

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, Jie Yang, (Wei Pan)

IETF 108: 2020-07-30

ANIMA Working Group

History of Documents

ANIMA!

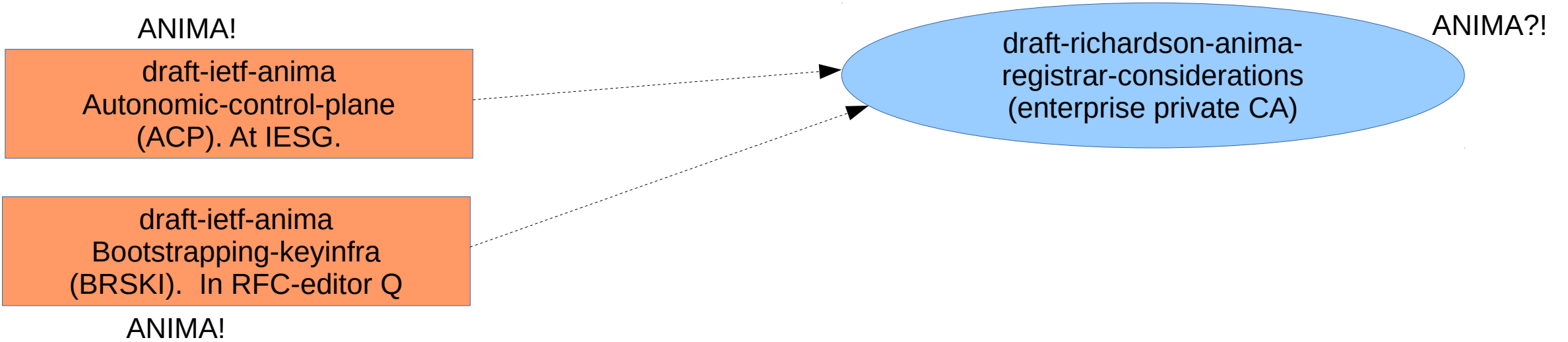
draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.

draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

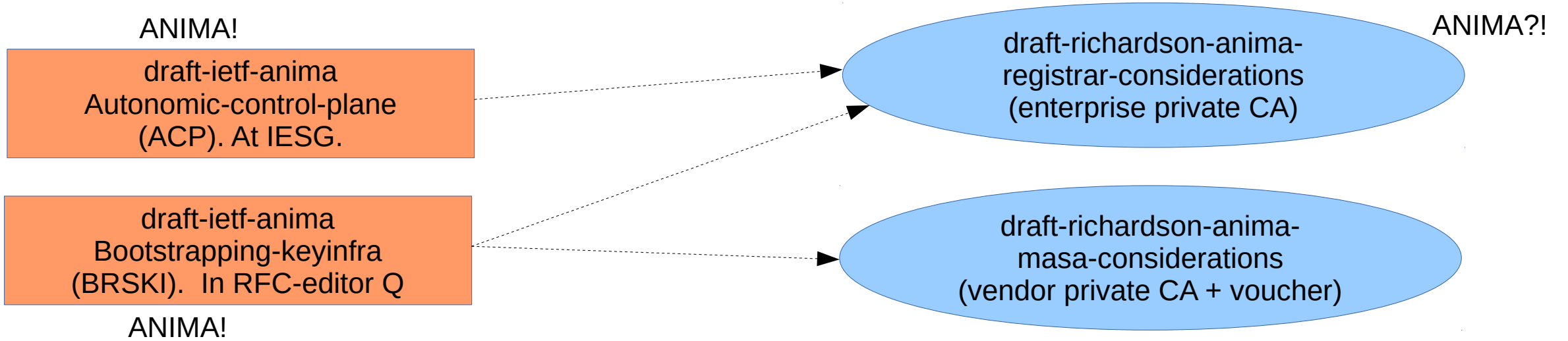
ANIMA!



