Challenges and Lessons Learned in deploying RFC6492, 8181 and 8183

Provisioning, Publication, ID key exchanges
Before we start...

• Thank you for RFC 6492, 8181 and 8183!

• At least 6 CA implementations, 1000+ instances

• At least 4 Publication Server implementations, 50+ instances
Before we start…

Parent CA

Child CA

Publication Server

RFC 8183 set up

RFC 6492 provisioning

RFC 8183 set up

RFC 8181 publication

Tim Bruijnzeels, IETF 115 London
Anything Missing?

After a few years of implementation and operational experience..

- Some things are missing
- Other things can be improved
- Urgency varies
General Protocol - Messages

• Interop issues because of loose Cert / CMS specs
• Replay protection can be improved
• Identity Key roll at scale (>1000 delegated child CAs)
• Signing Algorithm for messages roll?
General Protocol - Control

- Error messages
- Rate limiting
- Other?
Publication Protocol

- Server side content verification?
  - Types?
  - Syntax?
  - Consistency (manifest, crl, all objects?)
  - Consider the risk of server errors..
- Quota
- Server notifications? Re-sync?
Provisioning Protocol

- Resources safe to use?
  - When will my certificate with new resources be published?
  - When will a resource be removed?
  - Server notification push?

- Algorithm Agility? (RFC 6916)
  - Separate trees? How does a child know?

- Other?
**Requirements**

- Graceful protocol negotiation
- No flag day, but allow new / extended where supported
- Stay close to current protocol where possible
- One new version with many fixes?
- Or support incremental features?
- Other?
Proposal

• Write document and ask for adoption. Focus:
  • problem statement
  • requirements
  • priorities

• Explore solutions for most urgent issue(s): ID key rolls and possibly message replay

draft-timbru-sidrops-rpki-publication-v2-00 is not that document.