X.509 Certificates

JIM SCHAAD

DRAFT-IETF-COSE-X5091

Current State

- Attributes Defined
  - Bag – random collection of certs
  - Chain – ordered collection of certs
  - Thumbprint – hash of certificate
  - URL – pointer to certificate
- Defaults depend on structure
- Added duplicates for Static-Static ECDH

Open Issues

- Should we define an Extended Key Usage
  - Restrict certificates to just COSE usage
- Is there a need to transport any revocation information
  - CRLs, OCSP
- Any unusual validation text needed?
- Defines a COSE_CertHash structure
  - If we define something in Hash document should we reference it?
- URL attributes use CBOR uri type, should this just be text?

Open Issues

- Define something for COSE_Keys
  - Create a new key type?
    - No Private Keys
  - Place in parallel to existing key information
    - This is what JOSE does
    - Makes validation rules complicated
  - Only leaf key or have a bag/chain?
- Implementation Experience
- What did I miss?

Going Forward

- Implementation Experience
- Missing Security Considerations
- Early assignment of code points

- Recently raised question of CWT