Recent X.509-Related Activities in the IETF

Second X.509 Day – Session 1

Russ Housley

9 May 2023

IETF LAMPS Working Group – already accomplished

The PKIX Working Group has been closed for some time. Some updates have been published to the X.509 certificate documents produced by the PKIX Working, including:

- Internationalized Email Addresses in X.509 Certificates
- DNS Certification Authority Authorization (CAA) Resource Record
- Online Certificate Status Protocol (OCSP) Nonce Extension
- X.509 Certificate Extension for 5G Network Function Types
- Logotypes in X.509 Certificates (replaces RFCs 3709 and 6170)
- Lightweight profile of Certificate Management Protocol (CMP)

IETF LAMPS Working Group – current work items

Current work items:

- Specify the use of short-lived X.509 certificates (no revocation)
- The Certificate Management Protocol (CMPv3)
- Certification Authority Authorization (CAA) for Email Addresses
- Support for Post-Quantum Cryptography (PQC)
- Mechanisms for transition from traditional cryptography to PQC
  - Hybrid key establishment
  - Dual signatures