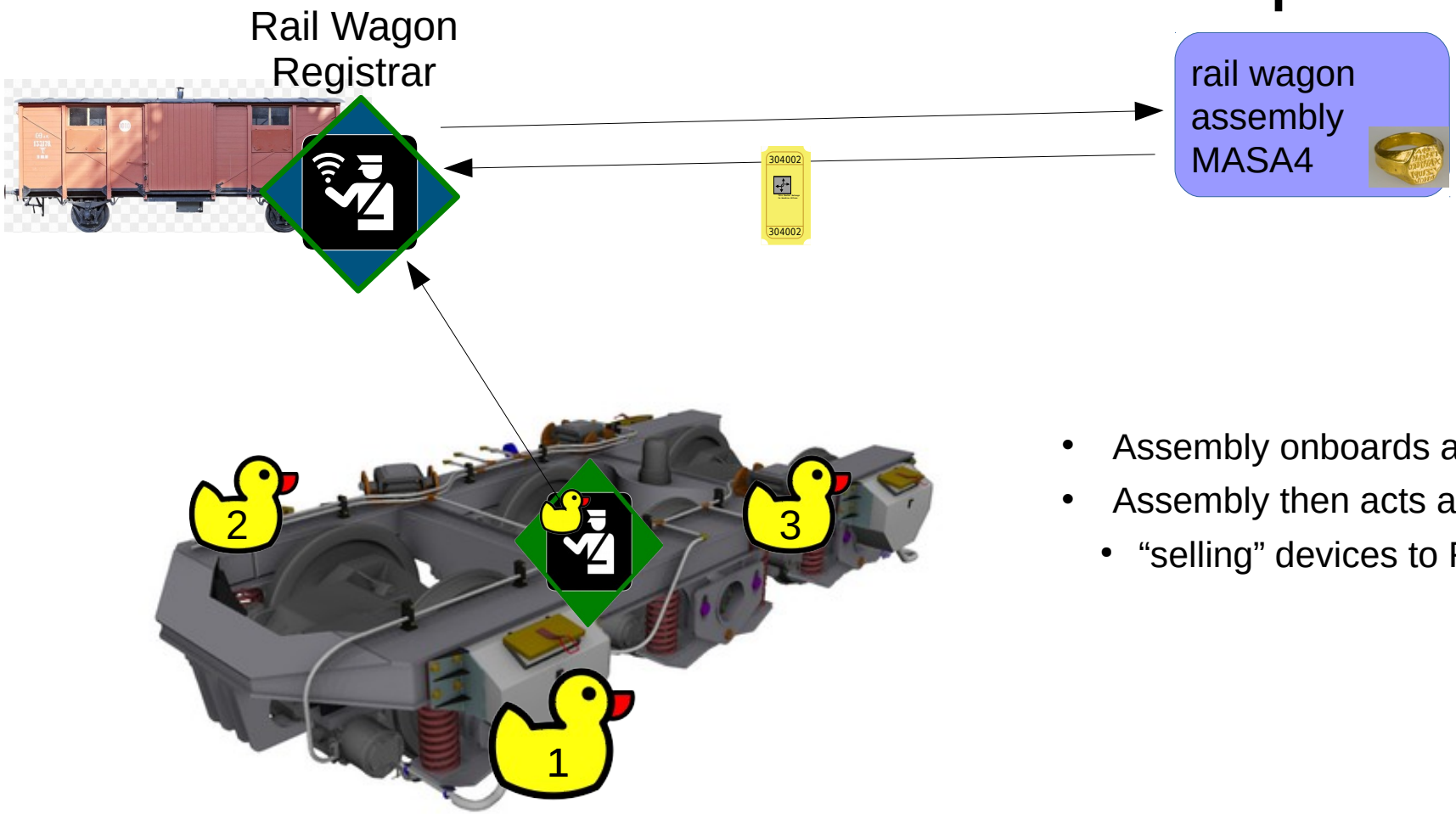
- Assembly onboards as normal

Applicability of Delegated Voucher: Transparent Assembly



