History of X.509

Jean-Paul Lemaire

ITU-T Q11/17 Rapporteur

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

The nine Editions of X.509

ITU-T Rec. X.509 is currently at Edition 9. This standard has been developed with ISO/IEC/JTC 1/SC 6 (ISO/IEC 9594-8)

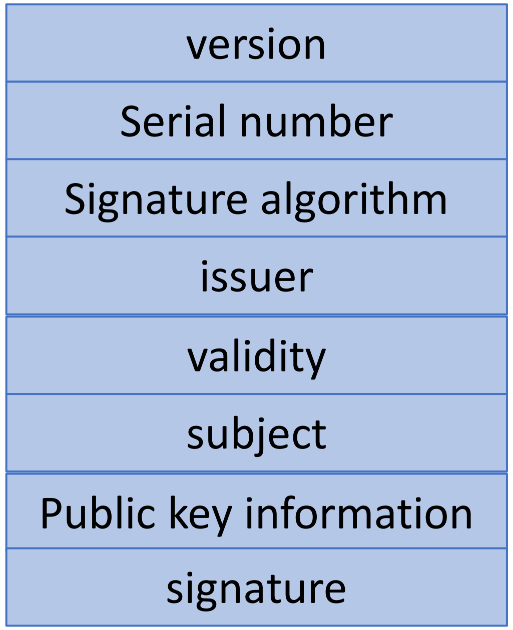
Edition	Title	Date	Study Group
1	The Directory: Authentication framework	1988-11-25	7
2	The Directory: Authentication framework	1993-11-16	7
3	The Directory: Authentication framework	1997-08-09	7
4	The Directory: Public-key and attribute certificate frameworks	2000-03-31	7
5	The Directory: Public-key and attribute certificate frameworks	2005-08-29	17
6	The Directory: Public-key and attribute certificate frameworks	2008-11-13	17
7	The Directory: Public-key and attribute certificate frameworks	2012-10-14	17
8	The Directory: Public-key and attribute certificate frameworks	2016-10-14	17
9	The Directory: Public-key and attribute certificate frameworks	2019-10-14	17

Edition 1 (1988) of X.509

- This first edition defines two methods of authentication:
  - Simple authentication with directory distinguished name and password with two options :
    - Unprotected simple authentication (password transmitted in clear text)
    - Protected simple authentication (password used by a function but not transmitted)
  - Strong authentication using asymmetric cryptography with three options (one-way, two-way and three-way authentication)
- This edition also defines the basis of strong authentication :
  - Public key certificate
  - Certification path
  - Certificate Revocation List

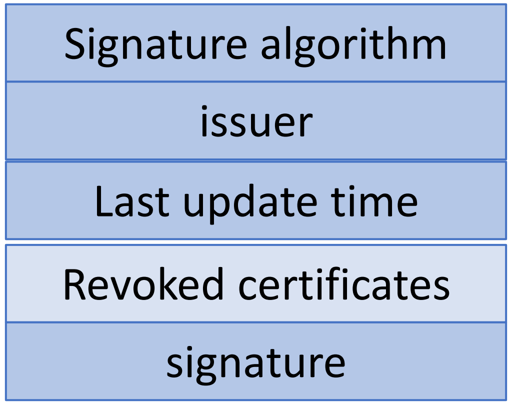
Certificate and Revocation list in edition 1

certificate structure



- version
- Serial number
- Signature algorithm
- issuer
- validity
- subject
- Public key information
- signature

certificate revocation list structure



- Signature algorithm
- issuer
- Last update time
- Revoked certificates
- signature

Edition 2 (1993) of X.509

- Second edition introduces some enhancements to certificate. Two new optional components have been added :
  - issuerUniqueIdentifier
  - subjectUniqueIdentifier
- These components can be used to distinguish issuers or subjects using the same distinguishedName.