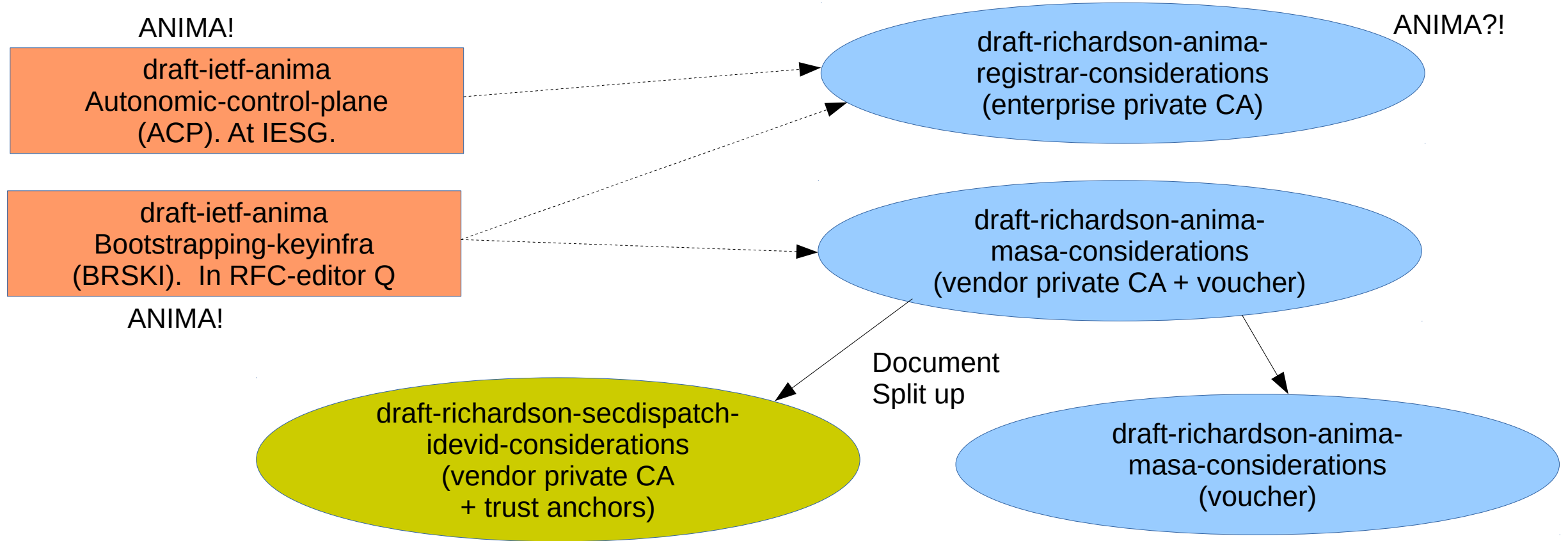
History of Documents



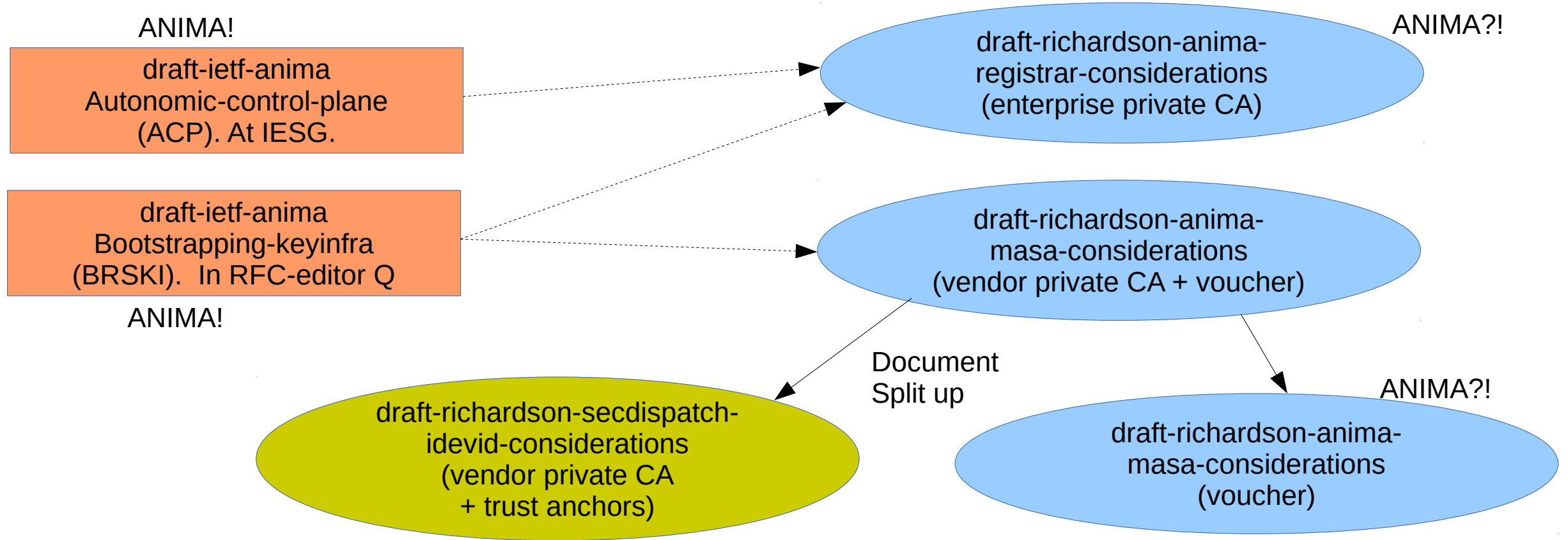
History of Documents



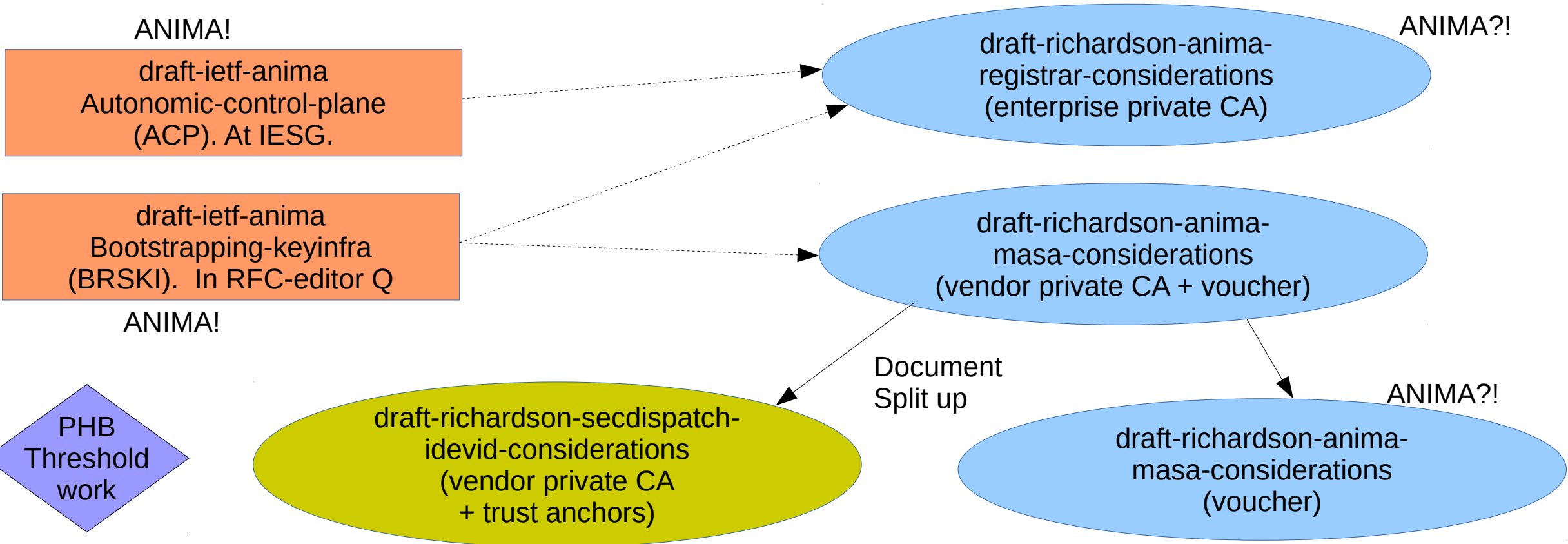
History of Documents



History of Documents

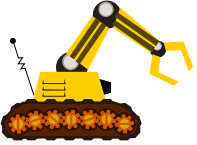


History of Documents



ANIMA ACP/BRSKI security architecture

Vendor/
Manufacturer



IDeVID
PKI



RFC8366
Voucher
Signer

Enterprise/Operator
Owner



Registrar:
LDeVID PKI



Device



IDeVID, LDeVID
Software Update Trust Anchor
Voucher validation Trust Anchor

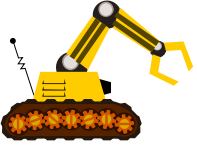


Join
Proxy



ANIMA ACP/BRSKI security architecture

Vendor/
