

# **Operational Considerations for MASA, Registrar and IDevID**

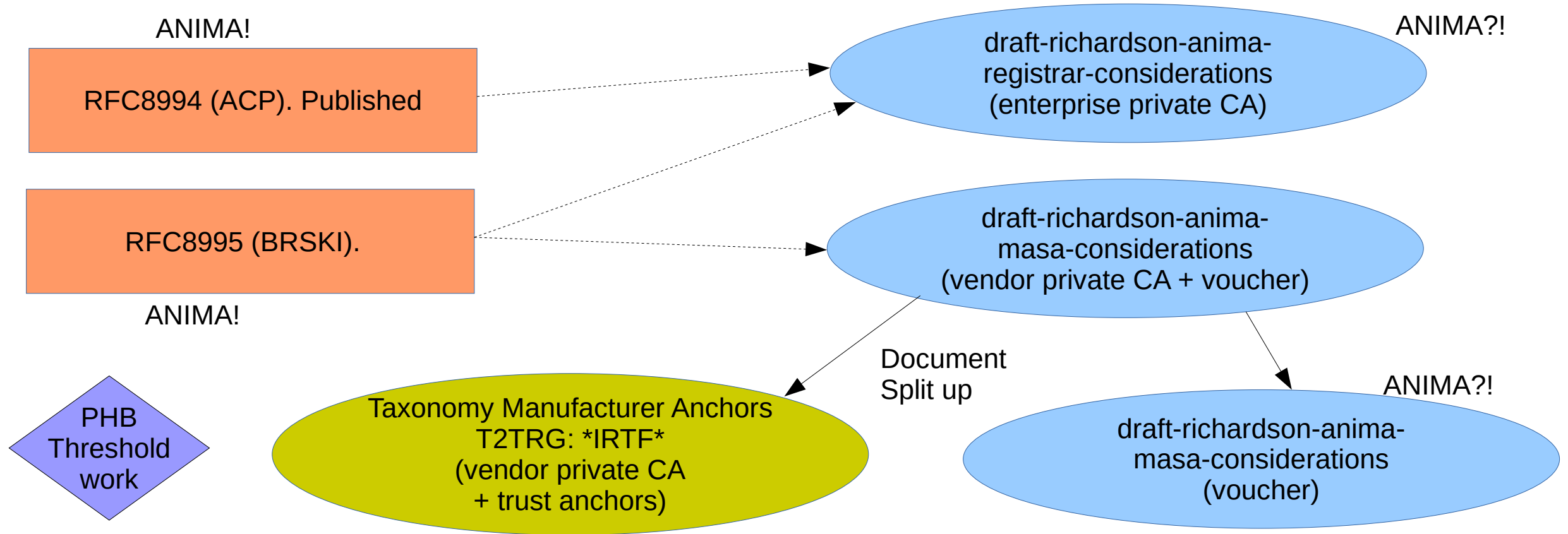
<https://datatracker.ietf.org/doc/draft-richardson-anima-masa-considerations/>  
<https://datatracker.ietf.org/doc/draft-richardson-anima-registrar-considerations/>  
<https://datatracker.ietf.org/doc/draft-irtf-t2trg-taxonomy-manufacturer-anchors/>