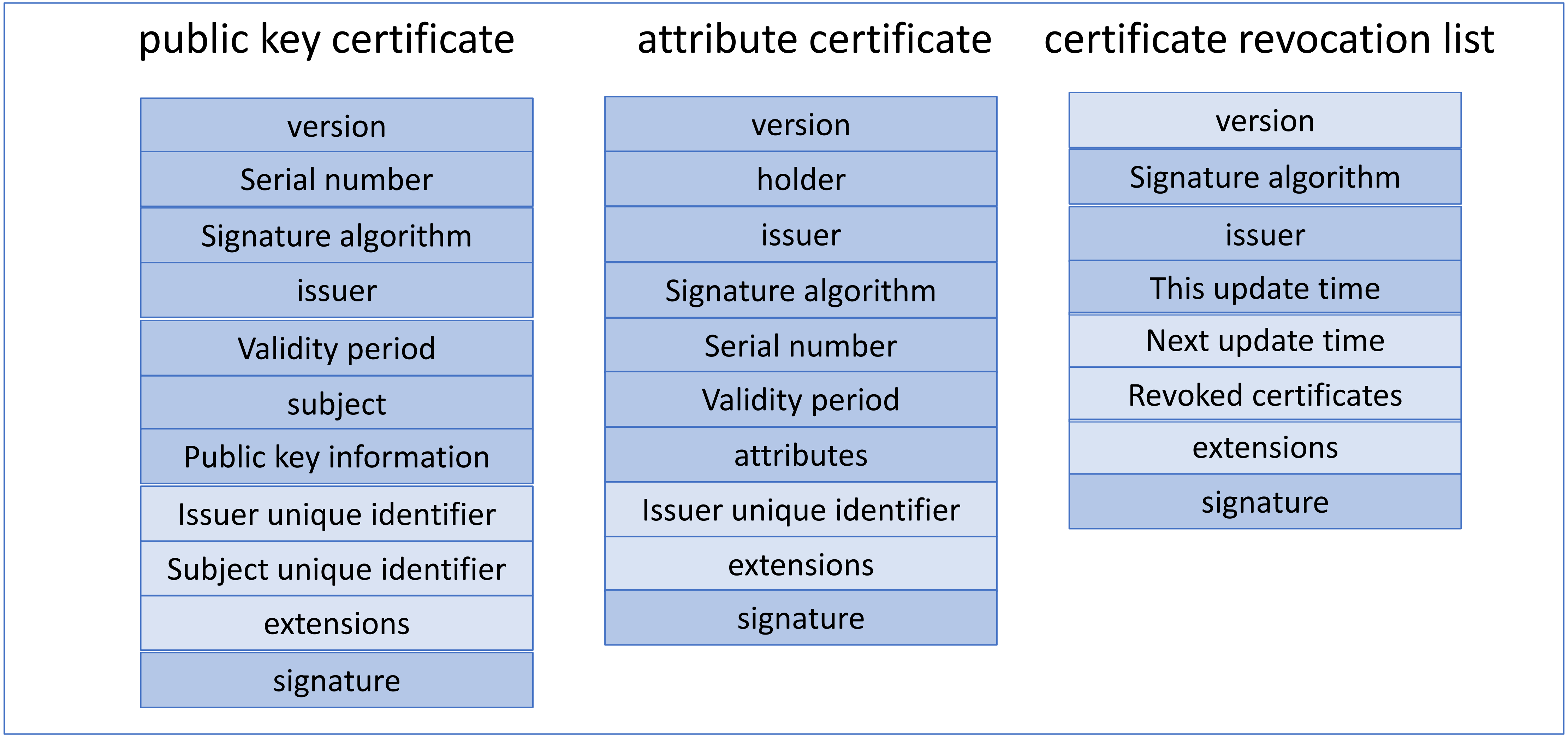
Edition 3 (1997) of X.509 (1)

- This edition has added several important enhancements to certificate and certificate revocation list:
  - Extension : the extension mechanism allows addition of new fields to certificate and certificate revocation list. Each extension is defined by a unique object identifier and contains a critical flag which specifies if the extension can be ignored or not by a receiver which does not recognize it. Some extensions are defined in X.509, others can be defined by Certification Authorities.
  - Certificate revocation list distribution points: possibility to update automatically a revocation list from a Web site or a directory server.
  - Delta CRL: modification of an existing revocation list.