Manufacturer



IDeVID
PKI



RFC8366
Voucher
Signer

Enterprise/Operator
Owner



Registrar:
LDeVID PKI

anima-
registrar-
considerations



Device



IDeVID, LDeVID
Software Update Trust Anchor
Voucher validation Trust Anchor



Join
Proxy



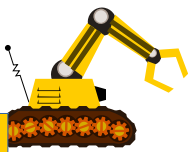
ANIMA ACP/BRSKI security architecture

Vendor/
Manufacturer

Enterprise/Operator
Owner

anima-
registrar-
considerations

anima-
masa-
considerations



IDeVID
PKI



Registrar:
LDeVID PKI



RFC8366
Voucher
Signer



Device



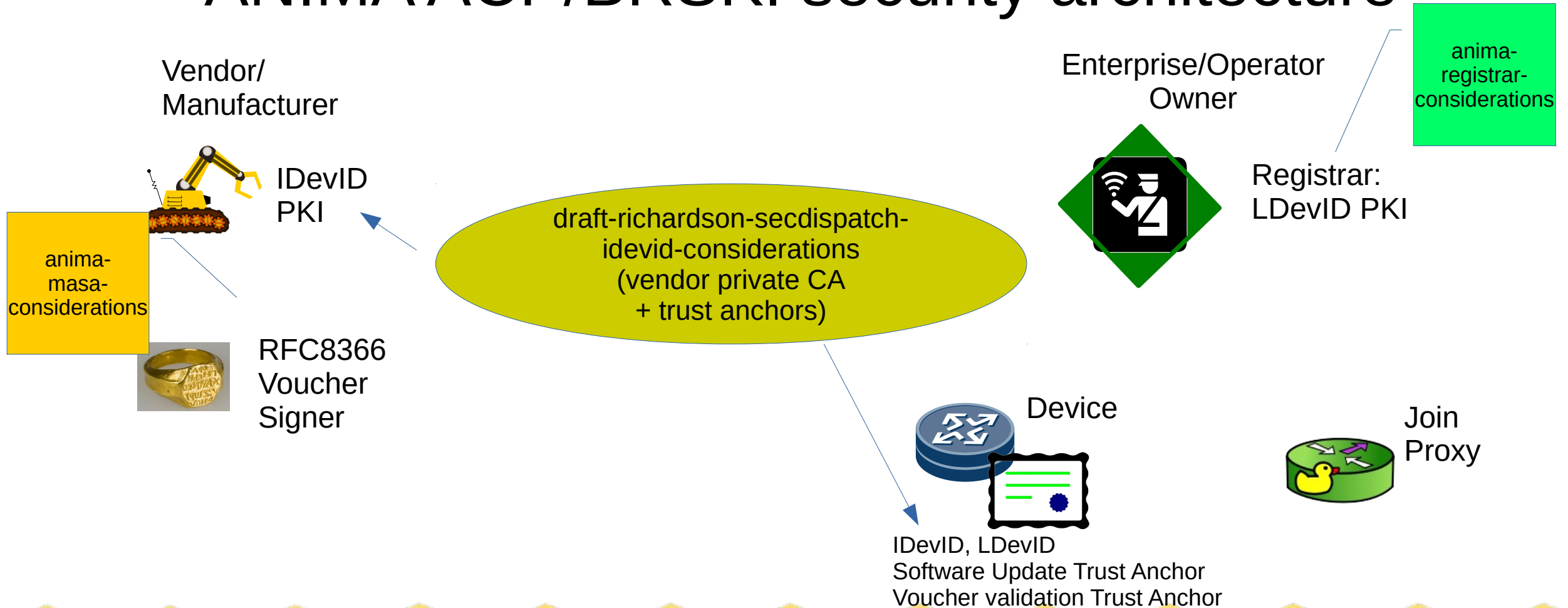
IDeVID, LDeVID
Software Update Trust Anchor
Voucher validation Trust Anchor



