draft-vangeest-x509-hash-sigs-01

D. Van Geest
ISARA Corporation

S. Fluhrer
Cisco Systems
Adding Hash-Based Signatures in PKIX

• Specifically HSS (draft-mcgrew-hash-sigs-13); XMSS and XMSS^MT (RFC 8391)

• Hash-based signatures:
  • Well-studied (1970s)
  • Secure against large-scale quantum computers

• HSS/XMSS(^MT):
  • Small private and public keys
  • Fast signing and verification
  • Large signatures
  • Stateful
  • (potentially large but) limited number of signatures
Use Cases in X.509

• End-entity 🙅‍♂️👇
  • Managing state is hard, failure to manage state securely -> signature reuse.
  • Limited # of signatures complicates key expiry, increasing # of signatures increases signature size

• CA certs in interactive protocols 🤕👇
  • HSM to manage state, more control over # of signatures
  • Okay option if you can live with signature size

• CA certs in non-interactive protocols, code signing certs 👍👍
  • HSM to manage state, more control over # of signatures
  • Signature size less of an issue
  • Ready to deploy now for long-lived certs (IoT, automotive)
Asking

• SECDISPATCH
  • Comments?
  • Send to LAMPS?

• LAMPS
  • Interest?
  • Comments?
  • Review?
  • Align with draft-ietf-lamps-cms-hash-sig