Edition 3 (1997) of X.509 (2)

- It is possible to use public certificates to give privileges to user by using subjectDirectoryAttributes extension or specific extensions. In that case, a public key certificate has to be changed whenever a privilege is added or removed.
- Third Edition of X.509 contains the concept of attribute certificate. An attribute certificate is a signed structure like a public key certificate which, instead of public key, contains a list of privileges or roles (a role is a list of privileges defined in a specific attribute certificate which can be assigned globally to a user). Attribute certificates are created by specific authorities (Attribute authorities) and can be revoked with attribute certificate revocation lists.

Certificates and Revocation list in edition 3



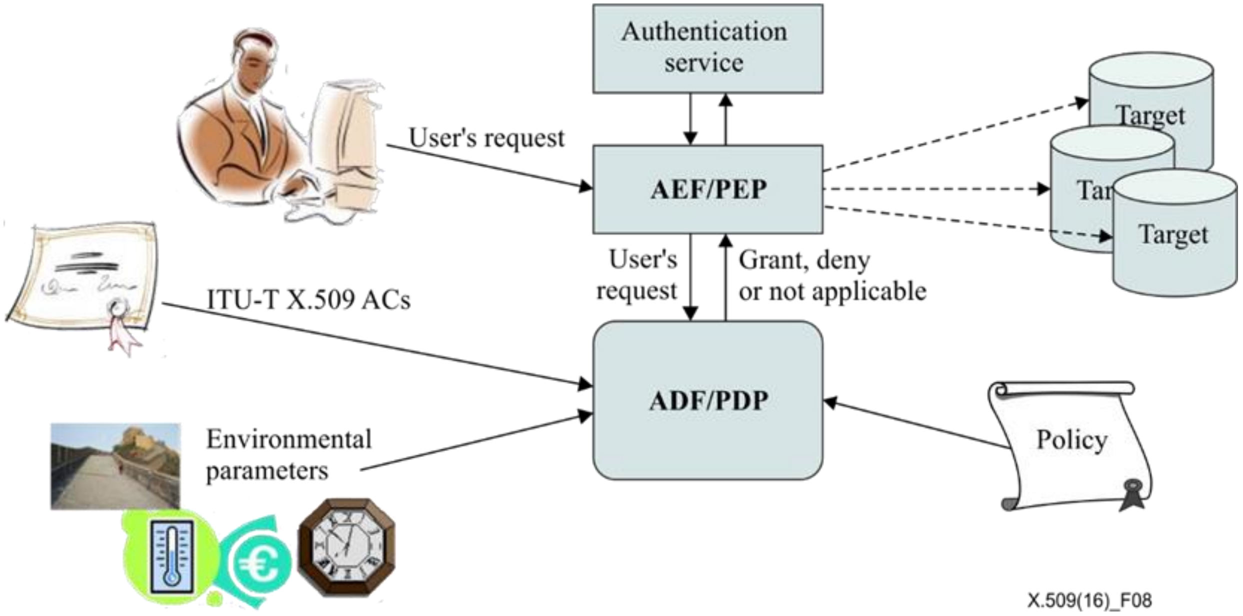
public key certificate	attribute certificate	certificate revocation list
version	version	version
Serial number	holder	Signature algorithm
Signature algorithm	issuer	issuer
issuer	Signature algorithm	This update time
Validity period	Serial number	Next update time
subject	Validity period	Revoked certificates
Public key information	attributes	extensions
Issuer unique identifier	Issuer unique identifier	signature
Subject unique identifier	extensions	
extensions	signature	
signature		

Editions 4 (2000) and 5 (2005) of X.509

- Since X.509 is used in many applications not related to directory, the title has been changed to “The Directory: Public-key and attribute certificate frameworks”.
- This edition adds :
  - several PMI models.
  - Specific extensions to attribute certificates like timeSpecification which restricts privileges to specified time periods.