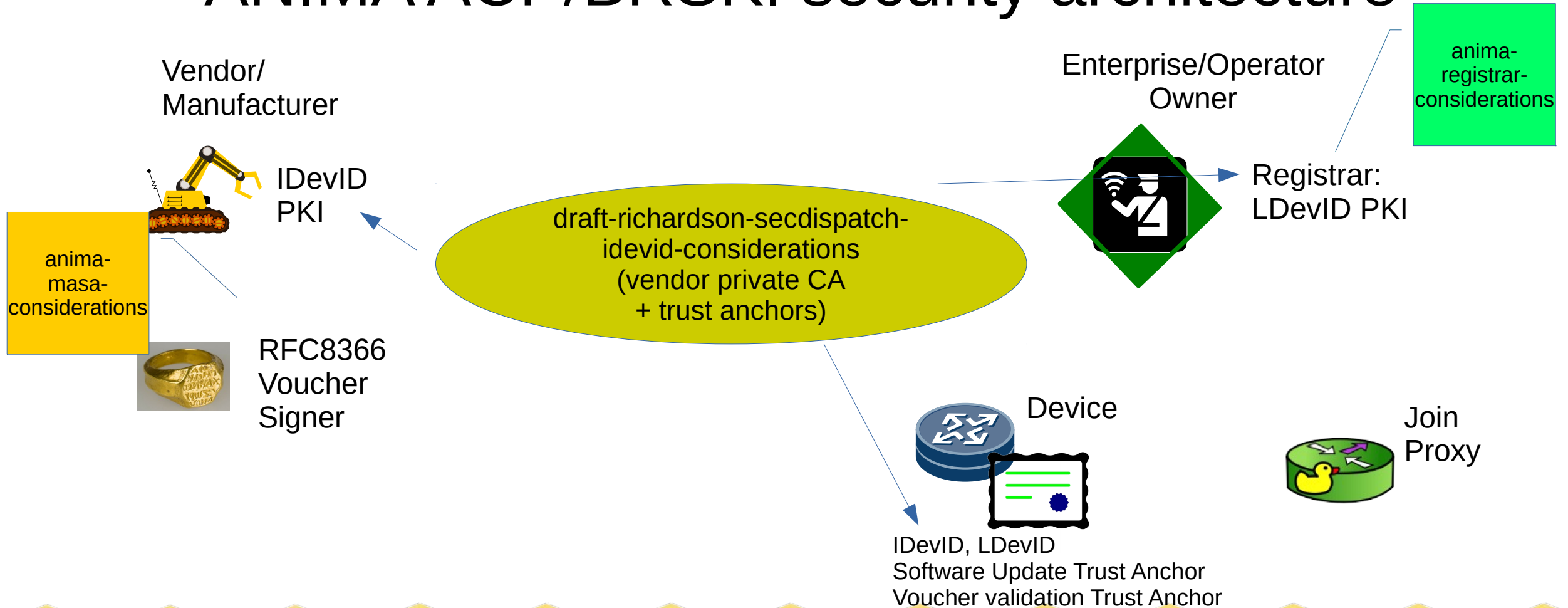
Join
Proxy



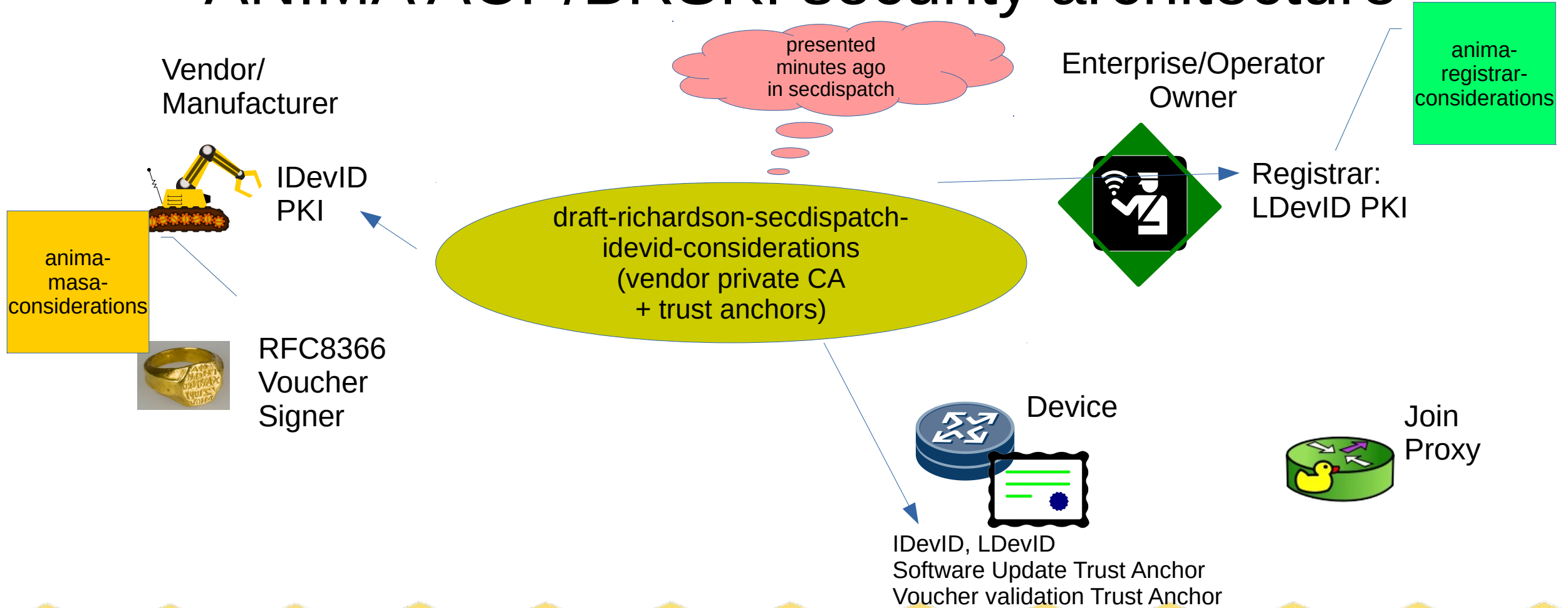
ANIMA ACP/BRSKI security architecture



ANIMA ACP/BRSKI security architecture

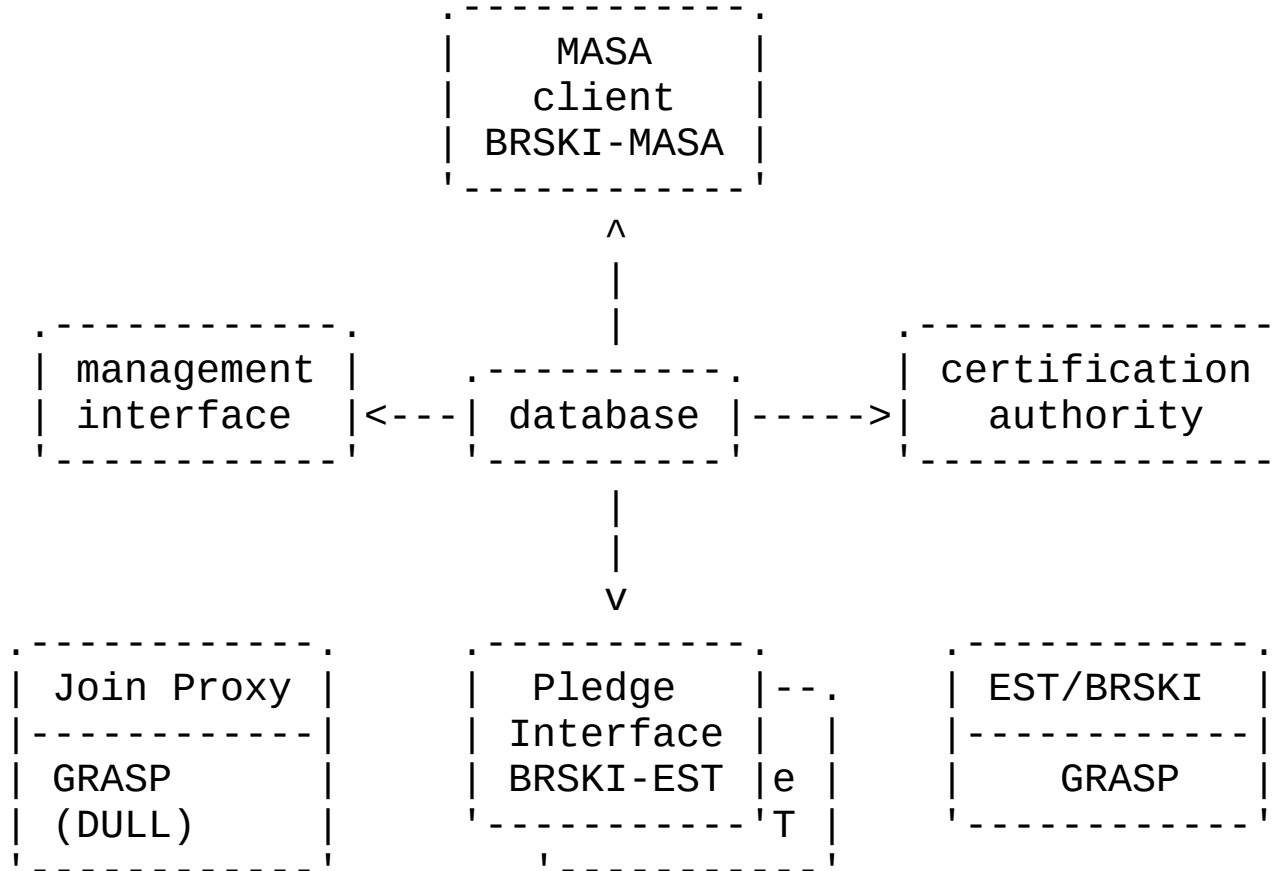


ANIMA ACP/BRSKI security architecture



