Operational Considerations for MASA

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

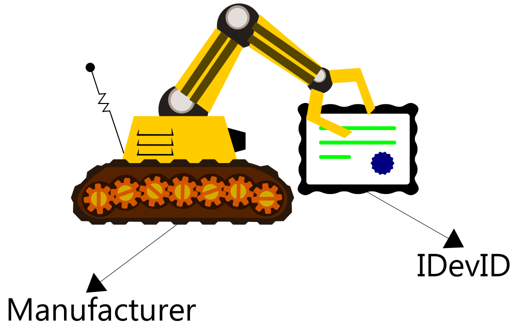
Michael Richardson, Wei Pan

IETF 107

ANIMA Working Group

Two Aspects of Relationship b/w Device and Manufacturer

- Manufacturer provisions an identity (IDevID) for the device
  - Device identity is validated by MASA before issuing the voucher
  - Considerations include:
    - Key Pair Generation
    - PKI for IDevID



- Manufacturer provides a mechanism that convinces the device to trust the new owner
  - Device can validate that the **voucher** is issued by a legitimate MASA
  - Considerations include:
    - PKI for MASA signing keys
    - Different MASA types

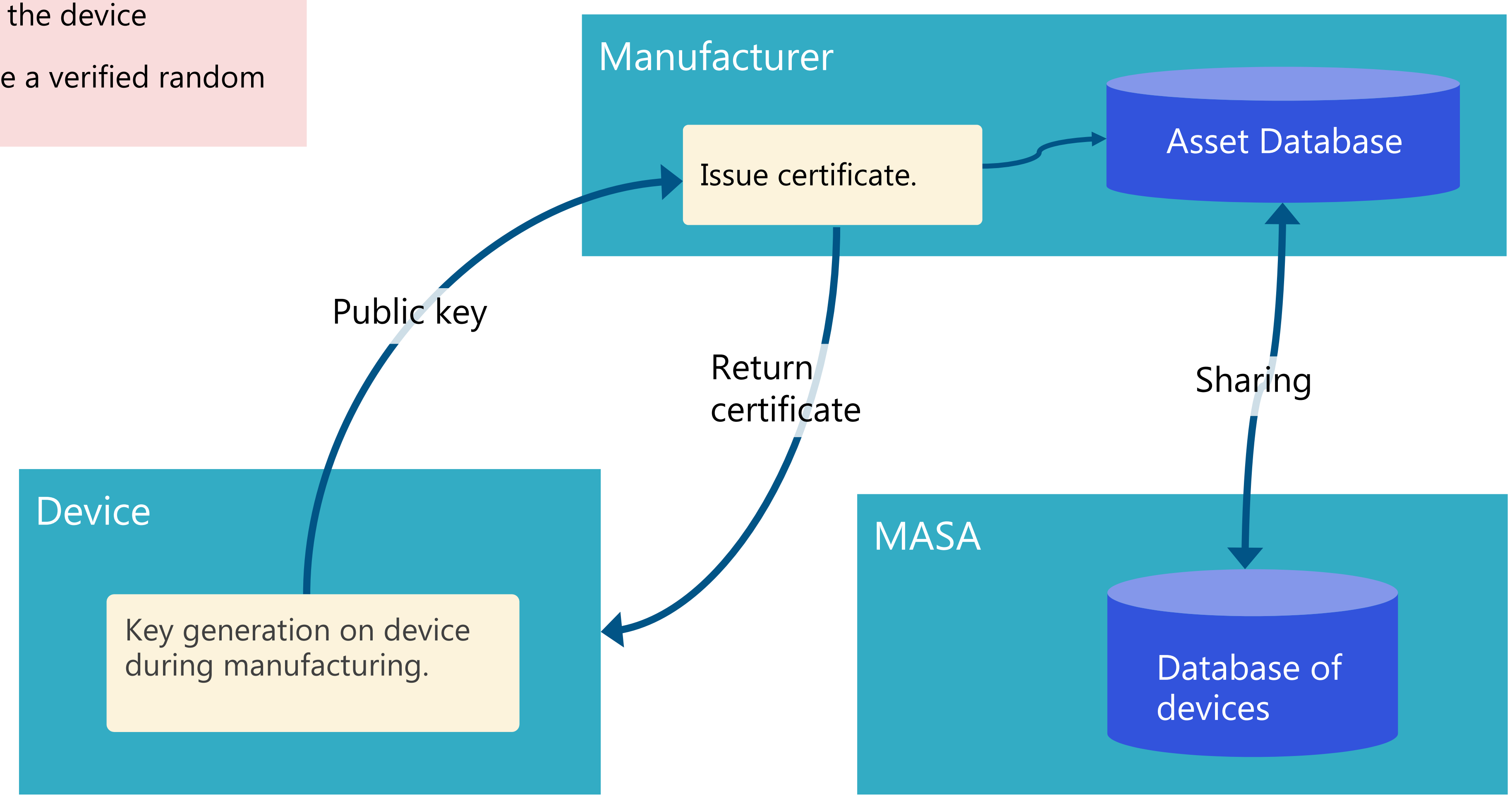
Operational Considerations for IDevID

—— Key Pair Generation

- On-device Key Pair Generation
- Off-device Key Pair Generation
- Key Pair Generation Based on 256-bit Secret Seed
  - (nice to have name for this)

On-device Key Pair Generation

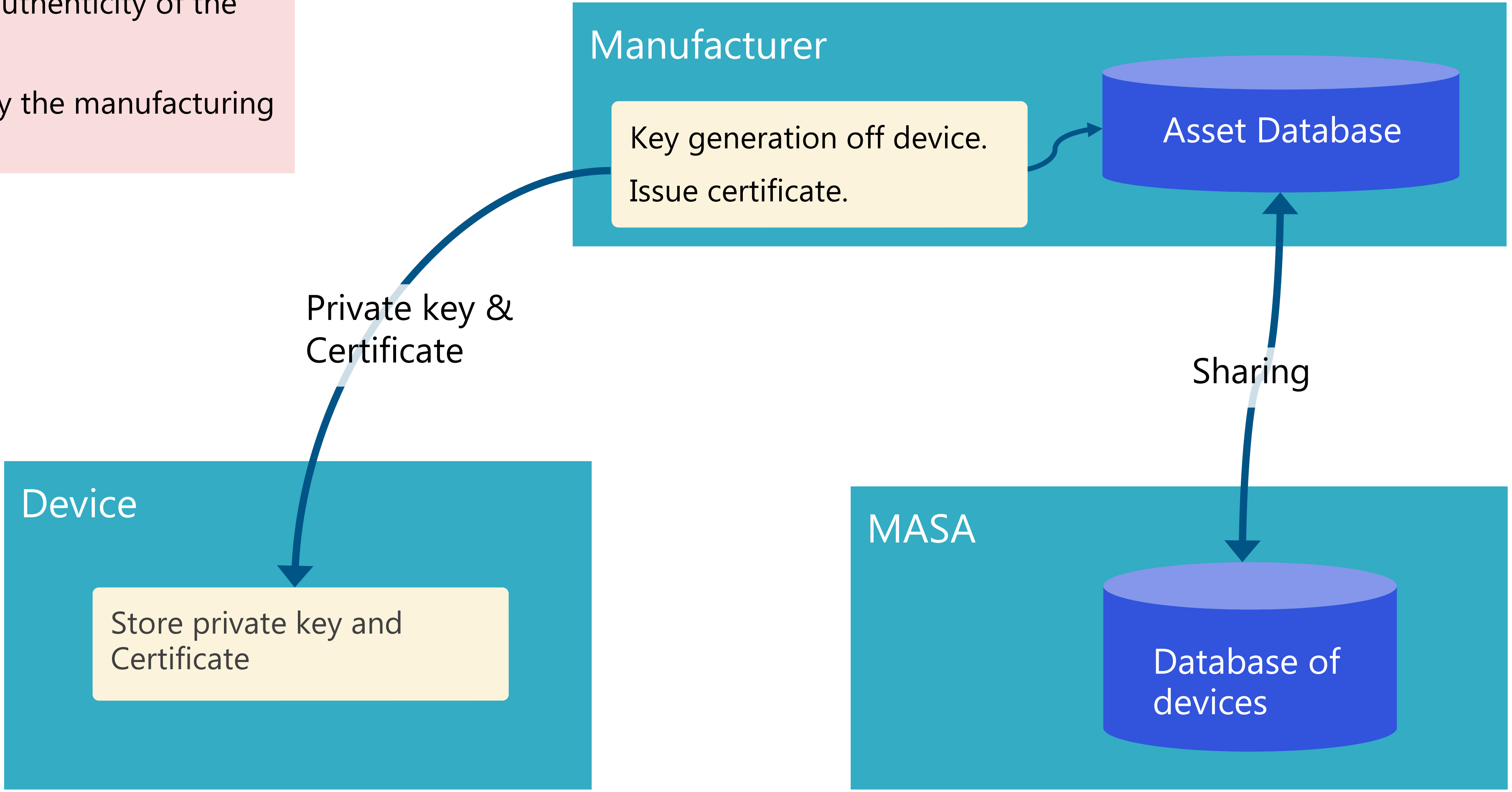
- Private key never leaves the device
- But, device may not have a verified random number generator



