Industry Requirements

Phillip Hallam-Baker

Current Status

- We have standards based certificate enrollment
- We have easy to use certificate enrollment

- These are not the same things
  - We would like them to be

Why Change to a Standard

- Plug ins don’t deliver
  - Installation cost of plug-in >> cost of a cert enrollment.
    - Have to be managing 10s of certs to begin to see benefits.
  - Have to maintain plug in
  - Can’t test interactions with other plug-ins

Common Requirements

- Frictionless usability
  - No unnecessary user effort
  - Enable short lived certs

- Read my lips – No new ASN.1
  - JSON is the way to go
  - Want approach that can be applied to related specs

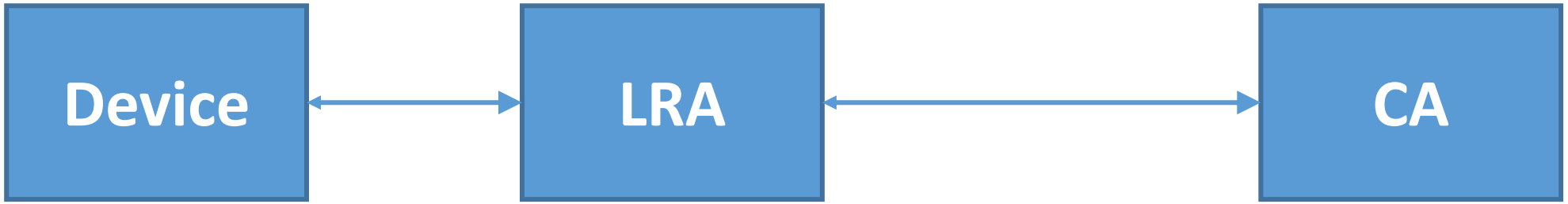
- Interop with existing back-end systems
  - Generate CSRs for proof of key possession

Industry Specific Requirements I

- Choice of CA
  - Payment(!)
- Support all PKIX based products
  - DV / OV / EV, TLS / S/MIME
- Can’t assume issue is immediate
  - Brand validation
  - Additional criteria OV, EV, private label

Industry Specific Requirements II

- Need to support Local Registration Authority Model



- Enable CA to provide management tools
  - How many devices do I have with active certs?

- CA or LRA may supply private key information for some apps

Some Technical Points

- DNS CAA record already has hooks that might be one CA discovery scheme
- Don’t need to necessarily support every feature
  - Must not close options
  - Can add JSON slots as required
- Don’t assume that the transactions are signed by the key the server is registering

IPR Issues

- Some DV schemes are covered by patents
  - Approach must be sufficiently flexible