



X.509

Rec. ITU-T X.509
vs.
constrained devices

Erik Andersen

Andersen's L-Service consultancy
Project editor for X.509 (+ much more)

era@x500.eu



A little X.509 history



First edition of X.509 was issued 1988

*

*



Ninth edition of X.509 was issued 2019



New editions planned



X.509 being the framework for public-key infrastructure (PKI) is one of the most important security standards

**It is part of the ITU-T X.500 series of Recommendations
Also issued as ISO/IEC 9594-8**

Security foundation for:

-  **E-banking**
 -  **E-government**
 -  **E-health**
 -  **Etc.**
-



Done deal?

It is out there. It is working. Thousands of working systems out there.



It is a done deal!

or is it?



Challenge

Two opposite trends:



Computers get faster - especially future quantum computers



Devices get smaller and numerous



Constrained on processing power



Battery driven



Storage constraint



Stringent response requirements




Etc.

The bad guys get stronger

The good guys get weaker with large attack surface



General challenges

-  **Requirement for lightweight, but strong cryptographic algorithms**
 -  **Lean and secure communication protocols**
 -  **Scalable specifications**
 -  **Adapting PKI to the new environment**
-



Basic principle



PKI puts several requirements on participating entities



Offload some of these requirements to a stronger entity for constrained entities



Facilitating using authorization and validation lists (AVLs) – An advanced whitelist



Two modes of operation



Environments without resource constraints



Environments with resource constraints:



Storage constrained



Processing constrained



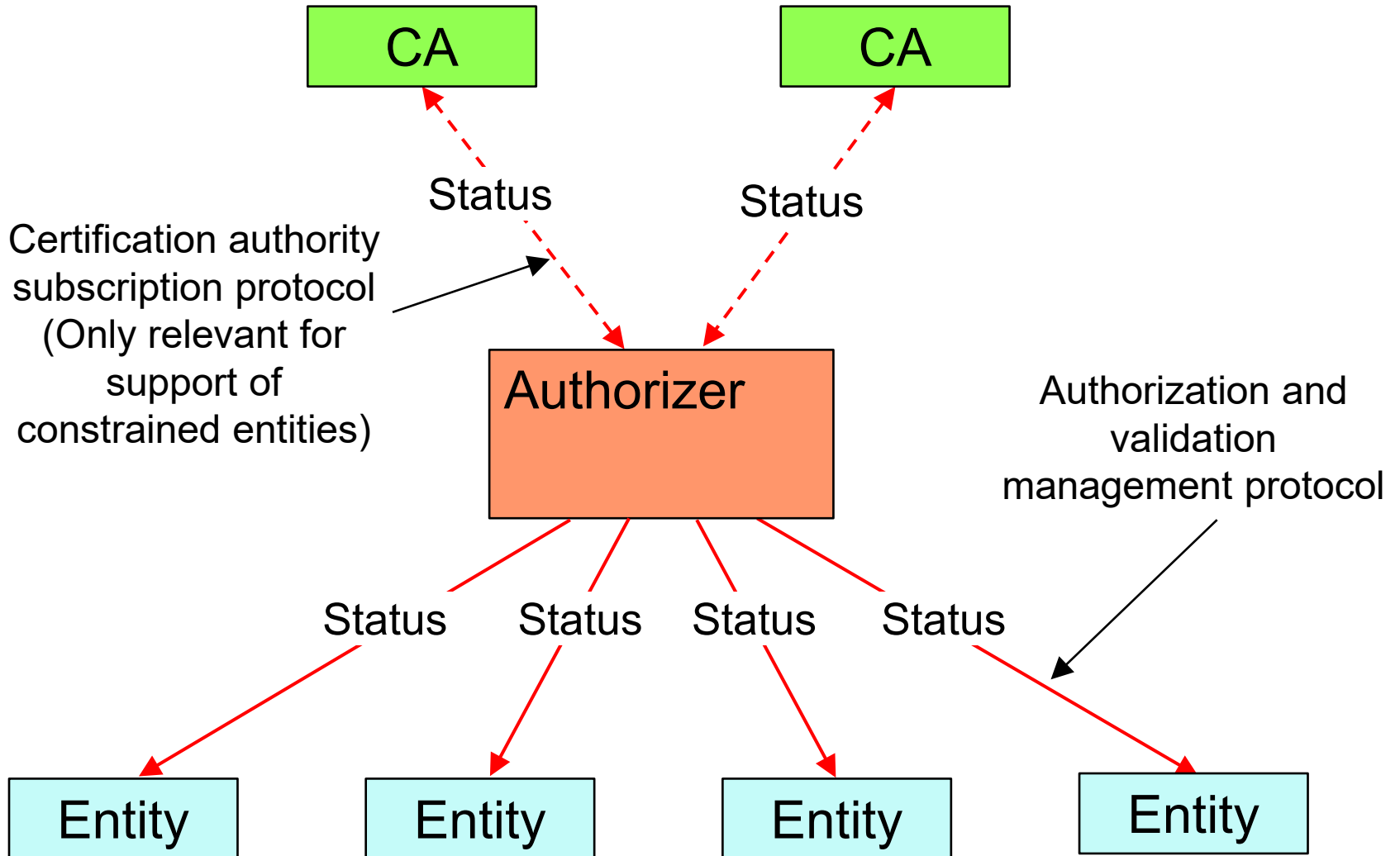
Limited bandwidth



Time requirements, e.g., 1 ms validation time

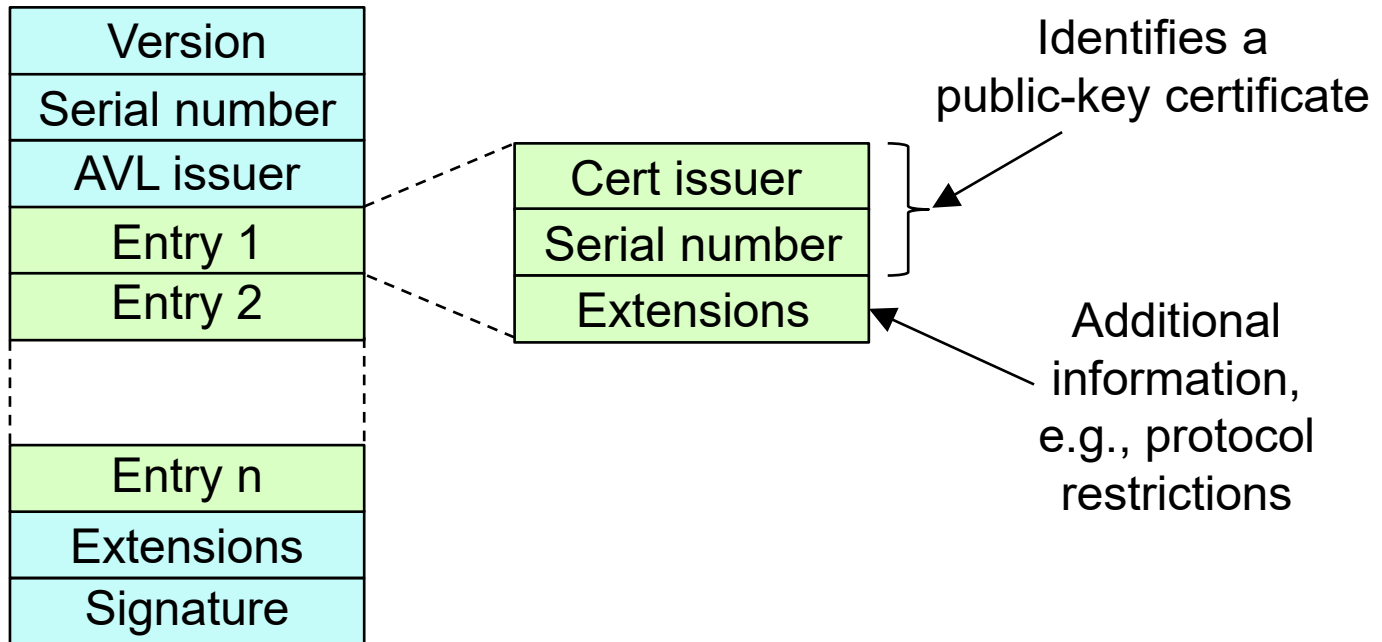


Authorizer relationships





Authorization and validation list (AVL) simplified





AVL general handling



If a certificate related to an incoming message is not reflected in the AVL, the message is rejected



When protocol restriction is imposed, the message is rejected if the used protocol is not listed in the entry.



New restrictions may be added in the future



AVL specific handling for constrained entities



The authorizer maintains status of all certificates in the AVL

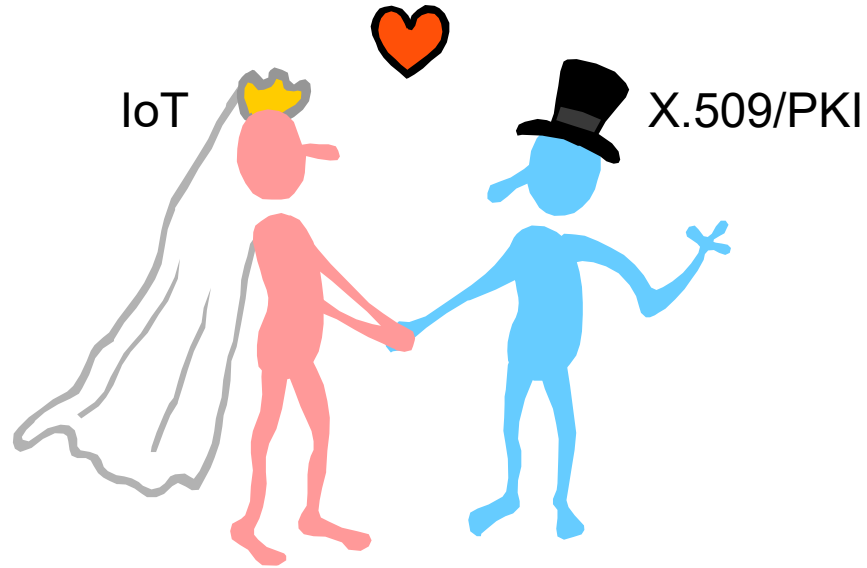


The authorizer updates the AVL whenever certificate status changes



If a certificate is reflected by the AVL, the entity may assume that the certificate is valid. No revocation checking needed

This is only the beginning!



END