Images adapted from those presented by Laurence Lundblade

Off-device Key Pair Generation

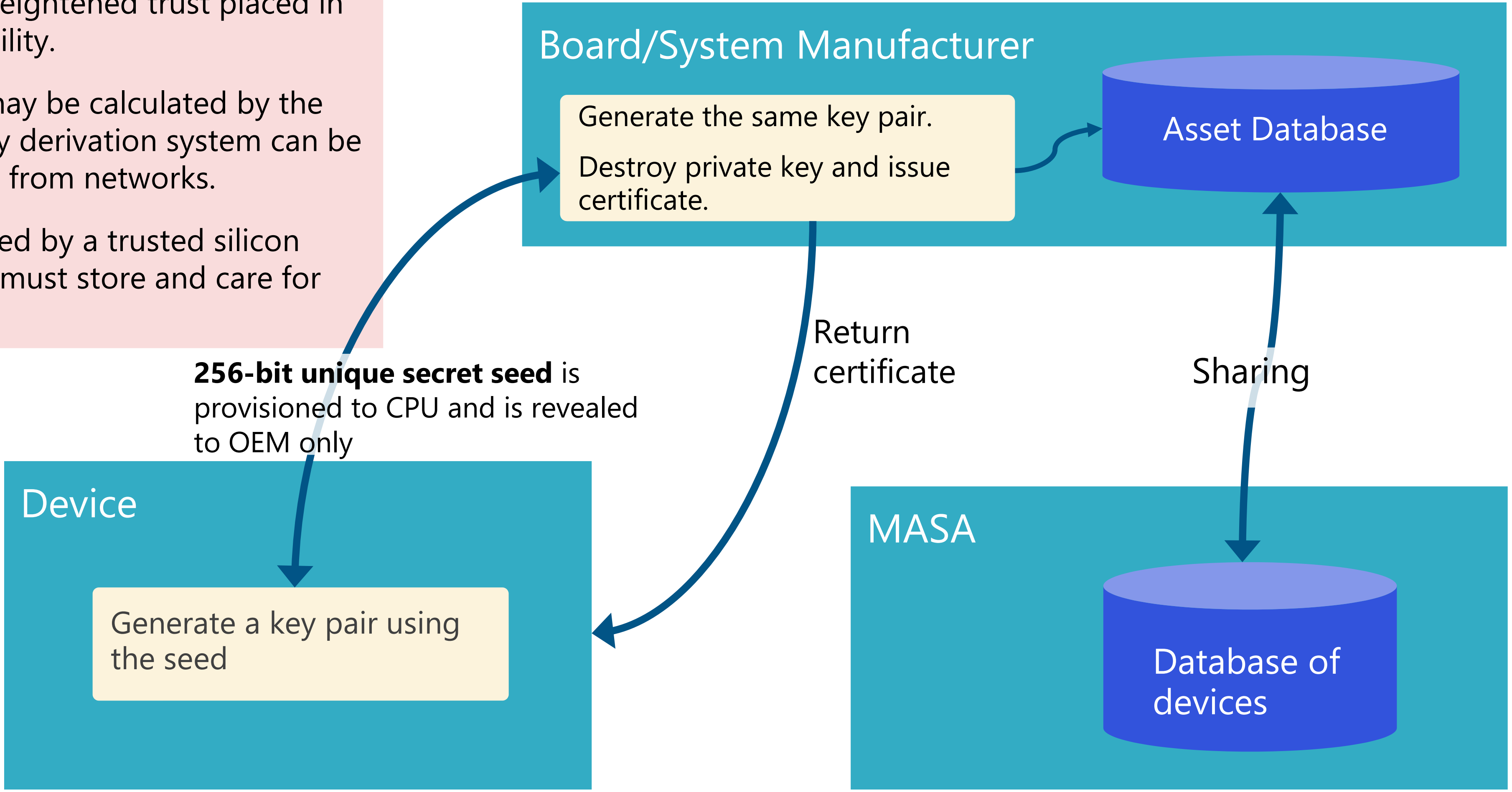
- Better randomness, the authenticity of the public key is well known
- But, private key is seen by the manufacturing infrastructure


