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

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

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

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

draft-richardson-anima-
registrar-considerations (enterprise private CA)

ANIMA!

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

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

draft-richardson-anima-
registrar-considerations
(enterprise private CA)

draft-richardson-anima-
masa-considerations
(vendor private CA + voucher)
History of Documents

- **draft-ietf-anima**: Autonomic-control-plane (ACP). At IESG.
- **draft-iets-anima**: Bootstrapping-keyinfra (BRSKI). In RFC-editor Q
- **draft-richardson-anima-registrar-considerations**: (enterprise private CA)
- **draft-richardson-anima-masa-considerations**: (vendor private CA + voucher)
- **draft-richardson-secdispatch-idevid-considerations**: (vendor private CA + trust anchors)
- **draft-richardson-anima-masa-considerations**: (voucher)

ANIMA!

ANIMA!

ANIMA?!
History of Documents

draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.
draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

draft-richardson-anima-
registrar-considerations
(enterprise private CA)
draft-richardson-anima-
masa-considerations
(vendor private CA + voucher)
draft-richardson-secdispatch-
idevid-considerations
(vendor private CA + trust anchors)
draft-richardson-anima-
masa-considerations
(voucher)
History of Documents

draft-ietf-anima
Autonomic-control-plane (ACP). At IESG.
draft-ietf-anima
Bootstrapping-keyinfra (BRSKI). In RFC-editor Q

draft-richardson-anima-registrar-considerations (enterprise private CA)
draft-richardson-anima-masa-considerations (vendor private CA + voucher)
draft-richardson-anima-masa-considerations (voucher)
draft-richardson-secdispatch-idevid-considerations (vendor private CA + trust anchors)

PHB Threshold work

ANIMA! ANIMA?!

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

Device

IDevID, LDevID
Software Update Trust Anchor
Voucher validation Trust Anchor

Join Proxy
ANIMA ACP/BRSKI security architecture

Vendor/Manufacturer

IDevID

PKI

Rule

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

draft-richardson-secdispatch-idevid-considerations (vendor private CA + trust anchors)

Registrar: LDevID PKI

Enterprise/Operator Owner

Join Proxy

Device

IDevID, LDevID Software Update Trust Anchor
Voucher validation Trust Anchor
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

draft-richardson-secdispatch-idevid-considerations
(vendor private CA + trust anchors)
ANIMA ACP/BRSKI security architecture

Vendor/Manufacturer

IDevID PKI

RFC8366 Voucher Signer

draft-richardson-secdispatch-idevid-considerations
(vendor private CA + trust anchors)

Enterprise/Operator Owner

Registrar: LDevID PKI

Join Proxy

Device

IDevID, LDevID
Software Update Trust Anchor
Voucher validation Trust Anchor

Presented minutes ago in secdispatch
Operational Considerations for Registrar

MASA
client
BRSKI-MASA

management
interface

database

certification
authority

Join Proxy

GRASP
(DULL)

Pledge
Interface
BRSKI-EST

EST/BRSKI

GRASP
Operational Considerations for Registrar

draft-richardson-anima-registrar-considerations

This document is about many design issues, including:

MASA
client
BRSKI-MASA

management
interface
<-- database

Join Proxy
GRASP
(DULL)

Pledge Interface
BRSKI-EST

certification
authority

EST/BRSKI

GRASP
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.
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
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
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

- 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 idevidev-considerations document as a “palette” of options
Operational Considerations for MASA and SZTP (RFC8572) part 2
draft-richardson-anima-masa-considerations

- 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

- 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: