Post-Quantum

Cryptography Conference

X9 Financial PKI: PQC Readiness and Crypto-Agility for Financial Services

Transitioning from legacy asymmetric algorithms to PQC algorithms also means upgrading your PKI and certificates, however the financial services industry has its own needs which no longer aligns with the CA/Browser Forum, the IETF, NIST, or other programs. Consequently, the Accredited Standards Committee (ASC) X9 Financial Services has launched the X9 Financial PKI as an alternative for PQC readiness and crypto-agility to banks, merchants, and third-party financial service providers. This session discusses the issues, the requirements, the technologies, the X9 Financial PKI program, and its first implementation using PQC enabled certificates.

Jeff Stapleton
Executive Director Cybersecurity Researcher at Wells Fargo

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity ("business league") under Utah law (10462204-0140) | pkic.org

PKI Consortium

X9 Financial PKI

PQC Readiness and Crypto-Agility for Financial Services

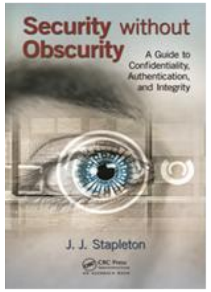
PKI Consortium: PQC Conference

January 2025

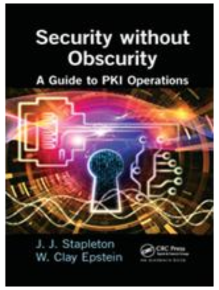
Jeff Stapleton – Executive Director Cybersecurity Researcher

Speaker Information

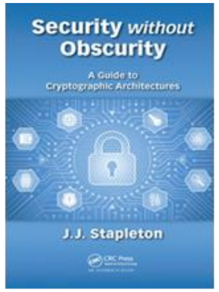
- **Jeff Stapleton jeff.Stapleton@wellsfargo.com**
- **X9F4 Cybersecurity and Cryptography workgroup chair (1998)**
- **ANSI X9 standards (1989)**
- **ISO TC68 standards (1994)**
- **ISSA Journal articles**
- **ISMH book chapters**
- **Security Without Obscurity**
- **Wells Fargo Patent Hall of Fame (2018)**
- **100th Wells Fargo Patent (2023)**


Security without Obscurity
A Guide to Confidentiality, Authentication, and Integrity
J. J. Stapleton
CRC Press

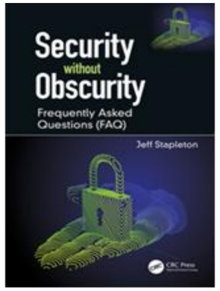
2014



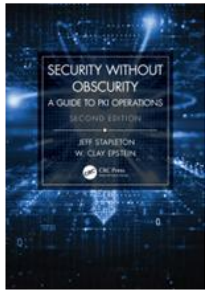
2016


Security without Obscurity
A Guide to Cryptographic Architectures
J.J. Stapleton
CRC Press

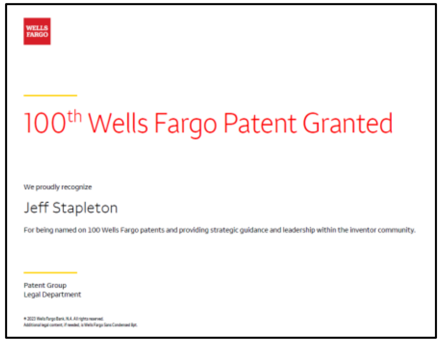
2019



2021



2024



WELLS FARGO

100th Wells Fargo Patent Granted

We proudly recognize

Jeff Stapleton

For being named on 100 Wells Fargo patents and providing strategic guidance and leadership within the inventor community.

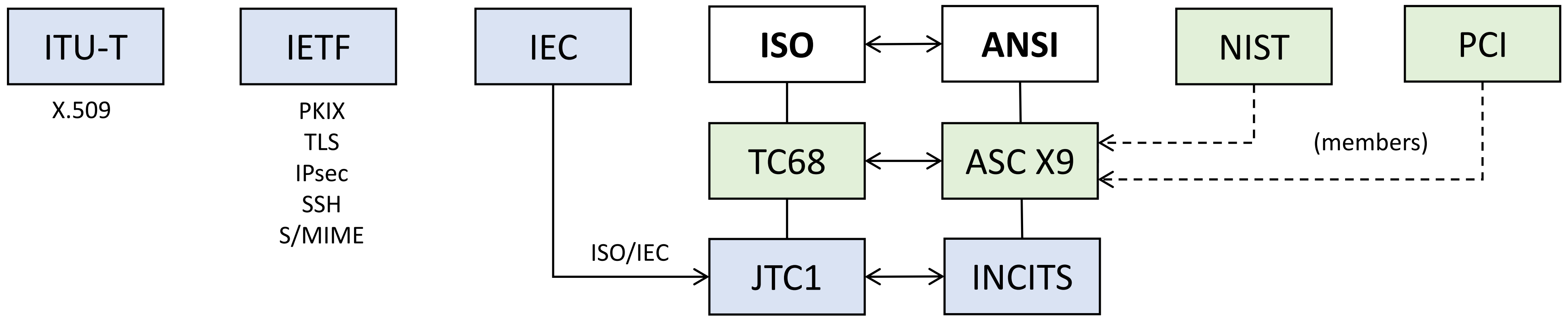
Patent Group
Legal Department

© 2023 Wells Fargo Bank, N.A. All rights reserved.
Additional legal content, if needed, is Wells Fargo Sans Condensed 8pt.

Agenda

- Industry Standards Organizations
- PKI Industry: abridged history
- X9 PKI Standards: abridged history
- X9 Financial PKI: abridged history
- X9 Financial PKI: architecture
- X9 Financial PKI: audit program
- X9 Financial PKI: summary
- Addendum: PKI Reference Material

Industry Standards Organizations



Information Technology

- International Telecommunications Union (ITU)
- International Electrotechnical Commission (IEC)
- Internet Engineering Task Force (IETF)
- ISO/IEC Joint Technical Committee One (JTC1)
- InterNational Committee for Information Technology Standards (INCITS)

Financial Services

- Technical Committee 68 Financial Services (TC68)
- Accredited Standards Committee (ASC) X9 Financial Services
- National Institute Standards and Technology (NIST)
- Payment Card Industry (PCI) Security Standards Council

PKI Industry: abridged history

- **PKI Forum** (2000 – 2003) merged into OASIS PKI standards (2003)
  - Public advocacy group promoting PKI technology and standards
  - Infamous “CA shootout” in Wash DC (2002) resulted in other industry initiatives
- **Webtrust CA** (2000 – current) auditing standard
  - Auditing standard version 1.0 based on ANSI X9.79 PKI standard
  - Auditing standard version 2.0 based on ISO 21188 PKI standard (a.k.a. X9.79)
- **CA Browser Forum** (2005 – current)
  - Founded by browser manufactures adopting Webtrust CA
  - Established the Extended Validation (EV) certificate criteria
- **EU** Qualified Trusted Service Providers (**QTSP**) ~2016
  - QTSP registered CA for the Payment Services Directive 2 (PSD2)
- **UK** Open Banking Implementation Entity (**OBIE**) ~2020
  - QTSP breakaway due to BREXIT