**Michael Richardson**, (Wei Pan)

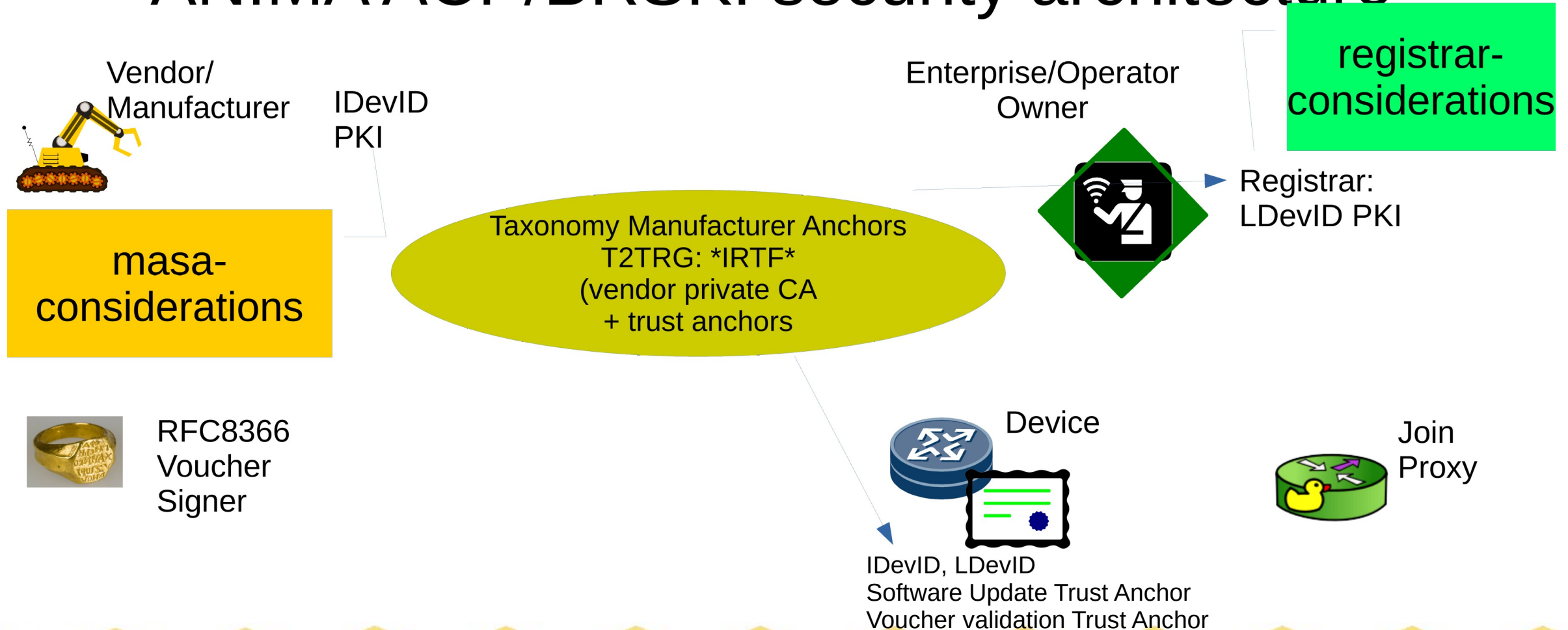
IETF 116: 2023-03-29

ANIMA Working Group

# History of Documents

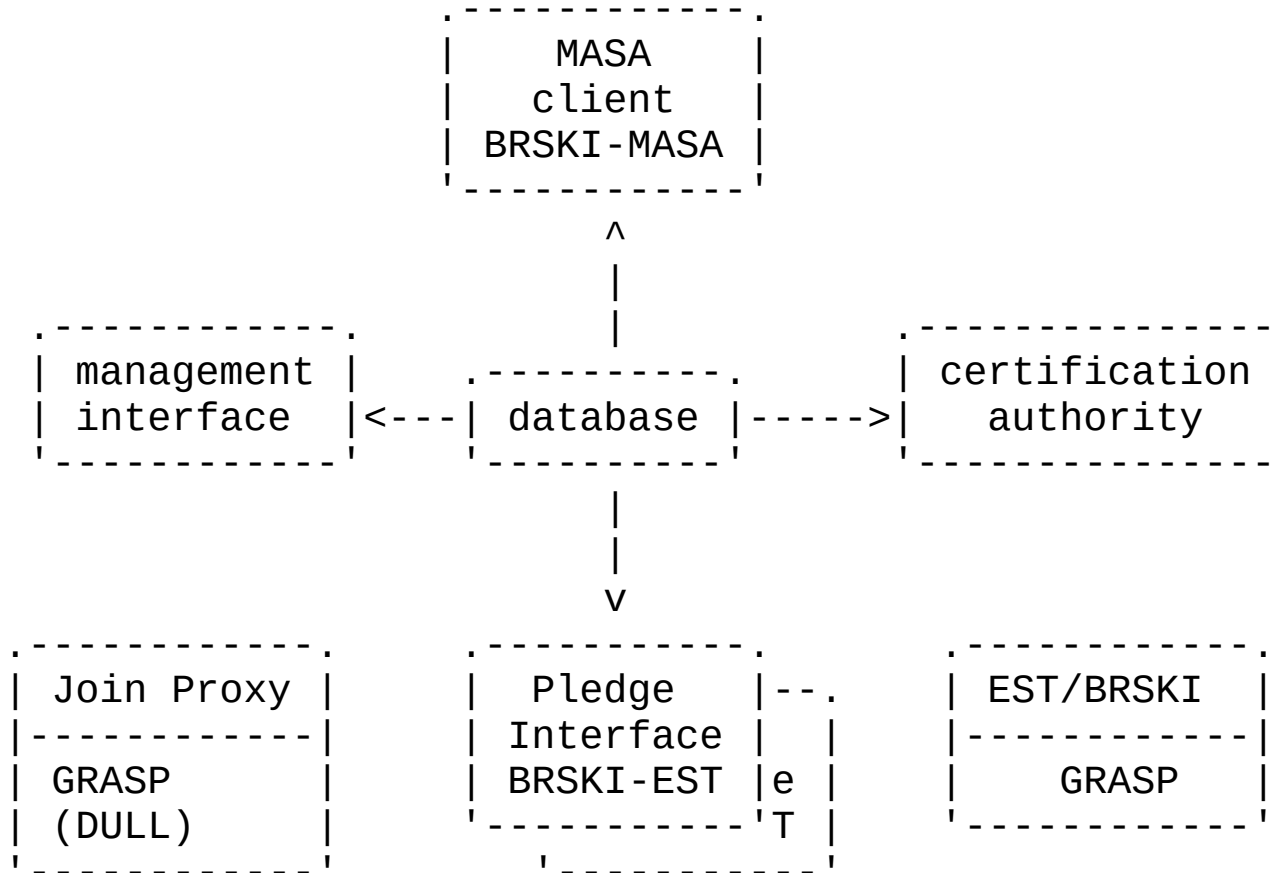


# ANIMA ACP/BRSKI security architecture



# Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations



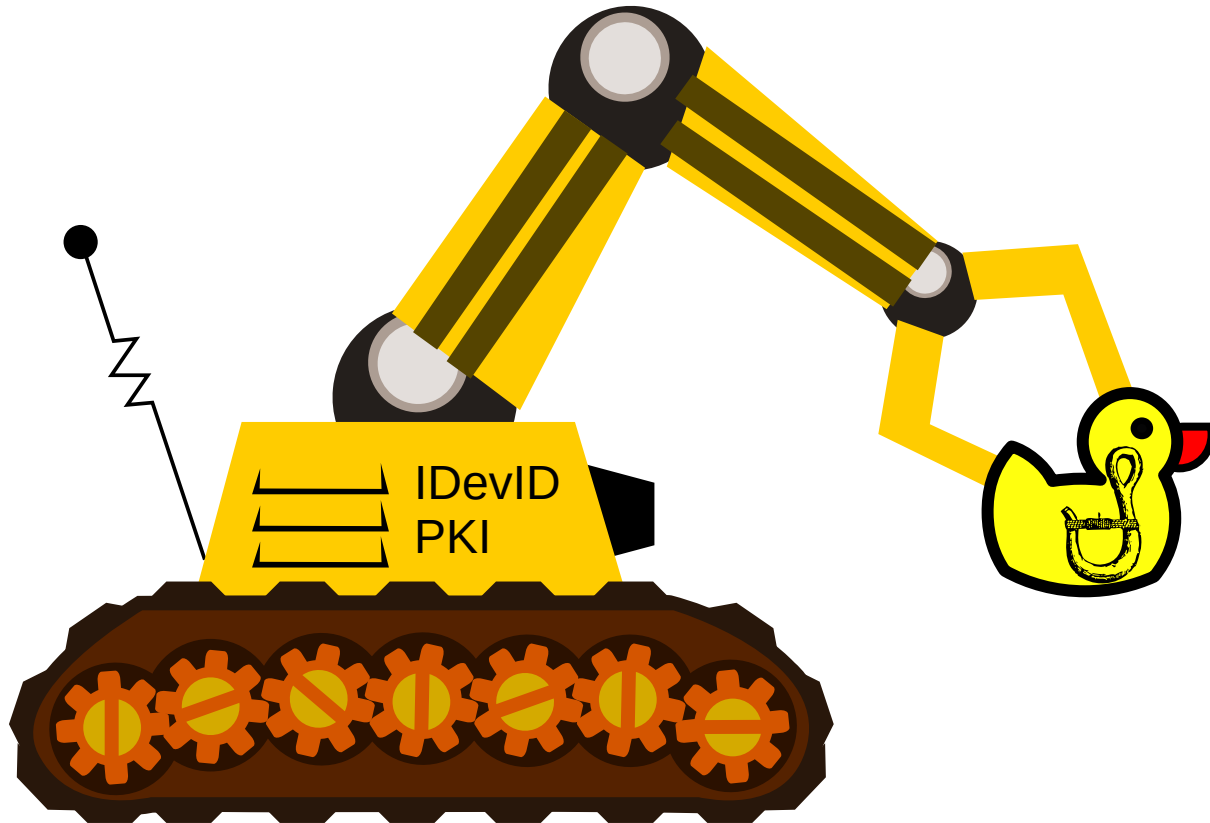
This document is about many design issues, including:

- 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

# Operational Considerations for MASA

draft-richardson-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”
  - Now references taxonomy-manufacturer-anchors document for the palette of options

# Operational Considerations for MASA and SZTP (RFC8572)

draft-richardson-anima-masa-considerations



RFC8366  
Voucher  
Signer

- manufacturer (or authorized entity) has to maintain private key to sign vouchers!
  - this document provides prescriptive advice on how the private parts are kept, by the manufacturer, **in** the “factory”
  - voucher signer can be single self-signed certificate, up to complex PKI
  - Now references taxonomy-manufacturer-anchors as palette of options

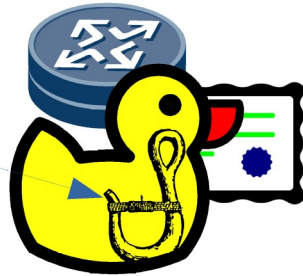


# Operational Considerations for MASA and SZTP (RFC8572) part 2

draft-richardson-anima-masa-considerations



RFC8366  
Voucher  
Signer



- manufacturer (or authorized entity) has to install a trust anchor (public key), into device.
- taxonomy-manufacturer-anchors deals with provisioning of trust anchors as well

# Changes to documents since IETF107

- masa-considerations
  - Rewritten to use taxonomy-manufacturer-anchors
- registrar-considerations-04
  - “certificate authority” → “certification authority”
  - change of authors
  - some editorial comments



**Would the WG  
like to consider  
adoption?**

**(MASA + Register)**

**Are these in charter?**

**Is there interest?**

**Unclear if we should/need to  
publish!**