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

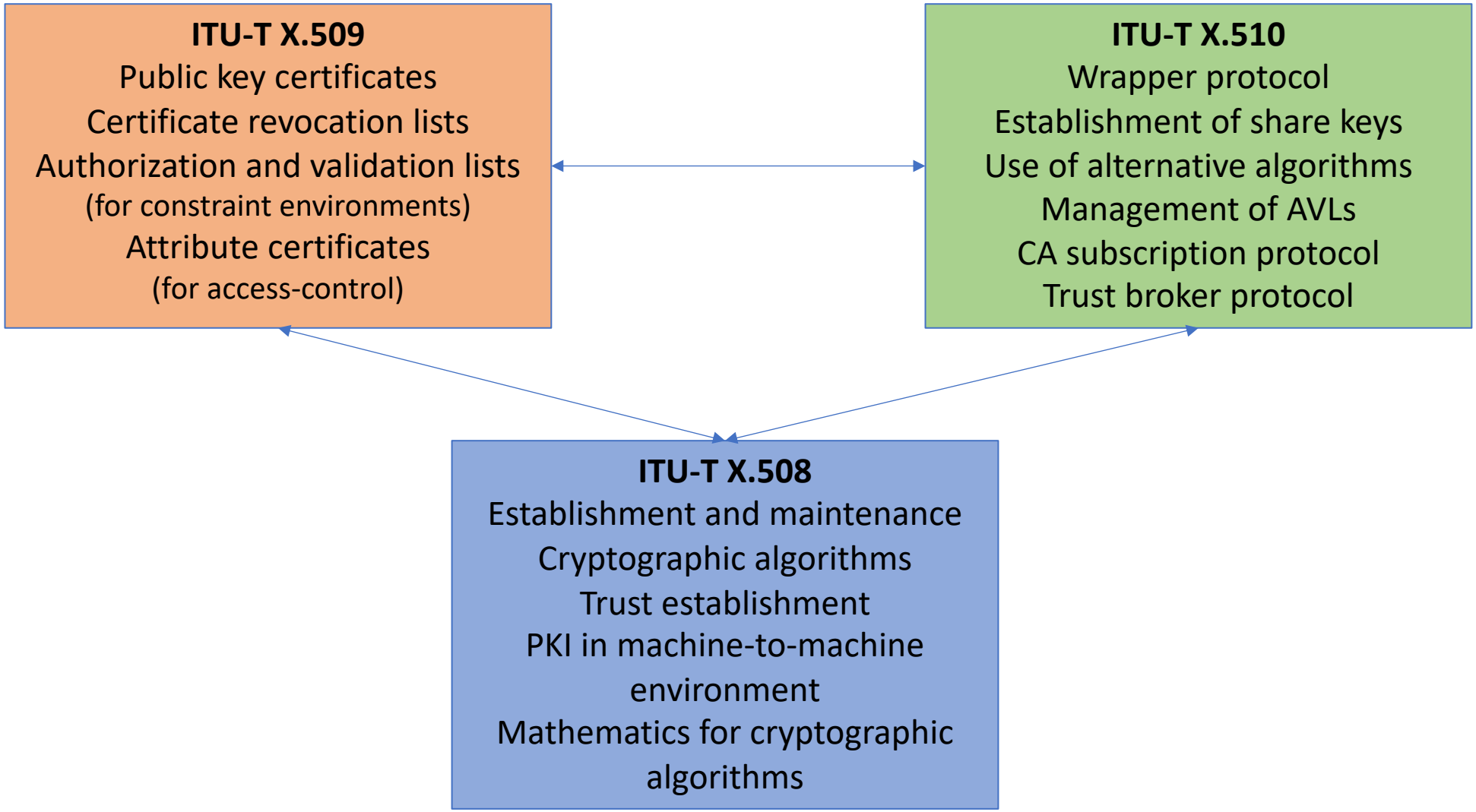
ITU-T Recommendation	Title	Date	ISO/IEC reference
X.508	Information technology - Open Systems Interconnection - The Directory: Public-key infrastructure: Establishment and maintenance	Planned for Sep. 2023	ISO/IEC 9594-12
X.509	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	Oct. 2019	ISO/IEC 9594-8
X.510	Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations	Aug. 2020	ISO/IEC 9594-11

New ITU-T Recommendation X.508 (1)
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.
- Post-quantum cryptography.

New ITU-T Recommendation X.508 (2)
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.


ITU-T X.509
Public key certificates
Certificate revocation lists
Authorization and validation lists
(for constraint environments)
Attribute certificates
(for access-control)
ITU-T X.510
Wrapper protocol
Establishment of share keys
Use of alternative algorithms
Management of AVLs
CA subscription protocol
Trust broker protocol
ITU-T X.508
Establishment and maintenance
Cryptographic algorithms
Trust establishment
PKI in machine-to-machine environment
Mathematics for cryptographic algorithms

Current and future activities
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 definition from other parts of X.500 series recommendations.
- ASN.1 definitions imported from cybersecurity modules will be moved to the "UsefulDefinitions" module.
- The "AuthenticationFramework", "CertificateExtensions", "AttributeCertificateDefinitions" and "UsefulDefinitions" module will be used by cybersecurity recommendations and directory recommendations.

Current and future activities
Other possible extensions

- Usage of Authority and Validation lists for IoT devices which have limited capacity.
- Usage of quantum safe algorithms.
- Split ITU-T X.509 to separate Public Key Infrastructure and Privilege Management infrastructure.