Operational Considerations for Registrar

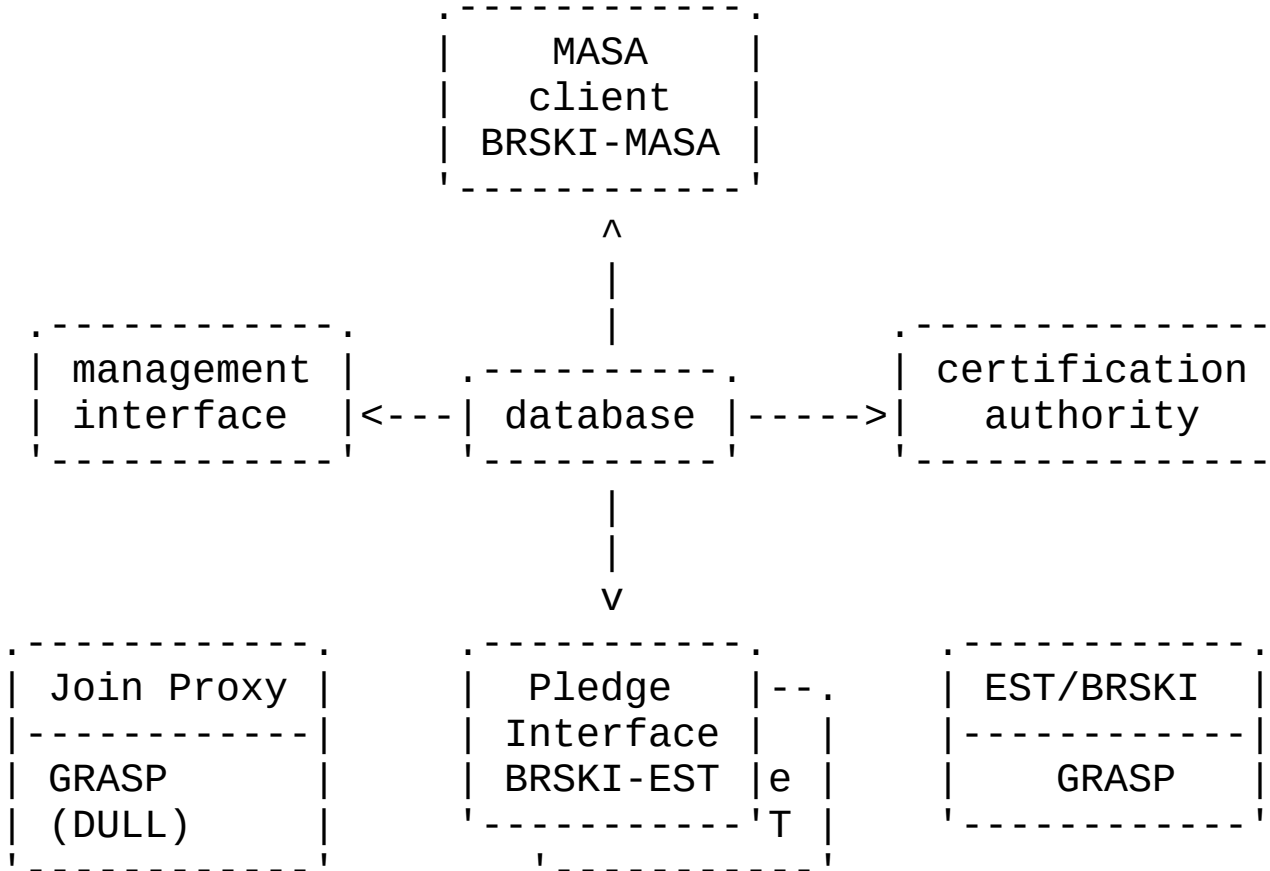
draft-richardson-anima-registrar-considerations



Operational Considerations for Registrar

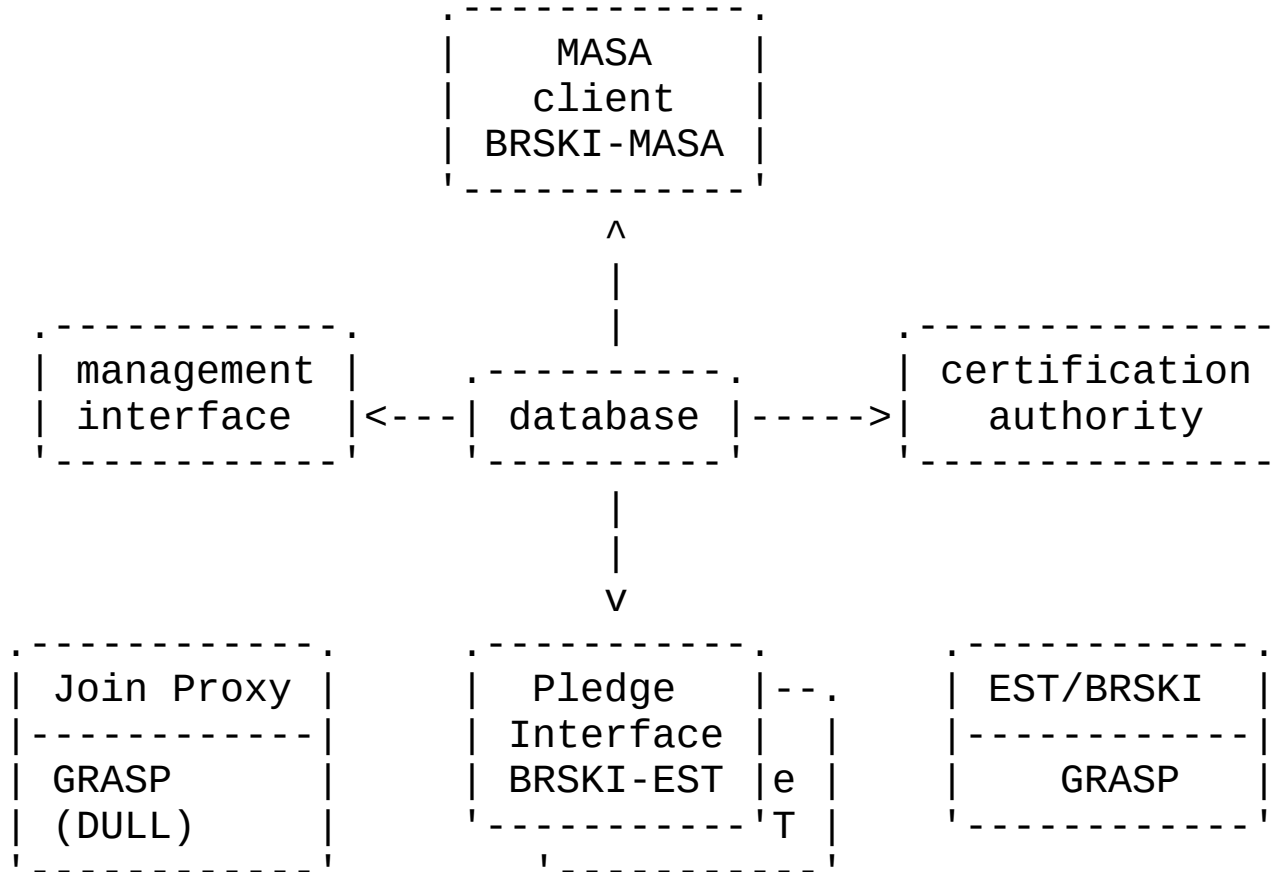
draft-richardson-anima-registrar-considerations