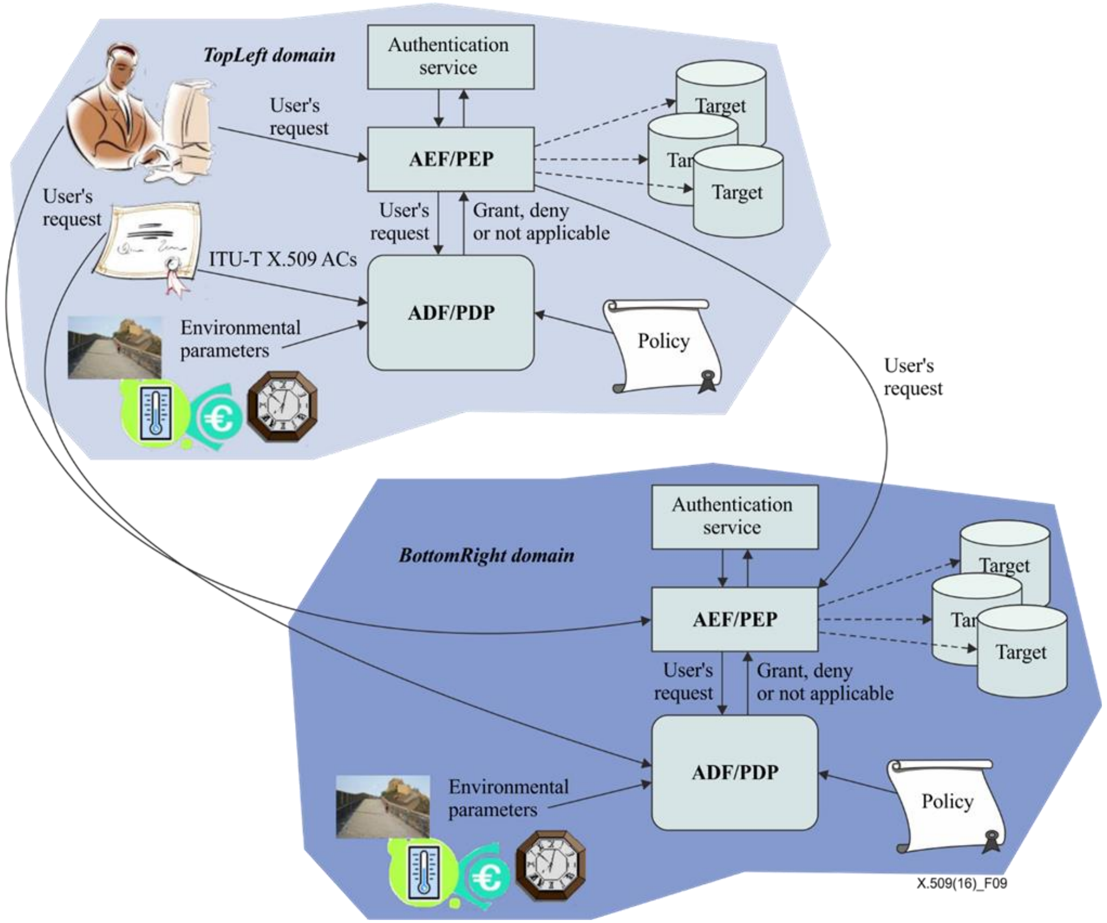
Editions 6 (2008) and 7 (2012) of X.509 (1)

- This Edition extends the Privilege Management Infrastructure with federated PMI models. This Edition introduce concepts of:
  - Policy Decision Point (PDP), equivalent to ADF (Access Control Decision Point)
  - Policy Enforcement Point (PEP), equivalent to AEF (Access Control Enforcement Point)



Editions 6 (2008) and 7 (2012) of X.509 (2)

- It is possible to connect PMIs so that attribute certificates issued in one domain can be used to gain access to resources in another domain. This can be done:
  - Statically by adding information in domain policy
  - Dynamically with specific attribute certificates (policy attribute certificates)

