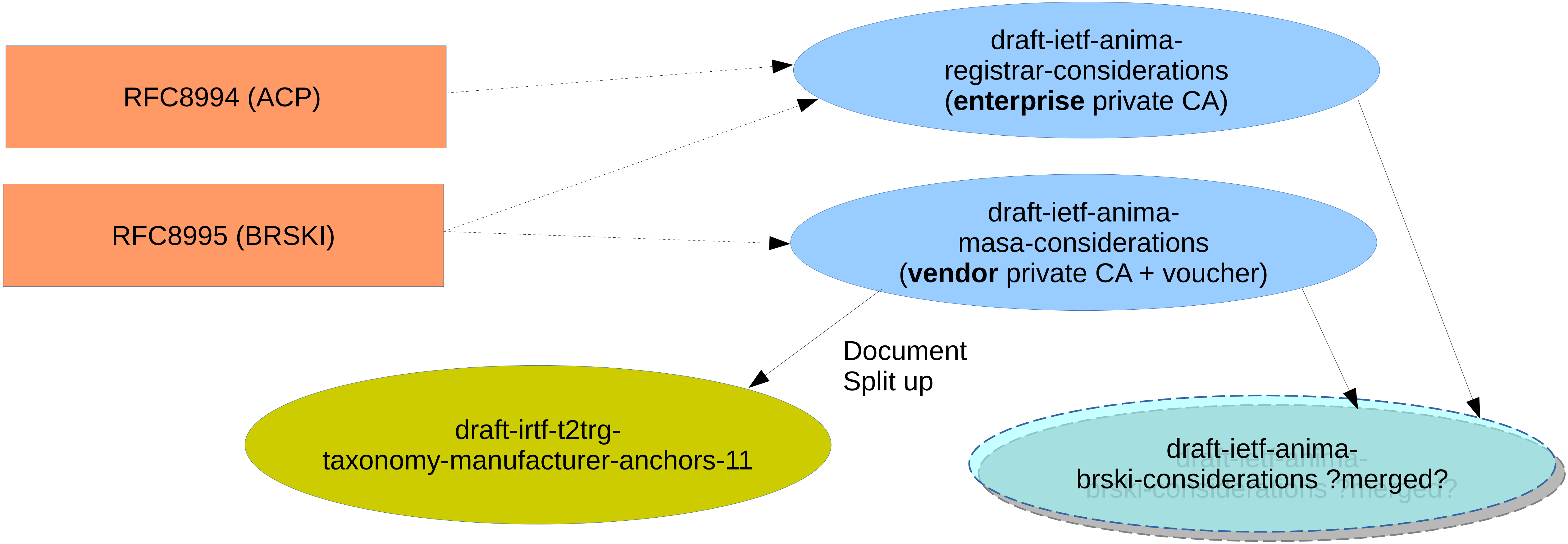
Operational Considerations for MASA, Registrar and IDevID

https://datatracker.ietf.org/doc/draft-richardson-anima-masa-considerations/
https://datatracker.ietf.org/doc/draft-richardson-anima-registrar-considerations/
https://datatracker.ietf.org/doc/draft-richardson-secdispatch-idevid-considerations