This document is about many design issues, including:



Operational Considerations for Registrar

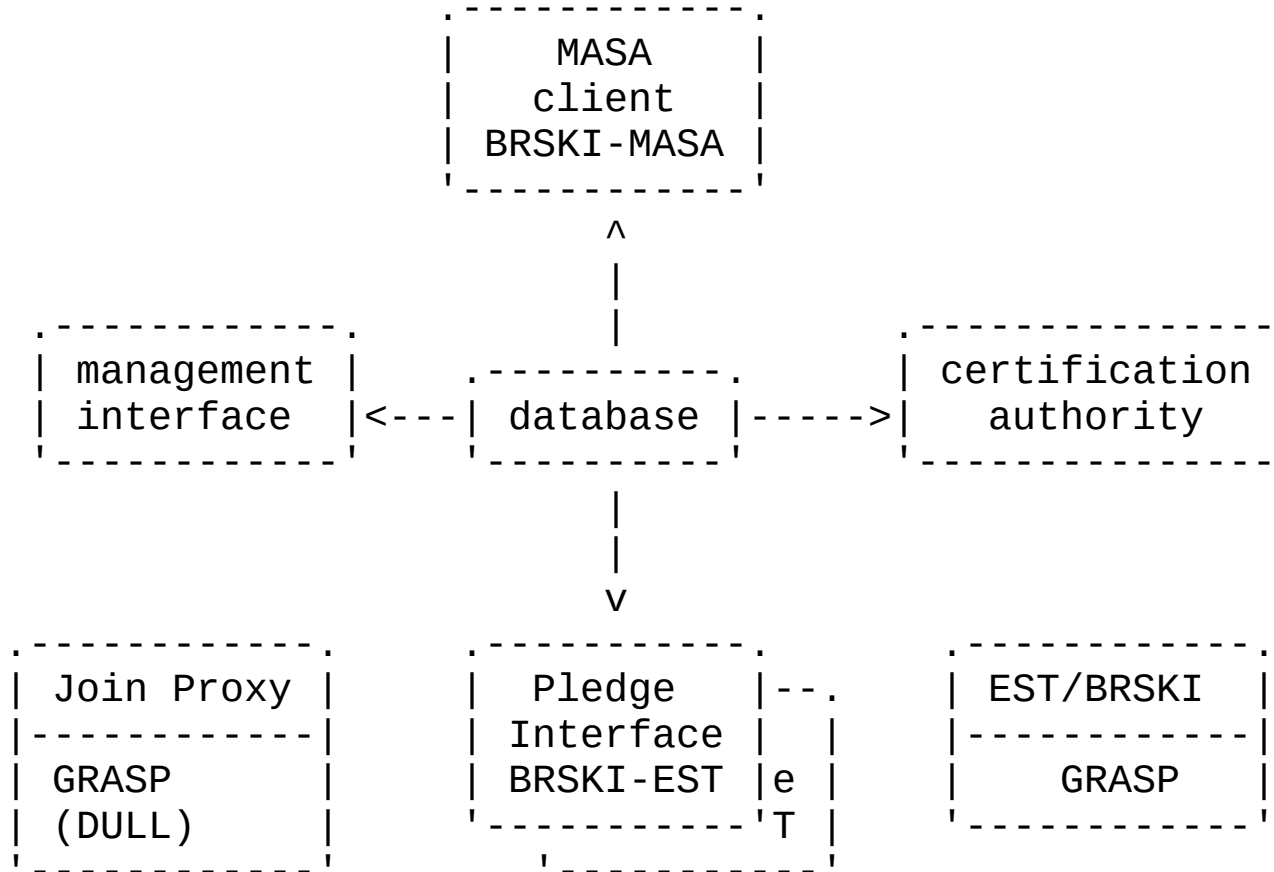
draft-richardson-anima-registrar-considerations



This document is about many design issues, including:
1) prescriptive statements about appropriate security for the private certification authority

Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations

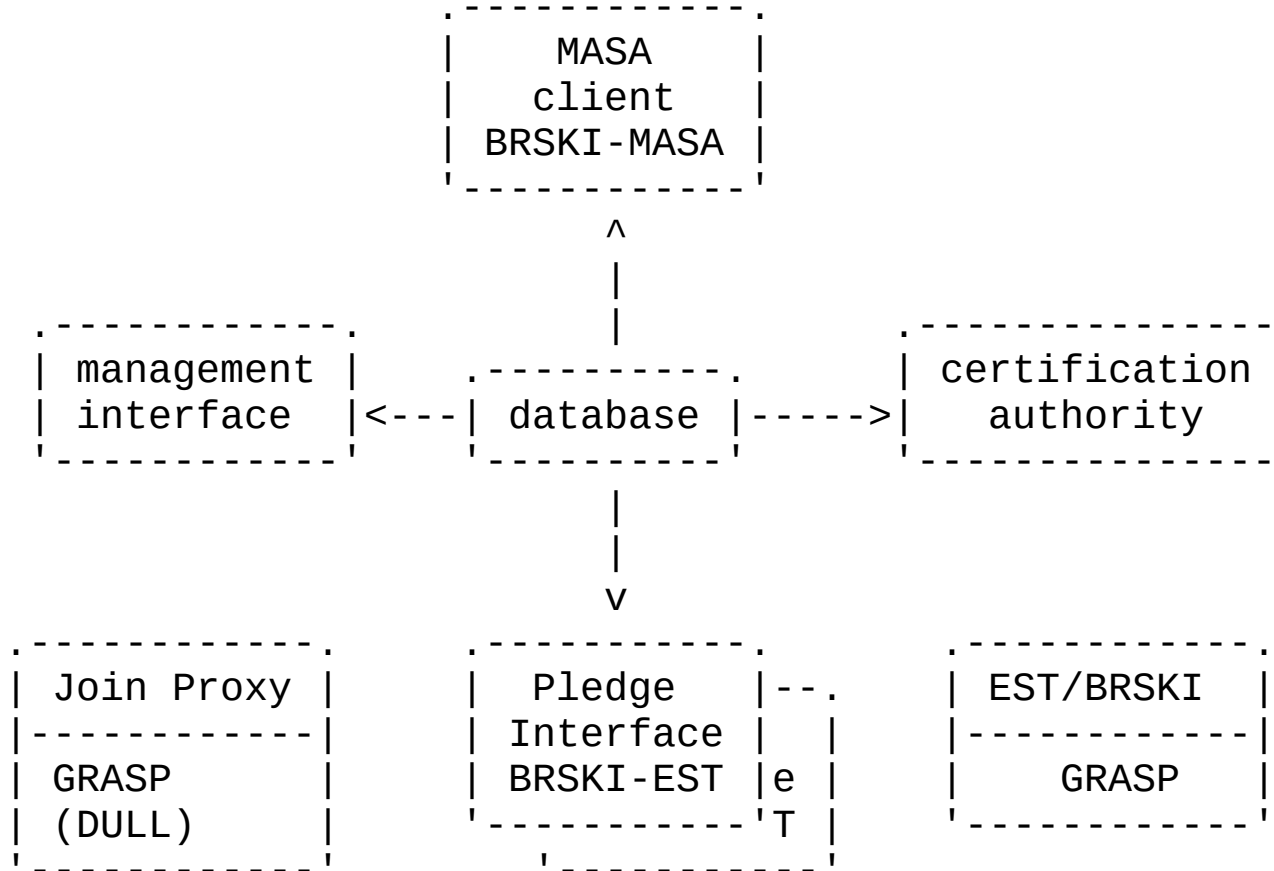


This document is about many design issues, including:

- 1) prescriptive statements about appropriate security for the private certification authority
- 2) scaling issues relating to TLS/HTTPS operations

Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations

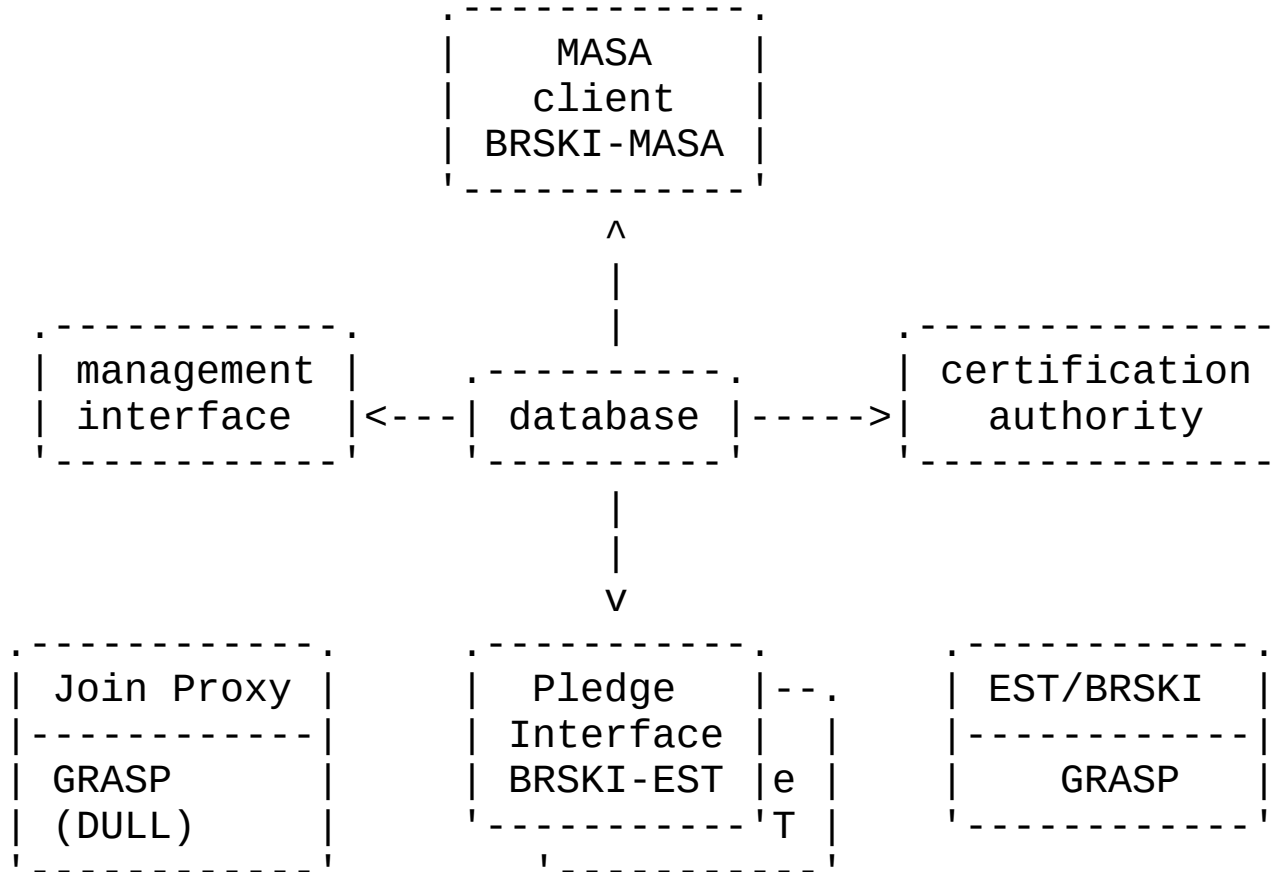


This document is about many design issues, including:

