



Status and plans for

ITU-T X.508 | ISO/IEC 9594-12

ITU-T X.510 | ISO/IEC 9594-11

Erik Andersen

era@x500.eu









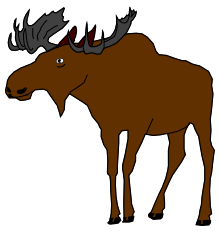
ITU-T X.508 | ISO/IEC 9594-12

WHAT MAY COME



Purpose and content

-  **To supplement ITU-T X.509 | ISO/IEC 9594-8 and ITU-T X.510 | ISO/IEC 9594-11**
 -  **Description of cryptographic algorithms**
 -  **Best practice for establishing a public-key infrastructure (PKI)**
 -  **Some mathematics behind cryptographic algorithm**
-



Status



The first edition has been out for Draft International Standard (DIS) vote within ISO/IEC JTC 1



A second DIS vote ongoing ending 17 June 2024



After completion of second DIS ballot and ballot comments resolution, approval (consent) within ITU-T Study Group 17 at the meeting 2-6 September 2024



After a last call within ITU-T Study Group 17, final editorial review by ITU-T editing team and then publication within ITU-T



FDIS vote within ISO/IEC JTC 1 and then publication within ISO



Already referenced in IEC 62351-9



Motivation for cryptographic algorithm



Description of cryptographic algorithms are spread over many document and detailed to a level for implementation



Recognized sources:



IETF RFCs



NIST specifications



ISO/IEC JTC 1/SC 27 WG 2



To have a collection in a single document



To have a more tutorial description that does not require high level of mathematical skill



References to more detailed descriptions



Scope of cryptographic algorithm description



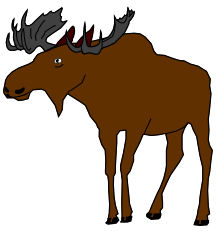
Quantum-safe cryptographic algorithms not included with few exceptions



Would delay the publication of a first edition



Work on a second edition will start when first edition completed



Motivation for annex on mathematical concept



Most descriptions assume that readers have a basic understanding of some mathematical concepts



Only mathematic models used for defining currently used cryptographic algorithms



Some quantum-safe algorithms are based on mathematical models not yet included



Planned to be included in next edition



ITU-T X.510 | ISO/IEC 9594-11

WHAT MAY COME



Formal specifications of cryptographic algorithms

 ITU-T X.510 introduces a concept of pluck-in of cryptographic algorithms in communication protocol

 Requires that formal specifications of algorithms are as specified by ITU-T X.509 and explained in detail in ITU-T X.510.

 If not specified correctly, algorithms must be redefined preferable without changing the object identifier

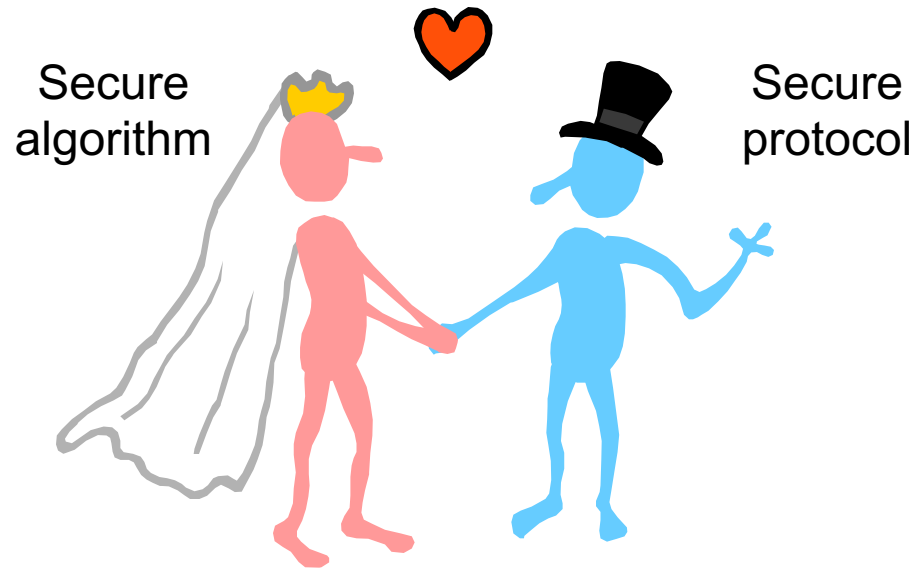
 Current ITU-T X.510 has already many redefined formal specifications

 **Many redefinition will be needed in the future**



X.510 has tools and guidance on techniques for protocol migration to new cryptographic algorithms





END