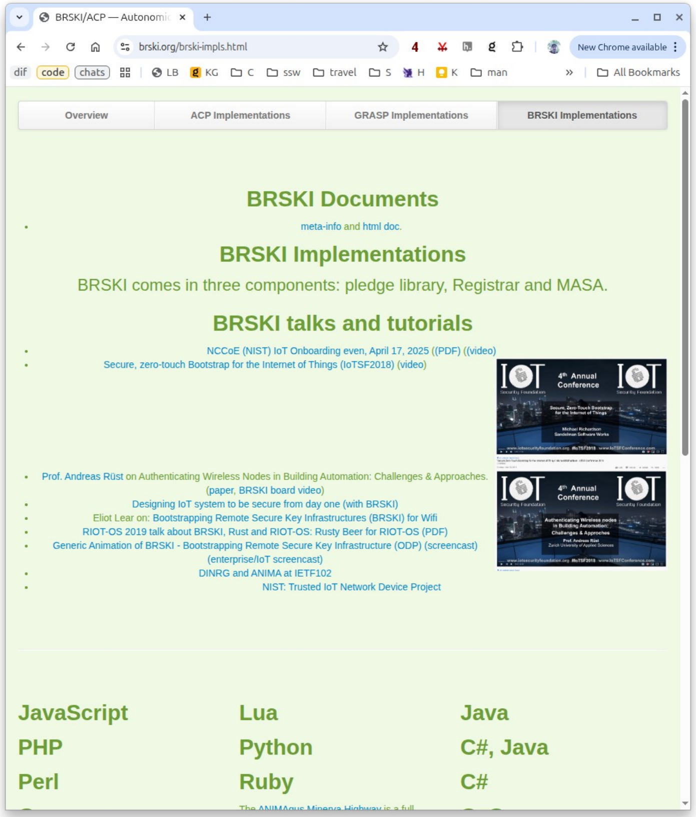
Michael Richardson
IETF 124: 2024-11-05

ANIMA Working Group

History of Documents



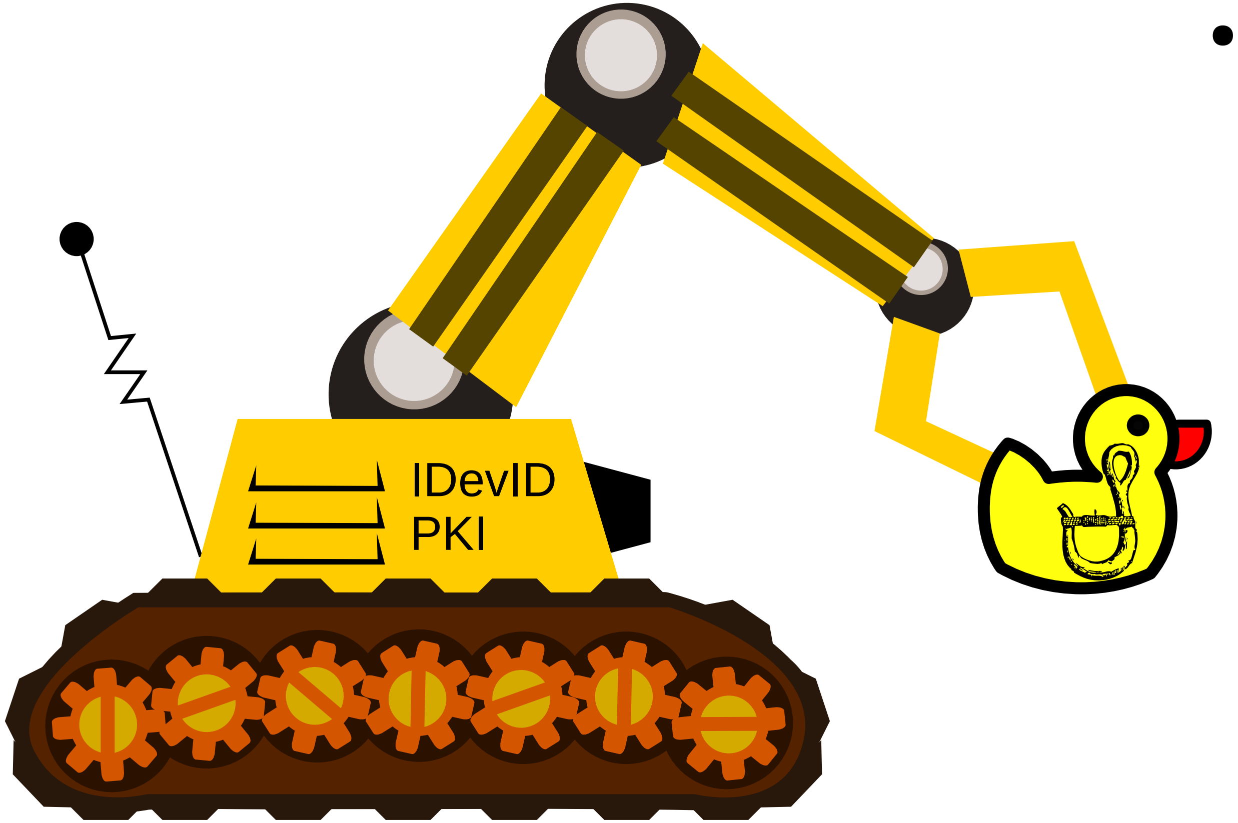
ANIMA ACP:
BRSKI.org / RFC8994.org / RFC8995.org



- any resemblance to cbor.io is intentional.
- static jekyll site,
  https://github.com/AnimaGUS-minerva/brski.org
  fork and contribute
- not hosted at github, because no IPv6 at the time

