

# Consideration on future use of ITU-T X.509

Second ITU-T X.509 day

Erik Andersen

9 May 2023

# Stepping stone to cope with quantum supremacy?



Quantum safe algorithm development



Produce of algorithm standard by ISO/IEC SC 27, NIST or IETF to be used as normative reference



Inclusion of algorithm in protocol standards



Development of products



Deployment in the field


## Protection constrained devices (IOTs)?

 IOT devices in communication networks in large quantities

 “The good guys get weaker – the bad guys get stronger”

 Large public keys and signatures and heavy processing

 How to off-load?

 Further development of the authorization and validation lists (AVLs)?

## Attribute certificates as part of PKI



Attribute certificates important for access control



Identity assurance using public-key certificates also important for access control



Attribute certificates seen as (temporary) extensions to public-key certificates



Reorganizing ITU-T X.509 to make attribute certificates part of PKI



Attribute certificate may not be issued by the same authorities as public-key certificates