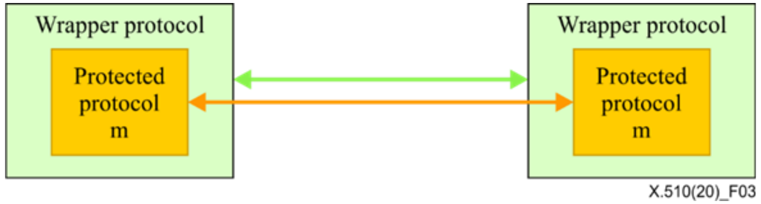


Edition 8 (2016) of X.509 (1)

- The directory authentication part has been moved to other parts of X.500 series.
- This edition:
  - Adds the concept of trust broker: trust broker, a third party trusted by relying parties to provide information about public-key certificates. Trust brokers are independent of certification authorities and have direct trust relationships with relying parties.
  - Adds the concept of authorization and validation lists: AVLs optimize certificate validation in some constraint environments (constraints on memory or communications). It is particularly useful in smart grid where validation time is constrained.
  - Contains a new section (Communication capabilities).

Edition 8 (2016) of X.509 (2)

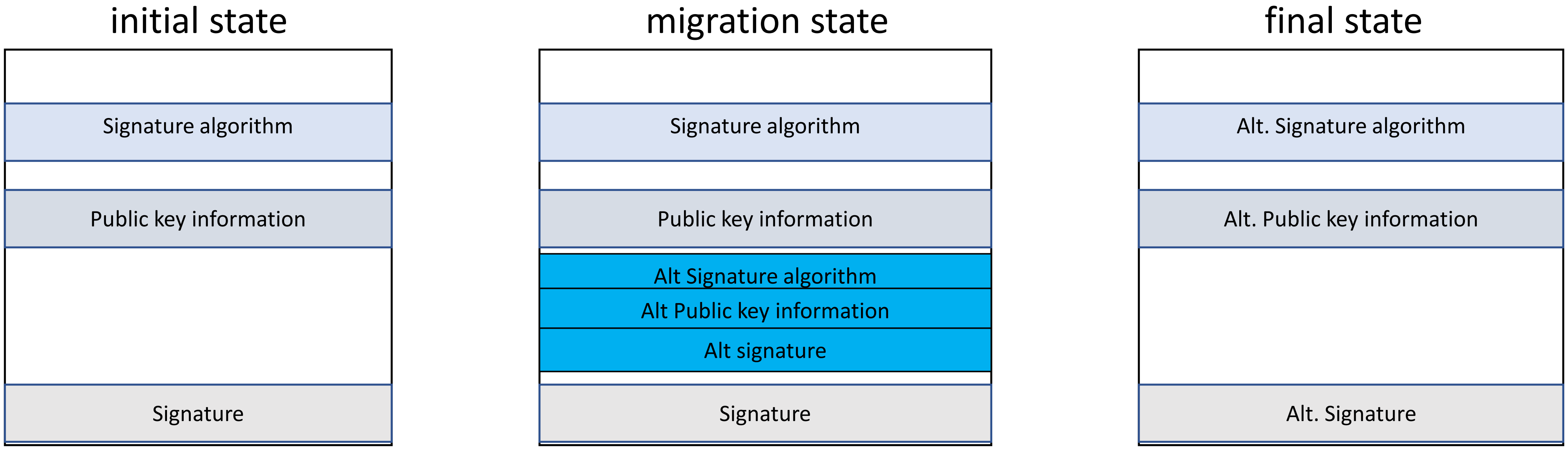
- The wrapper protocol has been defined to protect various protocols which have no security capabilities by embedding them.



- Edition 8 of X.509 defines the following protocols :
  - Authorization and validation management protocol (AVMP): this protocol is used between an authorizer and an AVL entity.
  - Certification authority subscription protocol (CASP): this protocol is used between an authorizer and a CA to subscribe to public key certificate status.
  - Trust broker protocol is used between a relying party and a trust broker.

