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/

Michael Richardson, (Wei Pan)

IETF 116: 2023-03-29

ANIMA Working Group
History of Documents

RFC8994 (ACP). Published

RFC8995 (BRSKI).

ANIMA!

Taxonomy Manufacturer Anchors T2TRG: *IRTF*
(vendor private CA + trust anchors)

ANIMA?

ANIMA!

ANIMA?

ANIMA?

Document Split up

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

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

draft-richardson-anima-masa-considerations (voucher)

PHB Threshold work
ANIMA ACP/BRSKI security architecture

Vendor/Manufacturer

IDevID PKI

Enterprise/Operator Owner

Registrar: LDevID PKI

masa-
considerations

Taxonomy Manufacturer Anchors
T2TRG: *IRTF*
(vendor private CA + trust anchors)

RFC8366
Voucher Signer

Device

IDevID, LDevID
Software Update Trust Anchor
Voucher validation Trust Anchor

Join Proxy
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 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

- 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

- 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!