MOTIVATION

- CA/B Ballots [CSC-13](link) and [CSC 17](link) 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?

draft-ounsworth-pkix-key-attestation
TECHNICAL OVERVIEW

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

Chain of 0 or more

HSM Device

Device Identity Cert (CA)

Device Delegation Cert (CA)

Key Attestation Certificate (EE)

The actual key being attested.

Chain of 0 or more

Ex.: per partition

draft-ounsworth-pkix-key-attestation
TECHNICAL OVERVIEW -- EXTENSIONS

- We want to put key policy info in a few v3 extensions throughout the cert chain:
  - DeviceInformation / DeviceSubkeyInformation / ApplicationKeyInformation
    - Vendor-agnostic info in defined fields.
    - Vendor-proprietary policy info goes in vendorinfo.

- New Extended Key Use (EKU) types indicate key policies within the HSM, ex.:
  
  `id-Recoverable OBJECT IDENTIFIER ::= { tbd }
  -- the key can be recovered under administrative control
  -- basically, an intentionally vague “can it be exported?”`

- Intention: A CA can tell if this key meets CA/B BRs without needing to parse the vendorinfo, but can do so to apply more detailed issuance policy.
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?)

Russ suggested combining with draft-ietf-lamps-key-attestation-ext, which also dodges the charter issue.

draft-ounsworth-pkix-key-attestation