Edition 9 (2019) of X.509

- The section related to protocols has been moved to a new part of X.500 series, X.510: Protocol specifications for secure operations.
- New extensions have been added to migrate to quantum safe algorithms.



initial state

Signature algorithm

Public key information

Signature

migration state

Signature algorithm

Public key information

Alt Signature algorithm

Alt Public key information

Alt signature

Signature

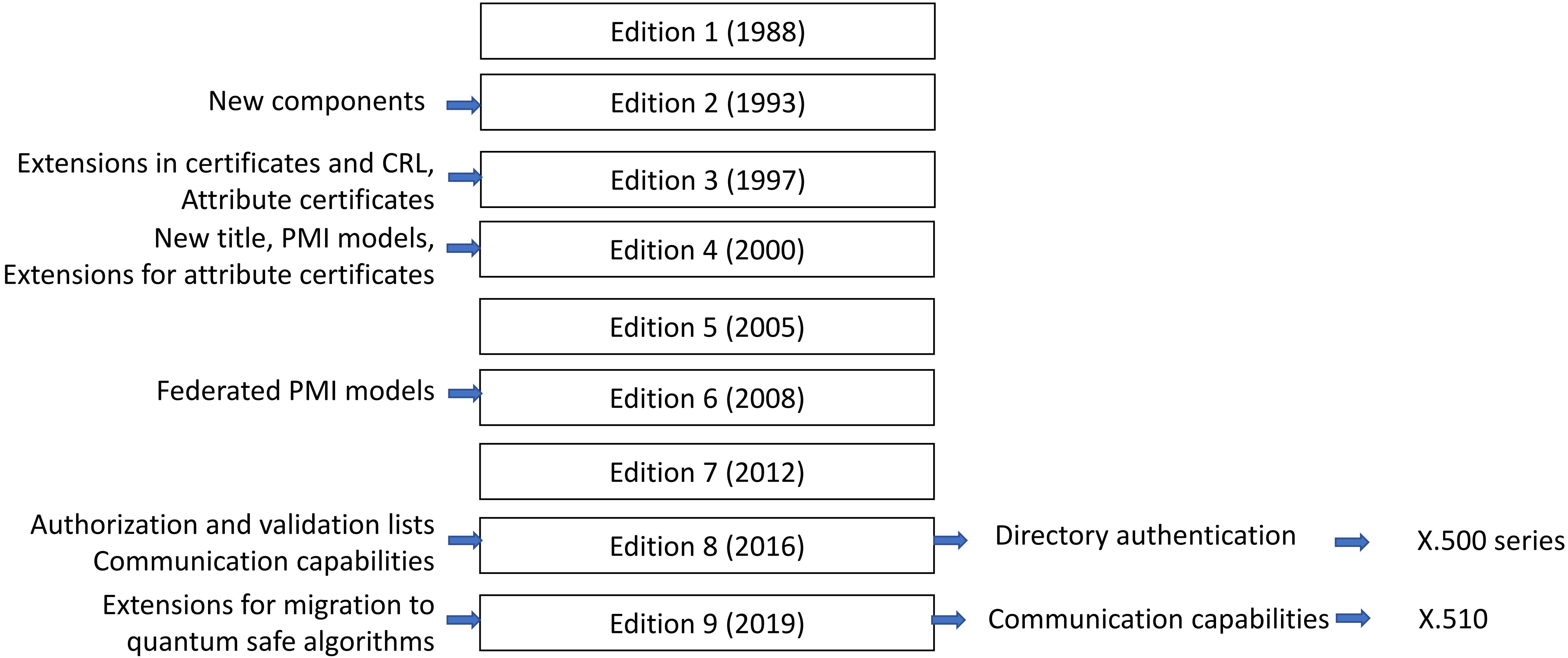
final state

Alt. Signature algorithm

Alt. Public key information

Alt. Signature

Summary



Edition 1 (1988)

New components → Edition 2 (1993)

Extensions in certificates and CRL,
Attribute certificates → Edition 3 (1997)

New title, PMI models,
Extensions for attribute certificates → Edition 4 (2000)

Edition 5 (2005)

Federated PMI models → Edition 6 (2008)

Edition 7 (2012)

Authorization and validation lists
Communication capabilities → Edition 8 (2016) → Directory authentication → X.500 series

Extensions for migration to
quantum safe algorithms → Edition 9 (2019) → Communication capabilities → X.510