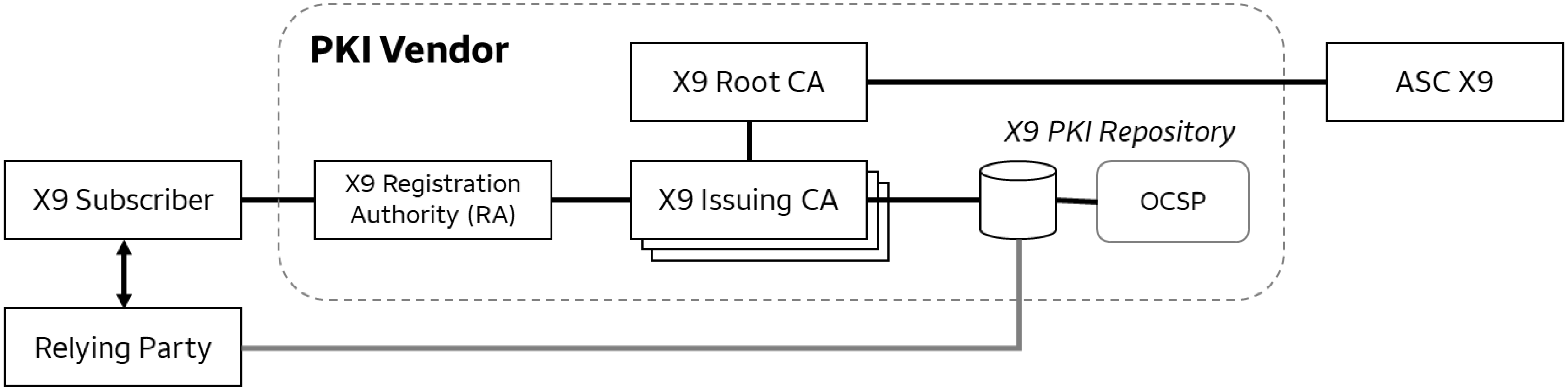
X9 PKI Standards: abridged history

- **X9.55 Certificate Extensions** (1997) published ANSI standard
  - USA submission to ISO TC68
- **X9.57 Certificate Management** (1997) published ANSI standard
  - USA submission to ISO TC68
- **ISO 15782 Certificate Management** (2001) published ISO standard
  - Merged X9.57 and X9.55
- **X9.79 PKI Policy and Practices** (2001) published ANSI standard
  - USA submission to ISO TC68
- **ISO 21188 PKI Policy and Practices** (2006) published ISO standard
  - Adopted X9.79
- **ISO 21188 PKI Policy and Practices** (2018) published ISO standard
  - Merged ISO 15782
- **ISO/IEC 27099 PKI Policy and Practices** (2022) published ISO/IEC standard
  - TC68 rejected JTC1 request to transfer ISO 21188 to JTC1/SC27

X9 Financial PKI: abridged history

- **2017**: ASC X9 established open forum X9F PKI study group
  - https://x9.org/x9f-public-key-infrastructure-pki-study-group/
- **2019**: X9F PKI study group reported to X9 Board of Directors
  - Phase 1: X9 Financial PKI Use-Cases 2019 v2.pdf (27)
- **2022**: PKI Certificate Policy (CP) completed
  - Phase 2: Final Release X9 CP v0 20230822.pdf
- **2024**: PKI Request for Proposal (RFP) for PQC-ready Root CA
  - Phase 3: ASC X9 Financial PKI https://x9pki.org/
    - Vendor selection completed – announcement forthcoming
    - Updating X9 PKI Use Cases (34)
- **2025**: X9 Financial PKI
  - Phase 4: UAT root CA (RCA) and issuing CA (ICA) for first PKI use-case
  - Phase 5: Production root CA (RCA) and issuing CA (ICA) for first PKI use-case

X9 Financial PKI: architecture



- X9 Financial PKI operated by third-party PKI service provider
  - Registration Authority (RA), Issuing CAs (ICA) and Root CA (RCA)
  - WebTrust for CA audit with X9 CP validation
- ASC X9 is the governing body for the X9 Financial PKI
  - Financial Services industry participants are the X9 Financial PKI customers

X9 Financial PKI: audit program

- Expand existing Webtrust for CA audit program
  1. Webtrust auditor validates the CA’s Certificate Practice Statement (CPS) against CA’s actual operations
  2. **Webtrust auditor (extra step) evaluates CPS against X9 Certificate Policy providing additional PKI requirements**
  3. Webtrust auditor provides annual audit report confirming compliance
- X9 reviews audit report
  - If approved: X9 certificates issued by CA for one or more PKI use cases
- Certificate subjects get X9 certificate from X9 Financial PKI
  - Private key usage: key management, digital signatures
- Certificate relying party recognizes X9 Financial PKI
  - Certificate validation: including revocation status

X9 Financial PKI: Summary

- X9 Financial PKI announced December 5, 2023 – https://x9pki.org/
- X9 Financial PKI bidders call held January 9, 2024
  - Eleven (11) vendors
- Bidders Q&A January – March 2024
- Evaluations April – May 2024
  - Three (3) vendors
- Notifications June 2024
- Agreements July – December 2024
- Next Steps January 2025

