Plans for X.508, X.509, X.510 Recommendations

Jean-Paul Lemaire

ITU-T Q11/17 Rapporteur

ISO/IEC/JTC 1/SC 6/WG 10 Convenor

Recommendations of X.500 series related to security

ITU-T Recommendation	Title	Date	ISO/IEC reference
X.508	Information technology - Open Systems Interconnection - The Directory: Public-key infrastructure: Establishment and maintenance	Planned for Sep. 2024	ISO/IEC 9594-12
X.509	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks Amendment 1	Oct. 2019 Planned for Sep. 2024	ISO/IEC 9594-8
X.510	Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations Amendment 1	Aug. 2020 Planned for Sep. 2024	ISO/IEC 9594-11

New ITU-T Recommendation X.508 (1)

(text common with ISO/IEC 9594-12)

Public-key infrastructure: Establishment and maintenance

- Introduction to cryptographic algorithms:
  - Symmetric key algorithms.
  - Hash algorithms.
  - RSA public key encryption algorithm.
  - Public key and digital signature algorithms (RSA, DSA and ECDSA).
  - Key establishment algorithms.
  - Authenticated encryption with associated data algorithms.
  - integrity check value algorithms.

New ITU-T Recommendation X.508 (2)

(text common with ISO/IEC 9594-12)

Public-key infrastructure: Establishment and maintenance

- Post-quantum cryptography: three key establishment algorithms are candidates:
  - BIKE: bit flipping key encapsulation
  - Classic McEliece
  - HQC: Hamming quasi-cyclic
- Hardware security modules (HSM): these modules are defined in ISO/IEC 19790 standard and are fully contained solutions for cryptographic processing, key generation, and key usage. Cryptographic information keys can not be extracted or removed from HSMs.

New ITU-T Recommendation X.508 (3)

(text common with ISO/IEC 9594-12)

Public-key infrastructure: Establishment and maintenance

- Public-key certificate content and extensions.
- Trust establishment.
- PKI in machine-to-machine environment using two PKIs:
  - A management PKI.
  - An operational PKI for M2M operations with private key and trust anchor information in a secure storage like hardware security module.
- PKI configuration.
- Annex about mathematics behind cryptographic algorithms.

Current and future activities
on ITU-T Recommendation X.509
(text common with ISO/IEC 9594-8)

- Usage of Authority and Validation lists for IoT devices which have limited capacity.
- Usage of quantum safe algorithms. A migration mechanism using specific extensions has already been added to the last Edition of X.509 Recommendation.
- Split ITU-T X.509 to separate Public Key Infrastructure and Privilege Management infrastructure used for access control.

Current and future activities common to X.508, X.509 and X.510 related to ASN.1 modules

- The cybersecurity recommendations (X.508, X.509 and X.510) belong to the X.500 series (directory) and the ASN.1 modules imports definitions from other parts of X.500 series recommendations often related to directory service.
- The plan is to reorganize ASN.1 definitions to have three categories of module:
  - Modules common to Directory Service and Cybersecurity (example: UsefulDefinitions)
  - Modules dedicated to Directory Service
  - Modules dedicated to Cybersecurity

Relations between X.508, X.509 and X.510 Recommendations