- 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

Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations

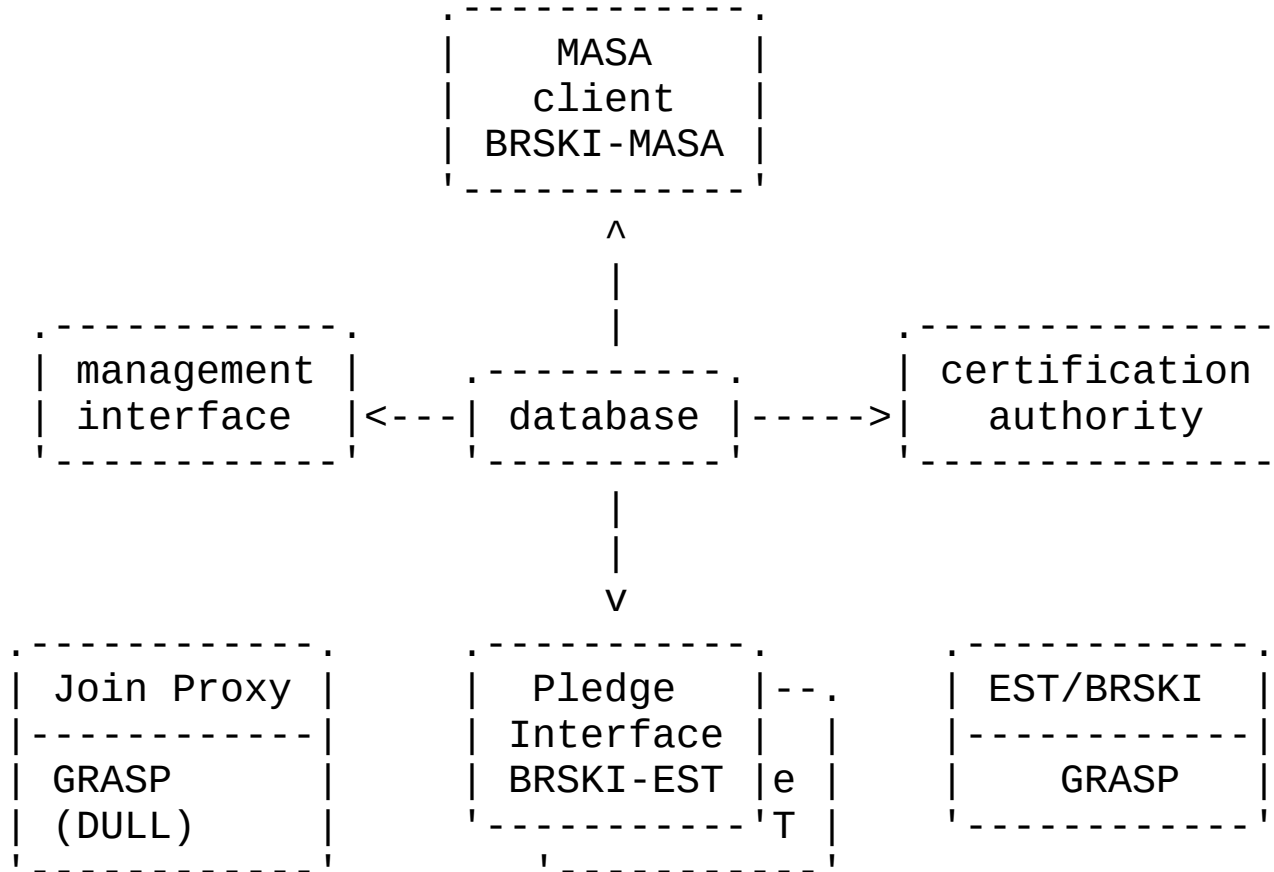


This document is about many design issues, including:

- 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

Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations

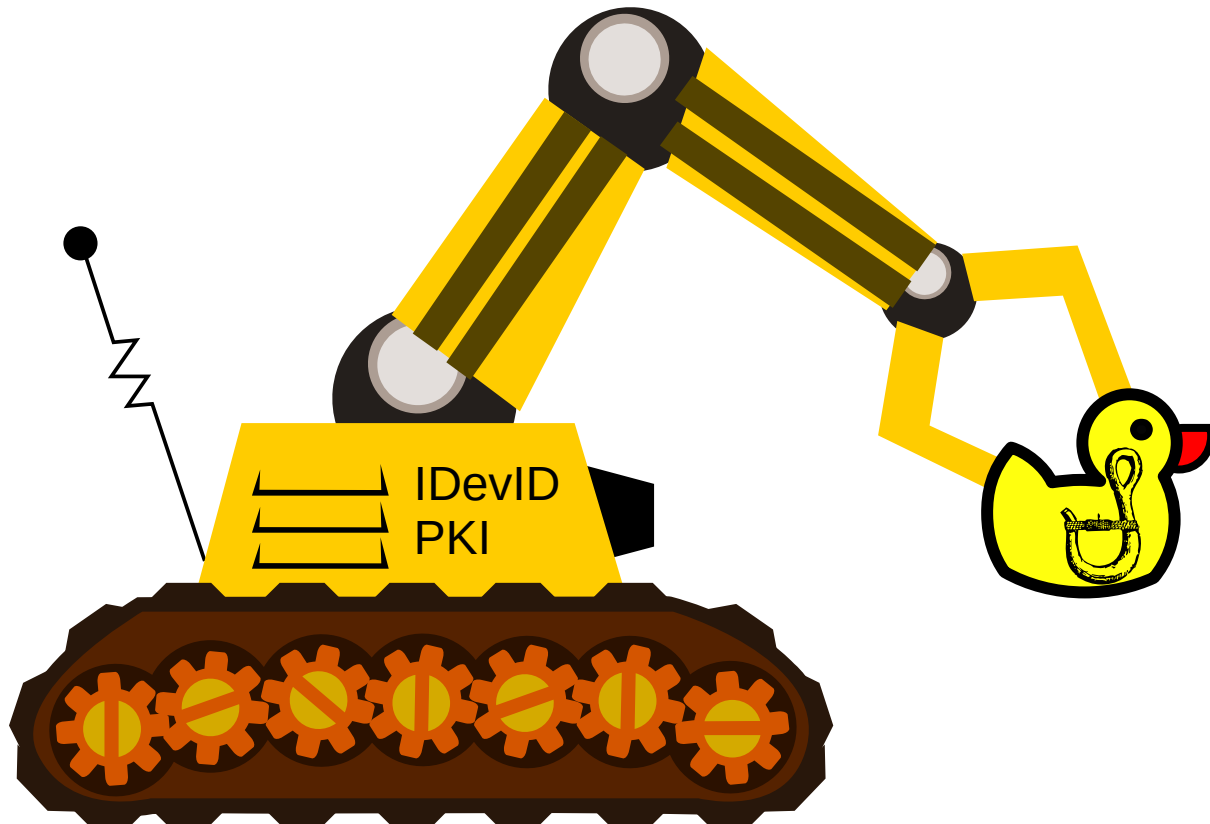


- This document is about many design issues, including:
- 1) prescriptive statements about appropriate security for the private certification authority
 - 2) scaling issues relating to TLS/HTTPS operations
 - 3) synchronous vs asynchronous issues on how BRSKI-MASA client interacts with BRSKI-EST server
 - 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”
 - intended to reference idevid-considerations document as a “palette” of options

Operational Considerations for MASA and SZTP (RFC8572)

draft-richardson-anima-masa-considerations



RFC8366
Voucher
Signer

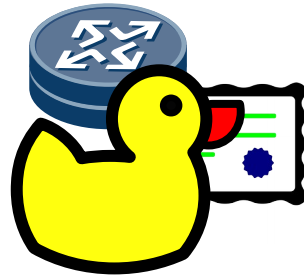
- manufacturer (or authorized entity) has to maintain private key to sign vouchers
 - this document provides prescriptive advice on how the private parts are kept, by the manufacturer, **in** the “factory”
 - voucher signer can be single self-signed certificate, up to complex PKI
 - intended to reference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

Operational Considerations for MASA and SZTP (RFC8572) part 2

draft-richardson-anima-masa-considerations



RFC8366
Voucher
Signer



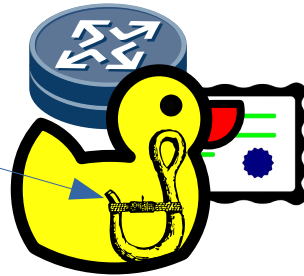
- manufacturer (or authorized entity) has to install a trust anchor (public key), into device.
- idevid-considerations deals with provisioning of trust anchors as well

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.
- idevid-considerations deals with provisioning of trust anchors as well

Changes to documents since IETF107

- masa-considerations
 - many editorial comments, some new references
 - gutted, most text went into idevid-considerations
 - idevid-considerations presented at secdispatch a few minutes ago
 - change of authors
 - needs to be re-written leveraging idevid-considerations (if document will find a home)
- 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?

Thank You!

idevid-considerations screencast:

<https://www.sandelman.ca/SSW/ietf/meeting/ietf108/idevid1-2020-07-24.ogv>