Manufacturer
Key generation off device.
Issue certificate.
Asset Database
Private key & Certificate
Sharing
Device
Store private key and Certificate
MASA
Database of devices

Images adapted from those presented by Laurence Lundblade

Key Pair Generation Based on (256-bit) Secret Seed

- Trust is replaced with a heightened trust placed in the silicon fabrication facility.
- Key Pair and certificate may be calculated by the OEM asynchronously. Key derivation system can be completely disconnected from networks.
- But, OEM must be supplied by a trusted silicon fabrication system. OEM must store and care for these keys very carefully



Board/System Manufacturer
Generate the same key pair.
Destroy private key and issue certificate.
Asset Database
Return certificate
Sharing
256-bit unique secret seed is provisioned to CPU and is revealed to OEM only
Device
Generate a key pair using the seed
MASA
Database of devices

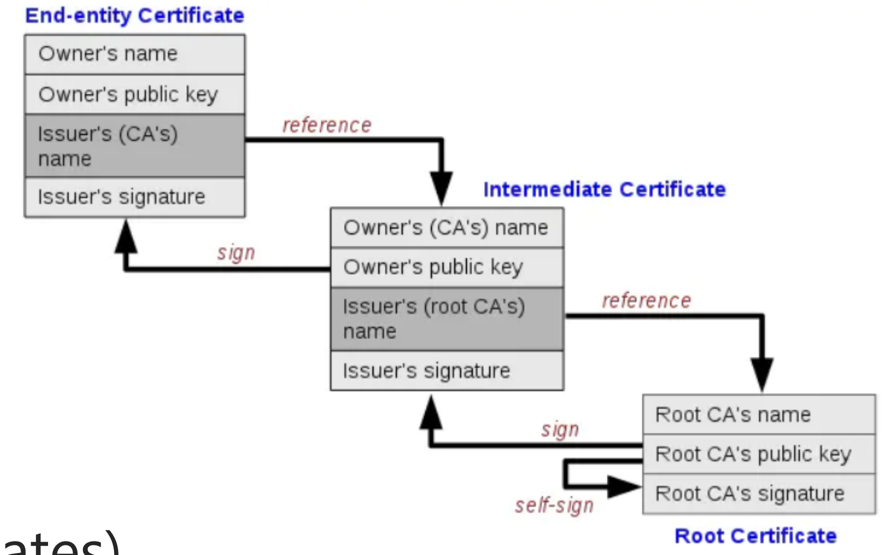
Images adapted from those presented by Laurence Lundblade

Operational Considerations for IDevID

—— PKI for IDevID

- Three-tier PKI infrastructure is appropriate
- A root CA
  - Private key kept offline
  - Issue intermediate CA certificates
- A number of intermediate CAs
  - Have online private keys
  - Issue IDevID certificates
  - Periodically destroy the private key and generate a new one
- Many End-Entity certificates (i.e., IDevID certificates)

