Adding Hash-Based Signatures in PKIX

- HSS (draft-mcgrew-hash-sigs); XMSS and XMSS^MT (RFC 8391):
  - HBS is well-studied (1970s)
  - Secure against large-scale quantum computers
  - Small public keys
  - Fast signing and verification
  - Large signatures
  - (potentially large but) limited number of signatures
  - Stateful
Adding Hash-Based Signatures in PKIX

- Use Cases:
  - HSM signing
  - CA certificates
  - Code signing certificates

- Isn’t cms-hash-sig enough?
  - cms-hash-sig only defines HSS usage
  - x509-hash-sigs also defines XMSS & XMSS^MT
  - RFC 8410 and RFC 8419 are separate documents
Since draft-vangeeest-x509-hash-sigs-01

• Aligning with cms-hash-sig: Full TBSCertificate is signed rather than being pre-hashed and the digest signed
• Fix signature ASN.1 encoding: BIT STRING(OCTET STRING(sig_octets))

NOTE: Full message signing
  • For large messages a streaming API may be needed
  • HSMs may not like streaming APIs because it adds session state to APIs
Next

• Adoption?
• Comments?
• Already aligned with cms-hash-sig, also align document structure with RFC 8410?