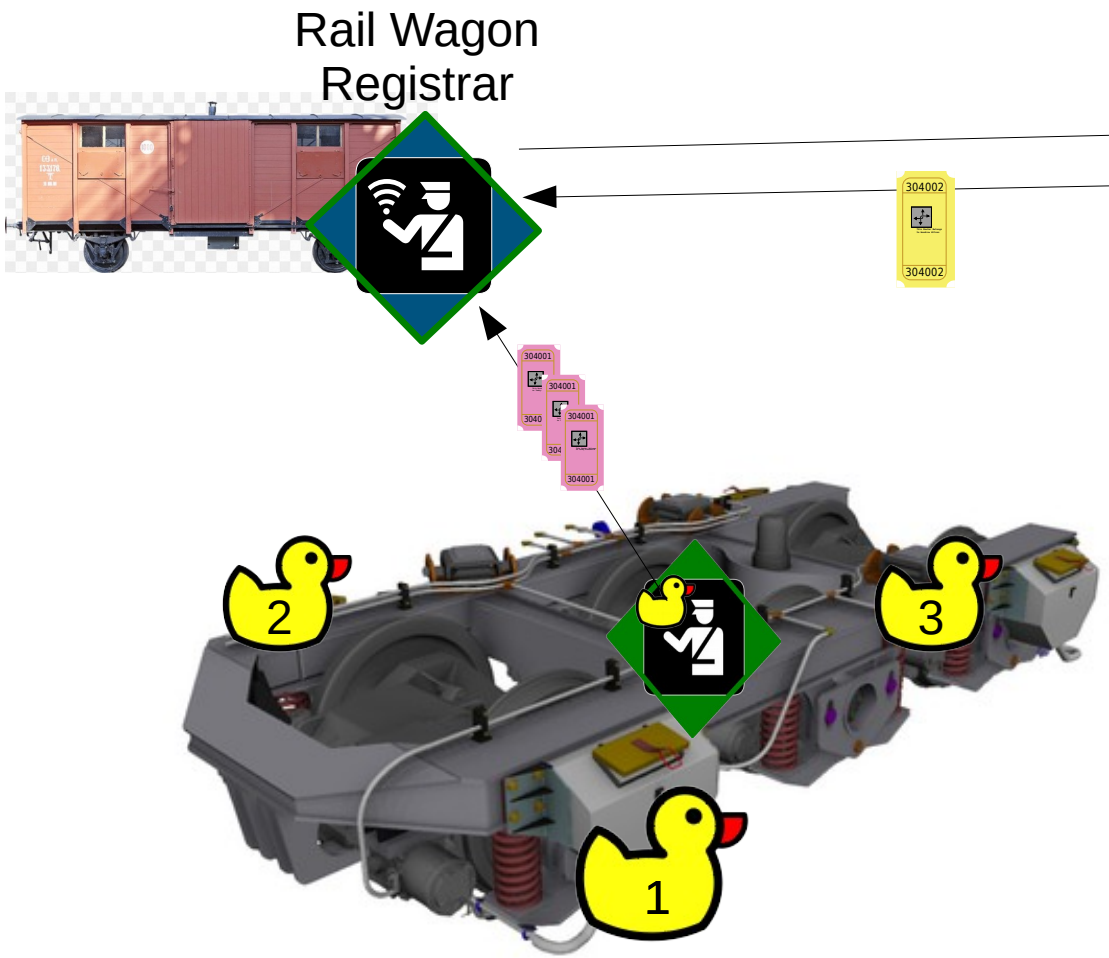
- Assembly onboards as normal

Applicability of Delegated Voucher: Transparent Assembly