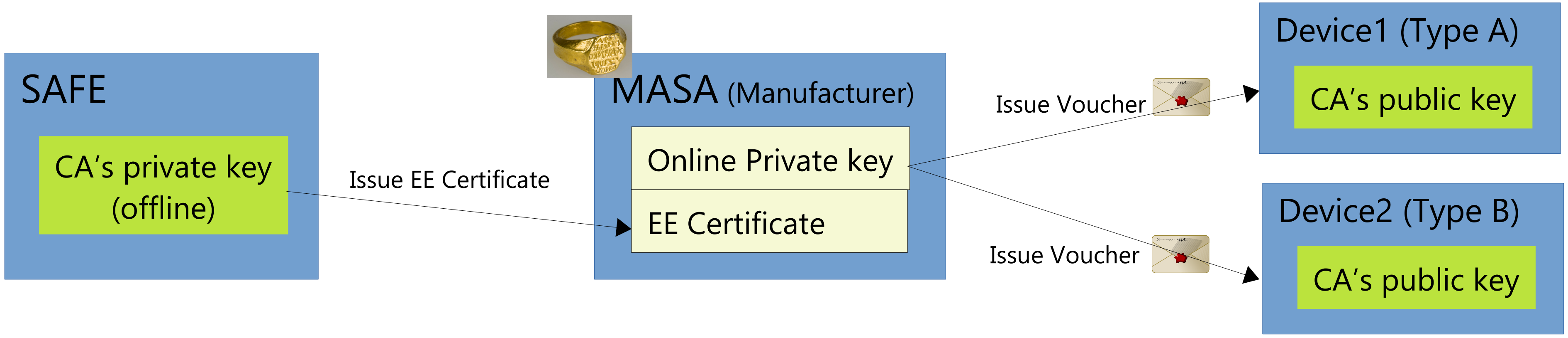
Some say this is properly a two-tier, as the EE leaf Should Not count



Operational Considerations for MASA

—— Self-contained multi-product MASA

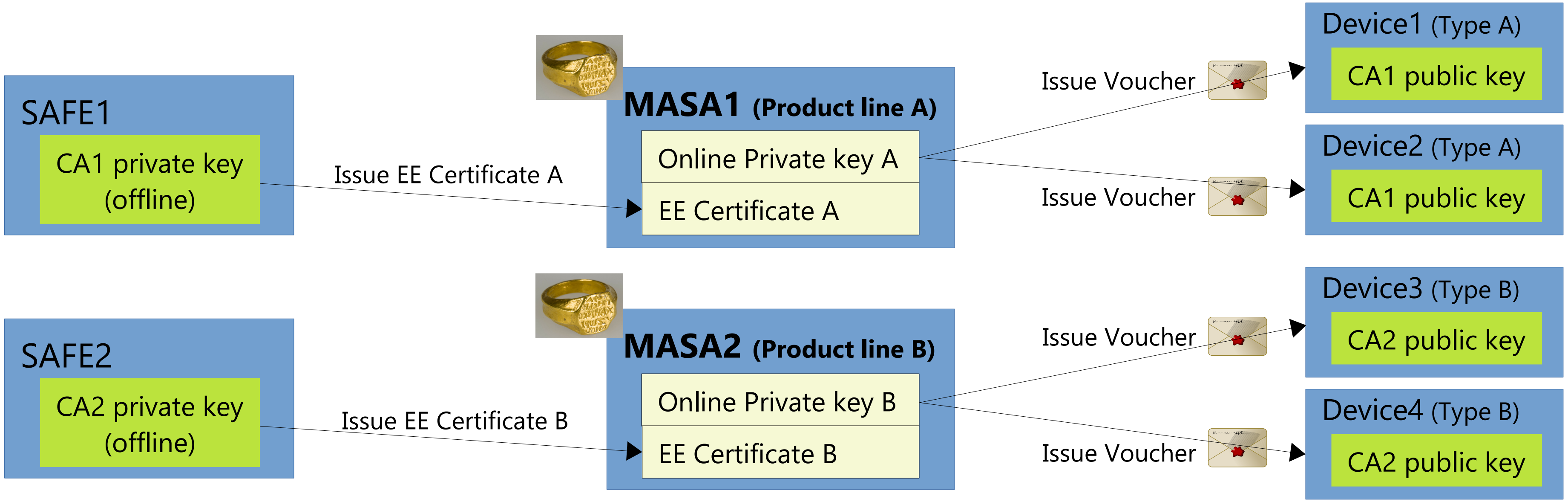
- A offline CA
  - Periodically sign a new End-Entity (EE) Certificate (i.e., MASA certificate)
- Use EE Certificate’s online private key to sign voucher
- Public key of the offline CA is built-in to the firmware of the device, providing a trust anchor with which to validate vouchers



