

DRAFT-OUNSWORTH-PKIX- KEY-ATTESTATION

IETF 116 – LAMPS

Entrust: [Mike Ounsworth](#), Richard Kettlewell

Crypto4A: Bruno Couillard, JP Fiset

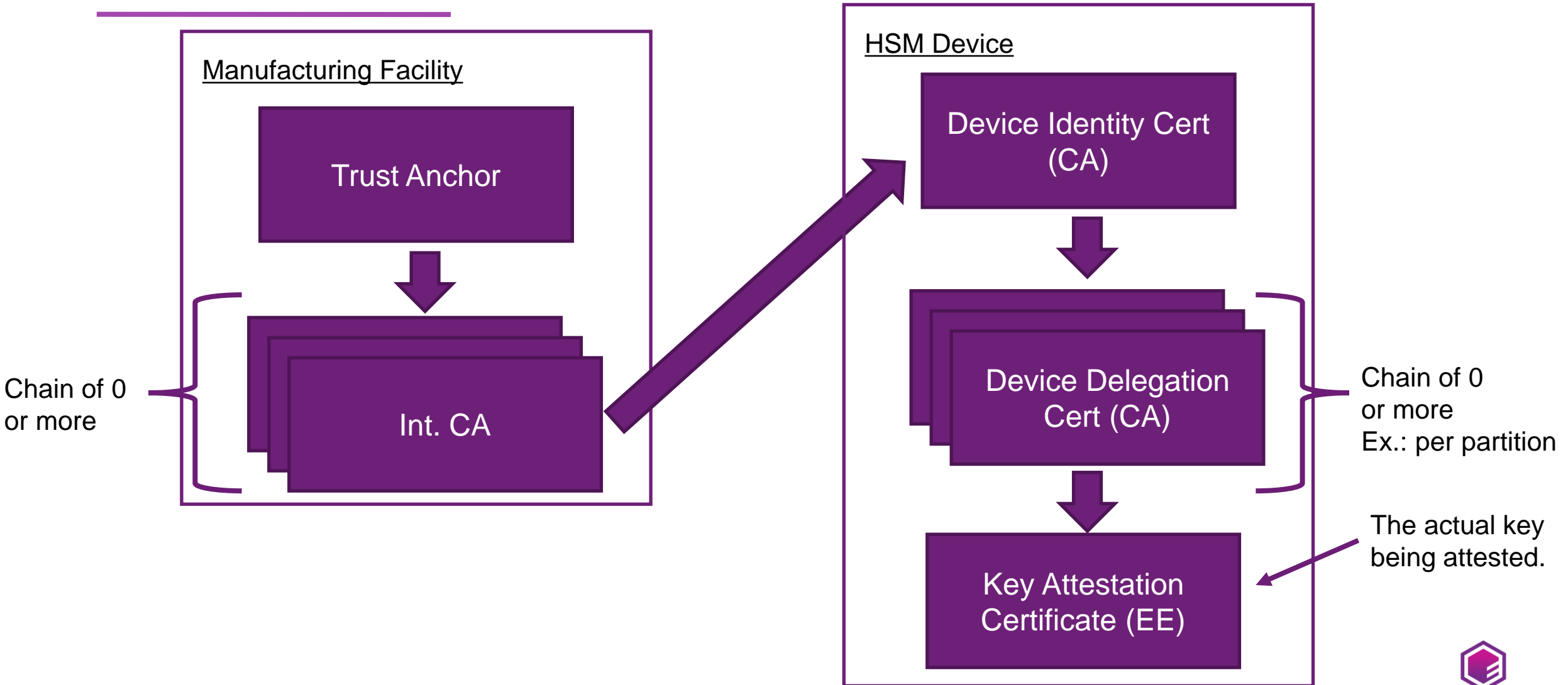


MOTIVATION

- › CA/B Ballots CSC-13 and CSC 17 require code signing certificates to be generated and stored in HSMs by 1 June 2023.
- › HSMs today don't tend to support any key attestation format, and where they do it's a wild west of proprietary formats.
- › Goal: avoid CAs needing to implement dozens of proprietary formats.
- › WebAuthn / RATS / EAT is not a good fit:
 - › We would need to define a WebAuthn Attestation Statement Format to carry the attributes that we care about for HSMs.
 - › Needing to support WebAuthn / CBOR inside HSM boundaries to then put that data into an ASN.1/DER CSR is ... weird.
- › Timeline: no way we'll make Standard + Adoption by 1 June 2023, but maybe within the year?

TECHNICAL OVERVIEW

- › Design principle: “Just an X.509 cert chain with some new v3 extensions”.



TECHNICAL OVERVIEW -- EXTENSIONS

- › Still in flux and under debate.
- › We want to put key policy info in a few v3 extensions throughout the cert chain:
 - › DeviceInformation / DeviceSubkeyInformation / ApplicationKeyInformation
 - › Key Use – we'll probably put this in EKU (may need new EKU types)
 - › Key Policies – high level, vendor-agnostic
 - › Exportable: true/false
 - › Recoverable: true/false
 - › Imported: true/false
 - › Detailed key policies in vendor-specific opaque blob `vendorinfo`.

```
ApplicationKeyInformation ::= SEQUENCE {  
    vendor UTF8String          -- manufacturer of device  
    model UTF8String           -- device model information  
    policy OBJECT IDENTIFIER   -- policy governing key use  
    vendorinfo OCTET STRING    -- vendor-specific information  
}
```

SUPPORTIVE VENDORS

- › Entrust

 - › Both Entrust CA and nShield HSM

- › Crypto4A

- › Forntanix

- › Keyfactor

- › I'm looking for more supporters. I'll be starting a bi-weekly author's meeting after 116.

Adoption?

(I suppose “because LAMPS” this actually needs a charter change?)

(Dispatch? is there a better place than LAMPS?)