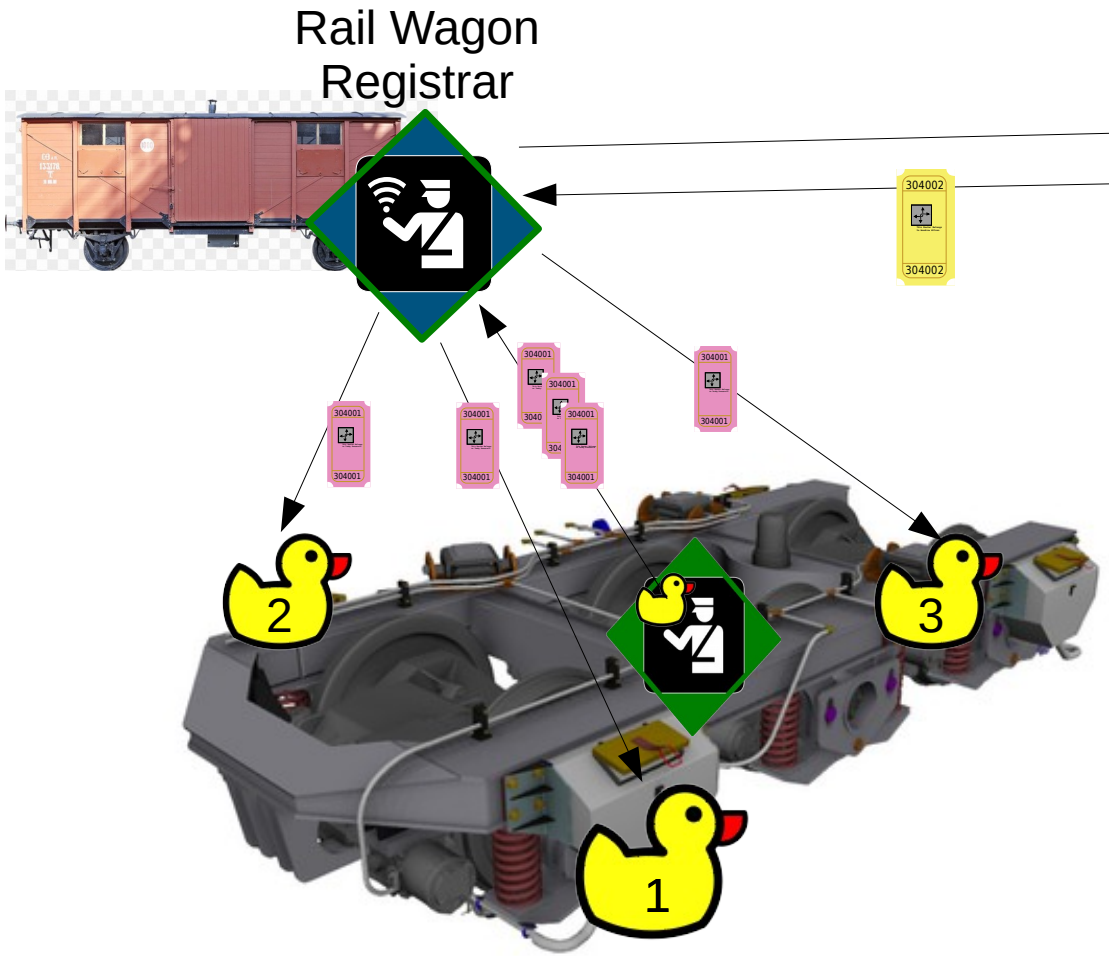
- Assembly onboards as normal
- Assembly then acts as Registrar,
  - “selling” devices to Rail Wagon Registrar