Operational Considerations for MASA

—— Self-contained per-product MASA

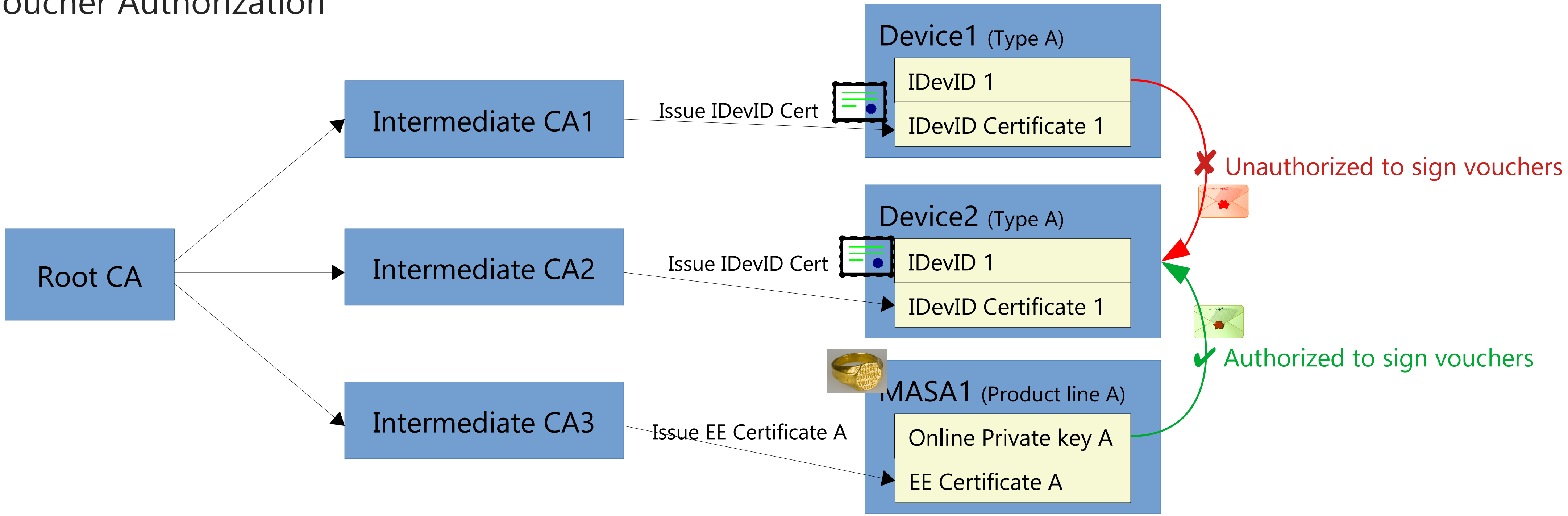
- A simple enhancement to the previous scenario is to **have a unique MASA offline key for each product line**
  - Private keys kept separately, compromise of a single product line MASA doesn't compromise all products
  - If a product line is sold to another entity, the MASA escrow process affects only this single product line
  - SerialNumber can be duplicated among different product lines
- Disadvantage: Requires a private key to be stored per product line
- **Per-product MASA signing keys is encouraged**



Operational Considerations for MASA

—— Per-product MASA keys intertwined with IDevID PKI

- **Use the same root CA for MASA Certificate and IDevID Certificates**
  - Pledge needs to make sure that the voucher is signed by a key which is authorized to sign vouchers
  - Prevent the voucher being signed by other devices’ IDevID
- Root CA needs to sign an intermediate CA or End-Entity certificate with an extension OID that is specific for Voucher Authorization



Operational Considerations for MASA

—— Rotating MASA authorization keys

- Have multiple MASA offline key for each product line, and these keys can be rotated though in some deterministic order
  - All of the MASA signing keys need to be online and available in order to respond to any voucher request
  - Keep track of which device trust which key in the asset database

Next steps

- More reviews and comments
- Does some part or all of this work fit into the IETF, and into ANIMA?

Thank You!