Operational Considerations for MASA

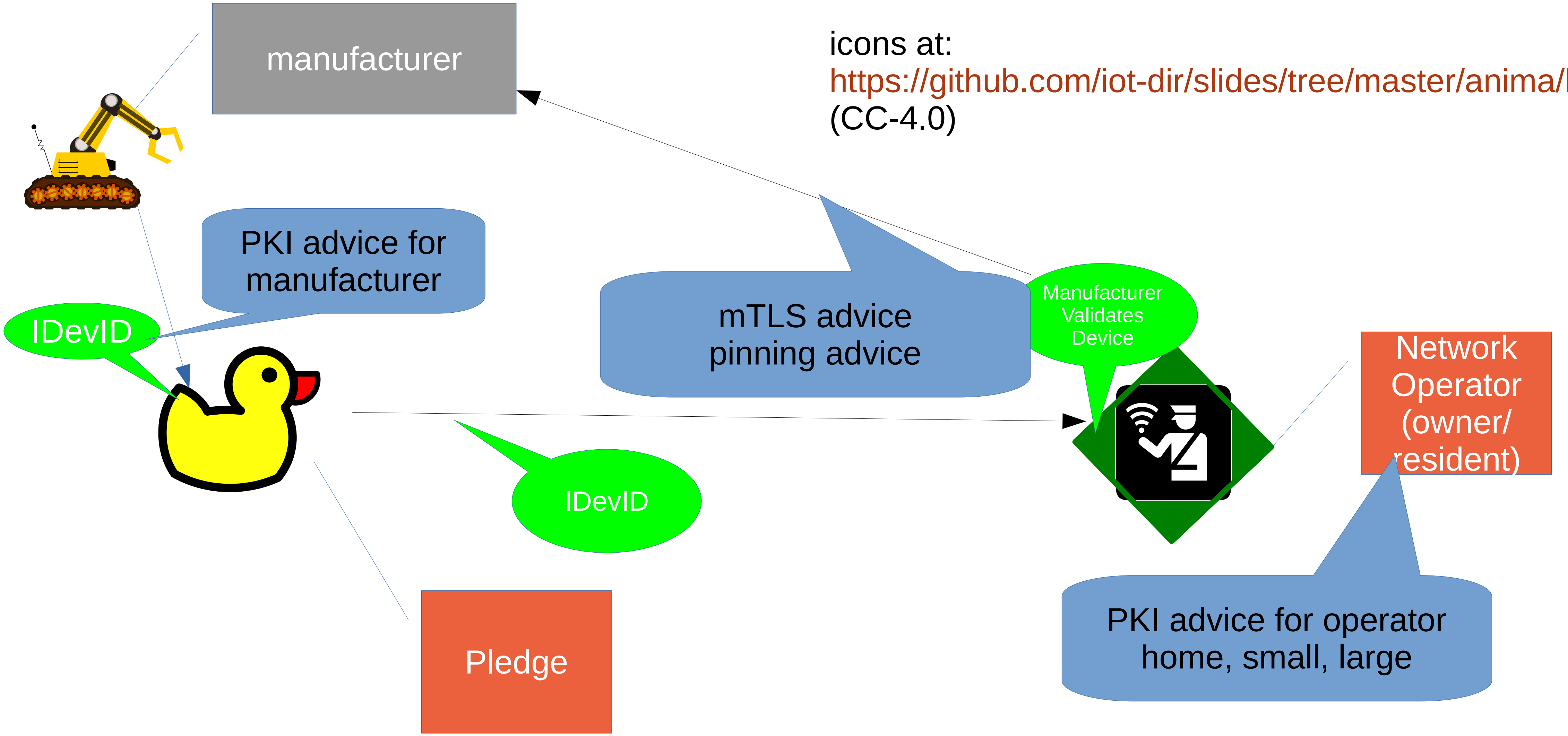
draft-ietf-anima-masa-considerations



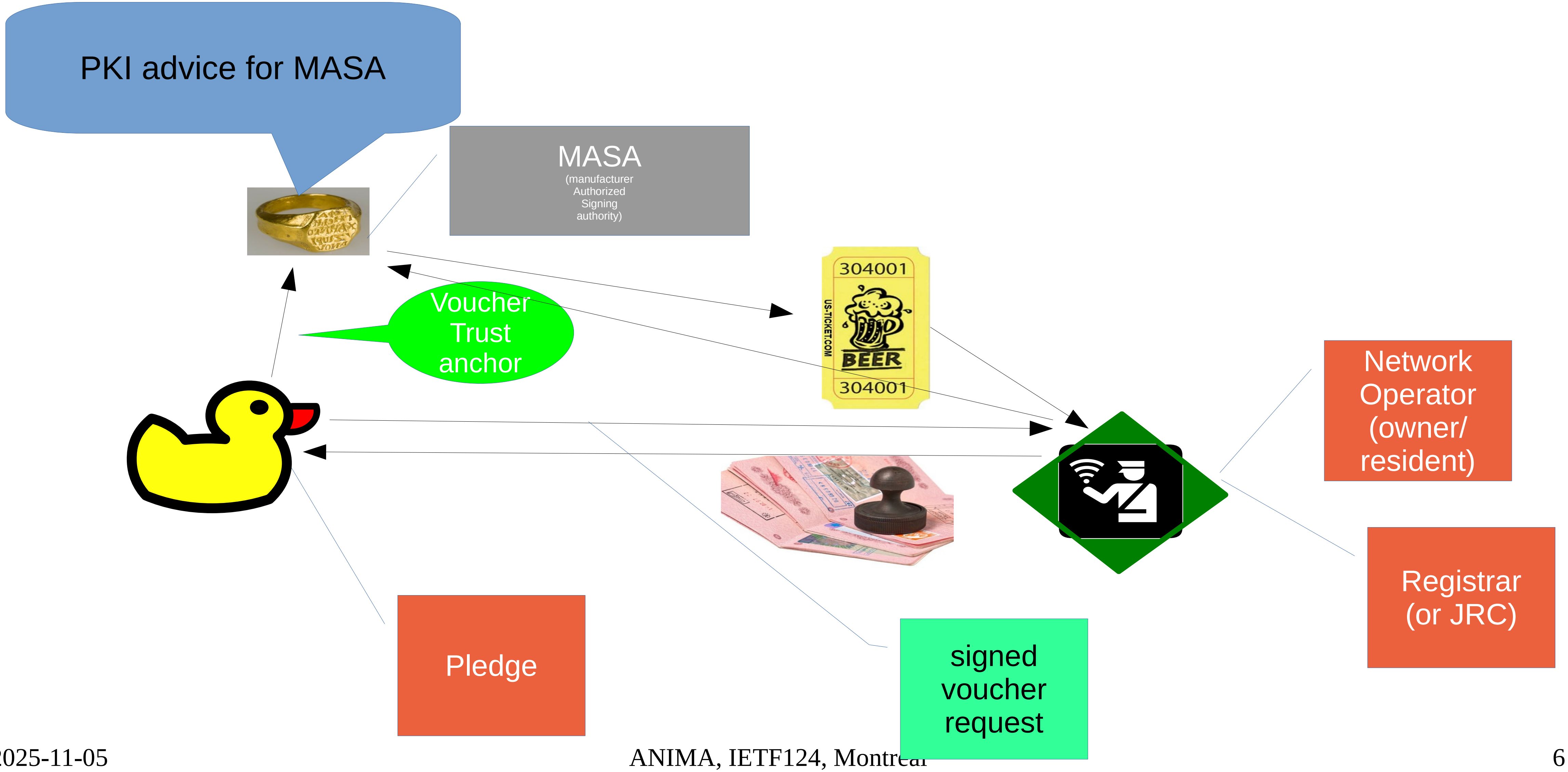
- manufacturer has to maintain a PKI.
  - this document provides prescriptive advice on how the private parts are kept, by the manufacturer, **in** the “factory”

BRSKI: where the Private PKIs go

icons at:
https://github.com/iot-dir/slides/tree/master/anima/brski
(CC-4.0)



BRSKI diagram: creating vouchers



Operational Considerations for Registrar

draft-ietf-anima-registrar-considerations

```
                  .-------------.
                  |    MASA     |
                  |   client    |
                  | BRSKI-MASA  |
                  '-------------'
                        ^
                        |
                        |
 .-------------.                      .----------------.
 | management  |    .-----------.     | certification  |
 | interface   |<---| database  |----->|   authority    |
 '-------------'    '-----------'     '----------------'
                        |
                        |
                        v
.-------------.     .-------------.      .-------------.
| Join Proxy  |     |  Pledge     |--.   | EST/BRSKI   |
|-------------|     | Interface   |  |   |-------------|
| GRASP       |     | BRSKI-EST   |e |   |    GRASP    |
| (DULL)      |     '-------------'T |   '-------------'
'-------------'        '-------------'
```

This document is about many design issues, including:

1) prescriptive statements about appropriate security for the private certification authority
2) scaling issues relating to TLS/HTTPS operations
3) synchronous vs asynchronous issues on how BRSKI-MASA client interacts with BRSKI-EST server
4) Incremental deployment of ACP into an existing NOC, including additional ACP-connect considerations

all
non-normative
advice

Merge Documents?

Discussion