Applicability of Delegated Voucher: Transparent Assembly



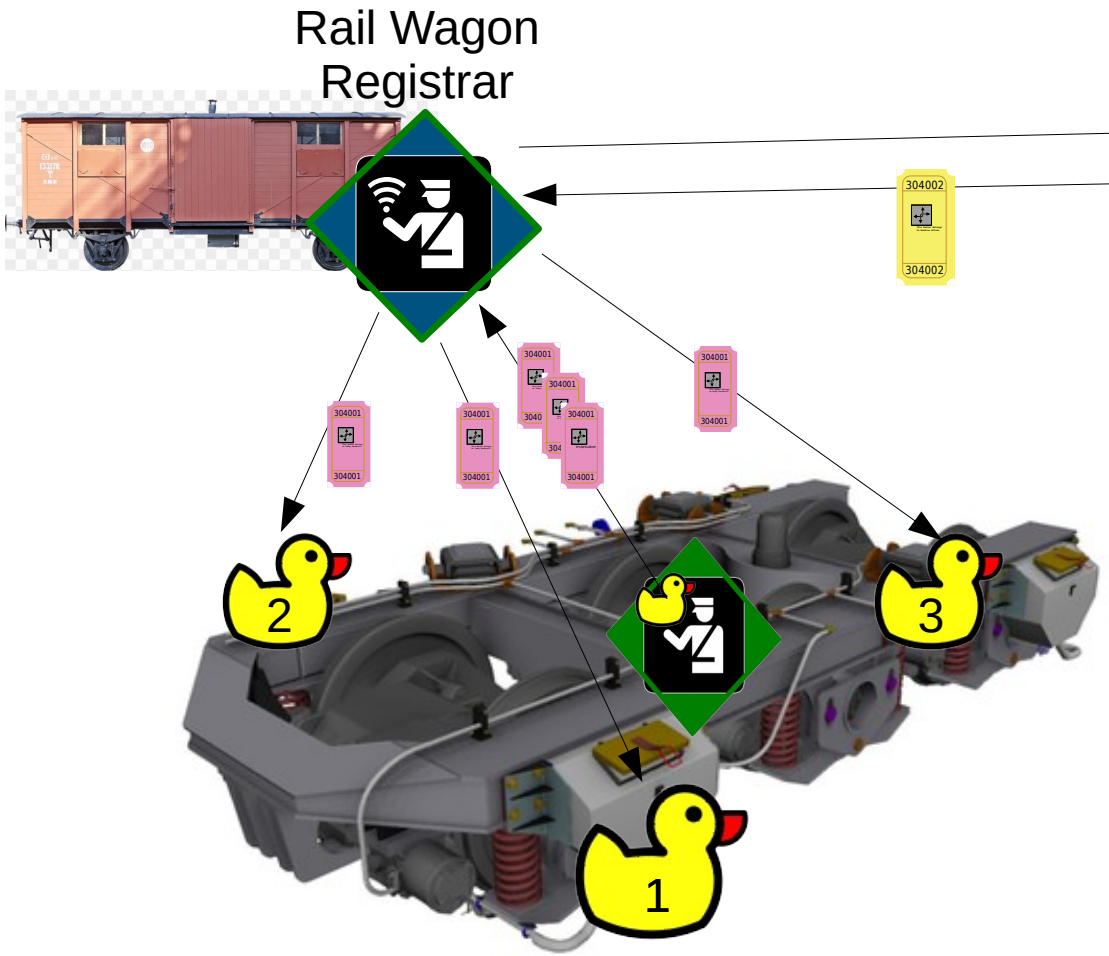
- Assembly onboards as normal
- Assembly then acts as Registrar,
  - “selling” devices to Rail Wagon Registrar

Applicability of Delegated Voucher: Transparent Assembly



- Assembly onboards as normal
- Assembly then acts as Registrar,
  - “selling” devices to Rail Wagon Registrar

Applicability of Delegated Voucher: Transparent Assembly



- Assembly onboards as normal
- Assembly then acts as Registrar,
  - “selling” devices to Rail Wagon Registrar
- Repeat to form Train!

Shape of proposed solution

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

```
{
  "ietf-delegated-voucher:voucher": {
    "created-on": "2020-03-14T06:28:31Z",
    “expire-on”: “2039-12-31T01:61:80Z”,
    "assertion": "logged",
     "serial-number": "JADA123456789",
    "pinned-delegation-certificate-authority": [“DASAbase64cert==“],
    "delegation-voucher":[DelegationVoucher1", " DelegationVoucher2", " DelegationVoucher3"],
    "intermediate-identities": ["IntermediateId1", "IntermediateId2", "IntermediateId3"],
    "delegation-countdown": 3,
  }
}
```

Issues to think about ...

- delegated voucher extension
  - I. pinned-certificate-authority:
    - Could this be omitted to use some DNS TLSA certification?
  - II. pinned-certificate-name:
    - Is it enough to pin an rfc822NAME, or do we need to be able to pin other D
  - III. delegation-voucher:
    - This is a flag, like CA= True. Do we need it?
  - IV. intermediate-identities:
    - This is voucher identity being consistent with delegation voucher. Do we need it?
  - V. delegation-countdown:
    - Do we need a way to limit how many times a delegation voucher can be created?

```
module: ietf-delegated-voucher

  grouping voucher-delegated-grouping
    +-- voucher
       +-- created-on                          yang:date-and-time
       +-- expires-on?                         yang:date-and-time
       +-- assertion                           enumeration
       +-- serial-number                       string
       +-- idevid-issuer?                      binary
       +-- pinned-domain-cert?                 binary
       +-- domain-cert-revocation-checks?      boolean
       +-- nonce?                              binary
       +-- last-renewal-date?                  yang:date-and-time
       +-- pinned-certificate-authority?       binary
       +-- pinned-certificate-name?            binary
       +-- delegation-voucher?                 binary
       +-- intermediate-identities?            binary
       +-- delegation-countdown?               int16
```

- Do we do any of this for JSON format vouchers, or do it only for COSE signed CBOR vouchers?
  - I won't feel that this even close to complete until code is written
- Registrar may need enhancing...

Thank You!