USING X.509 TO BUILD CONFIDENCE IN THE USE OF ICTs

Jos Purvis

Cisco Systems – Cryptographic Services

CA/Browser Forum

ITU X.509 Day, May 2022

Cisco Systems

- Cryptographic Services Group
- Corporate TLS Standards

CA/Browser Forum

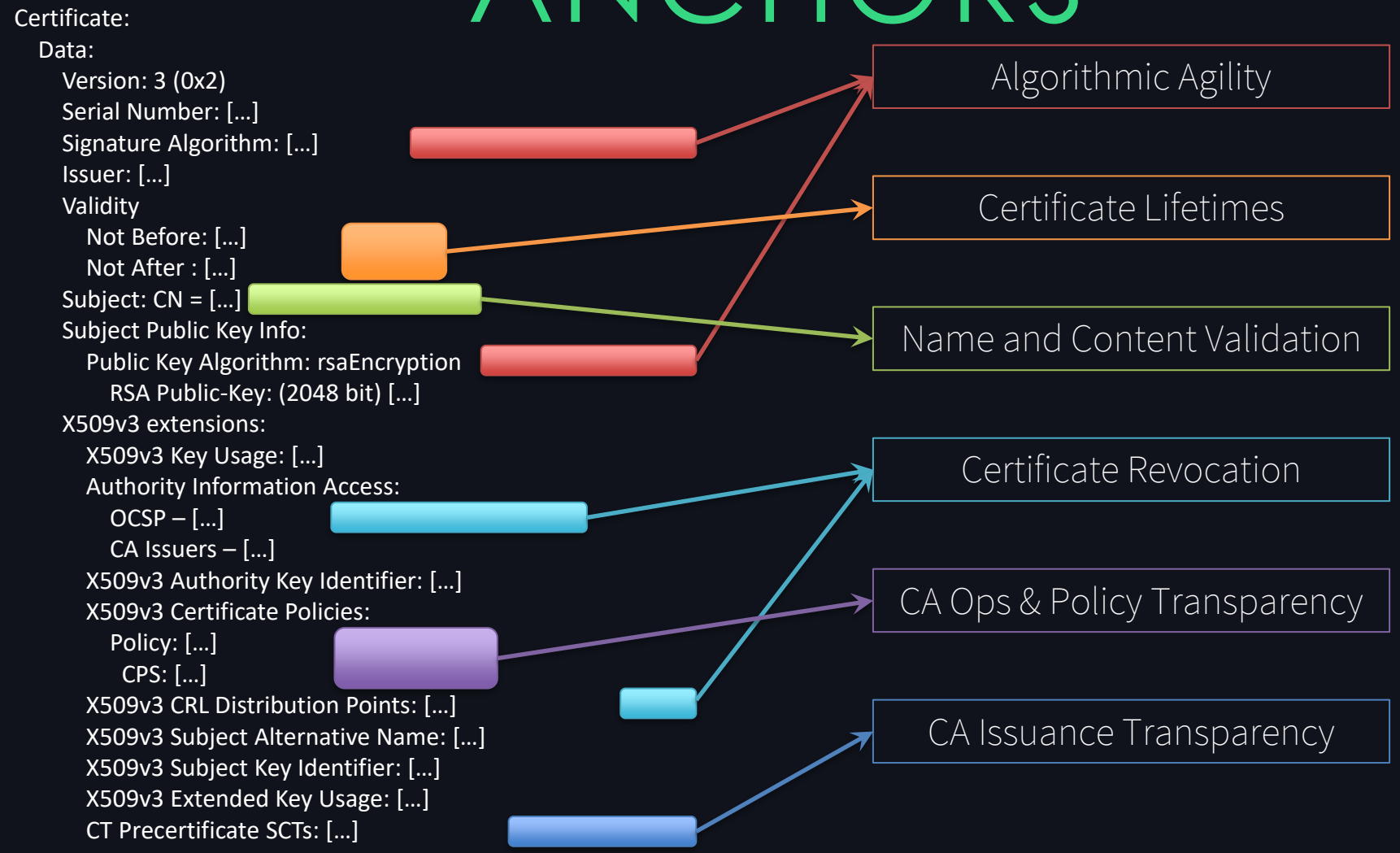
- Chair, Server Certificate (TLS) Working Group

Adjunct Faculty: UNC, NCSU, Boston Univ.

ABOUT JOS

(WHERE I'M COMING FROM)

X.509 TRUST ANCHORS



X.509 TRUST GROWTH

X.509 / PKI use is exploding

~~PKI is painful, manual, complicated~~

Modern PKI toolkits are
Simple,
Free,
Well understood & documented
Broadly supported

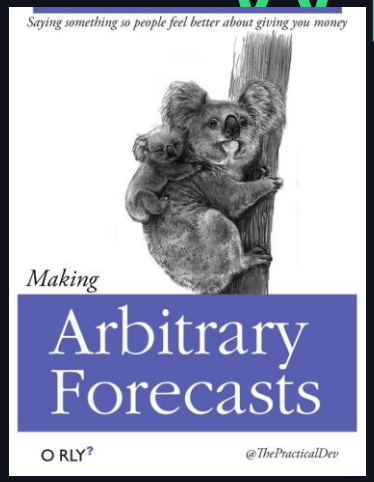
There are still pitfalls!

TLS
Web PKI
Service Encryption
mTLS and VPN

Device Identity
Hardware (802.1AR)
Manufacturer Certification
Cluster/Container (k8s)

Client Identity
NAC/802.1X
Zero Trust Frameworks
SAML/OAUTH

WHERE WE NEED TO GO



Ubiquity

- Automation is critical
- Flexible uses → Flexible rules
- IoT and Containerization
  - Resource consumption
  - Complexity

Agility

- Post-Quantum
  - New algorithm support
  - Hybrid certificates
- Legacy Issues
  - Supporting older clients
  - Cruft → Vulnerabilities
- New/Updated Protocols

Meaning

- X.509 Cert Validation
  - Complexity
  - Structure & Consistency
- What does a cert mean?
  - Software Signing
  - Device Identity

Coordination of Effort

- Structural Groups (IETF)
- Issuer Groups (CABF)
- PKI-Consumer Groups (eIDAS)

Leverage expertise
Define or be defined

Look further down the road
Deprecate faster & easier
BUT
Keep what's working
Beware Chesterton's Fence

COORDINATION

QUESTIONS?