Recent X.509-Related Activities in the IETF

Third X.509 Day – Session 1

Russ Housley
9 May 2024

IETF LAMPS Working Group

- The PKIX Working Group has been closed for many years
  - PKIX stands for “Public Key Infrastructure using X.509”
- The LAMPS Working Group is responsible for maintenance of PKIX-related documents and S/MIME-related documents
  - LAMPS stands for “Limited Additional Mechanisms for PKIX and S/MIME”
- Some X.509-related documents have been recently finished and others are in the process of being updated
- This presentation focuses on activities since the Second ITU-T X.509 Day (9 May 2023)

IETF LAMPS Working Group – recently completed

- Revisit Internationalized Email Addresses in X.509 Certificates
  - Avoid possible U-Label to A-Label conversion in path validation
- Policy graph algorithm improvements during path validation
- Expand DNS Certification Authority Authorization (CAA) to cover Email Addresses
- Online Certificate Status Protocol (OCSP) Nonce size guidance
- X.509 Certificate Extension for 5G Network Function Types
- Lightweight profile of Certificate Management Protocol (CMP)
- Avoid revocation checks for short-lived X.509 certificates

IETF LAMPS Working Group – current work items

- Assign additional extended key usage values
- Certificate Management Protocol (CMPv3)
- Certificate Management Messages over CMS (CMCbis)
- Support for Post-Quantum Cryptography (PQC)
- Mechanisms for transition from traditional cryptography to PQC
  - Locating related certificates for same subject
  - Hybrid key establishment
  - Dual signatures (and possibly composite signatures)