X.509 (2000): 4th edition:
Overview of PKI & PMI Frameworks

Sharon Boeyen

(X.509 Editor)

Senior Consultant, Advanced

X.509 scope

PKI framework

- Evolved over 4 editions of X.509
- Basic model has remained intact
- Certificate and CRL formats have been extended, but remain backward compatible
- Extensibility mechanism enables en5ln27 matto smpasfyrd application/business specific needs

Public-key certificate &

Additions to certificate format

v1 certificate	v2 certificate	v3 certificate

Additions to CRL format

v1 CRL **v2 CRL**

Certificate & CRL

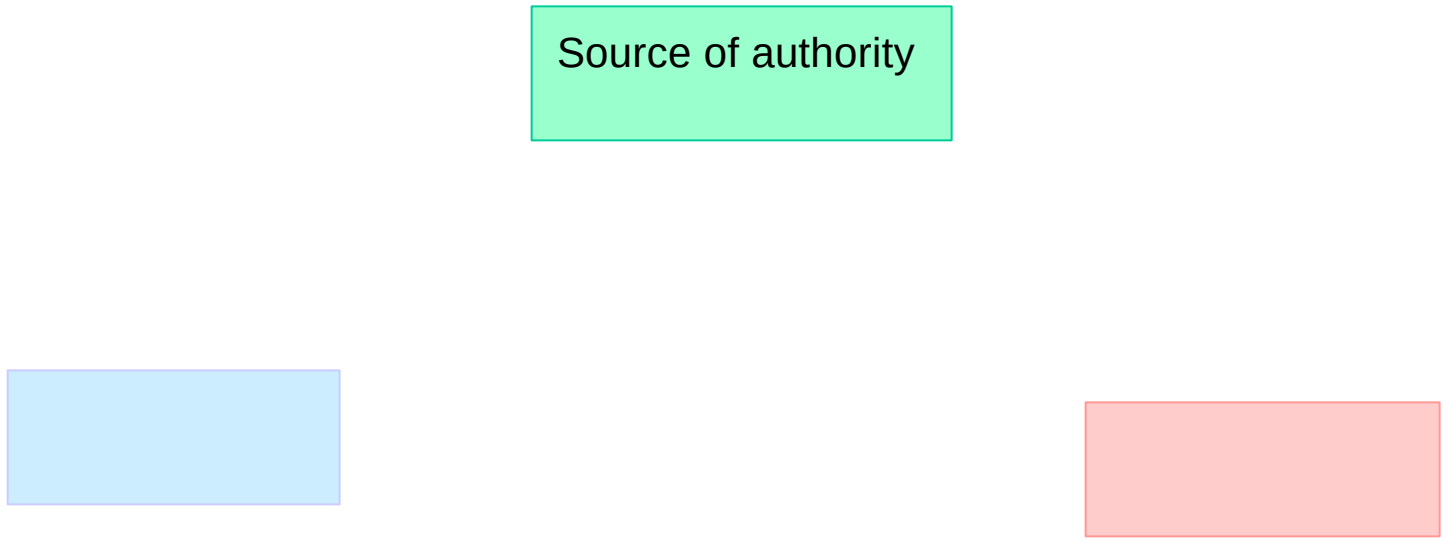
Why base PKI profiles on X.509 4th edition (2000)

-

PMI Framework

-

Basic PMI model



Attribute certificate syntax

-

Attribute certificate syntax

Basic syntax

version

PMI certificate extensions

-