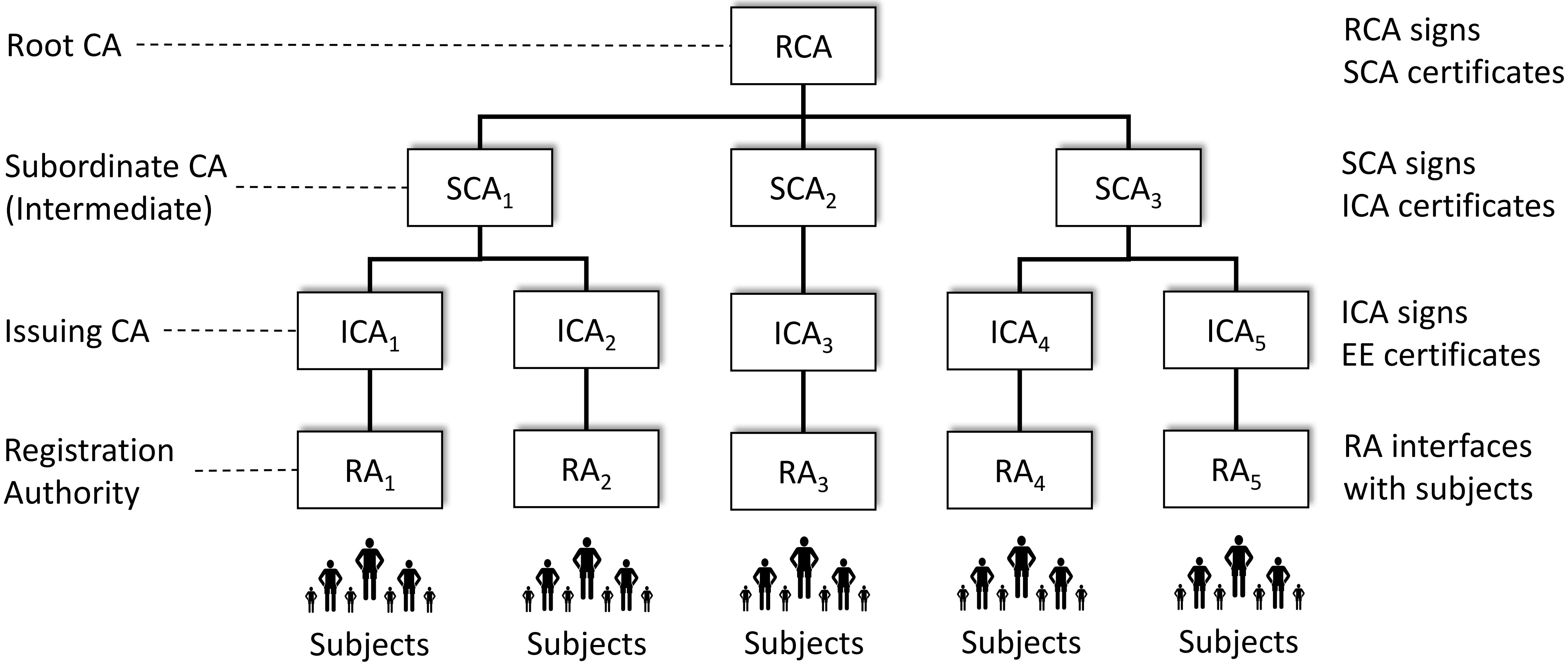
Accredited Standards Committee X9 Inc.
Financial Industry Standards

Addendum: Reference Material

Addendum: PKI Abbreviations and Acronyms

CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certificate Practice Statement
EE	End Entity
ICA	Issuing Certificate Authority
OCSP	Online Certificate Status Protocol
PA	Policy Authority
RA	Registration Authority
RCA	Root Certificate Authority
RP	Relying Party
SCA	Subordinate Certificate Authority

Addendum: example 3-Tier PKI



Root CA

RCA

RCA signs SCA certificates

Subordinate CA (Intermediate)

SCA$_1$ SCA$_2$ SCA$_3$

SCA signs ICA certificates

Issuing CA

ICA$_1$ ICA$_2$ ICA$_3$ ICA$_4$ ICA$_5$

ICA signs EE certificates

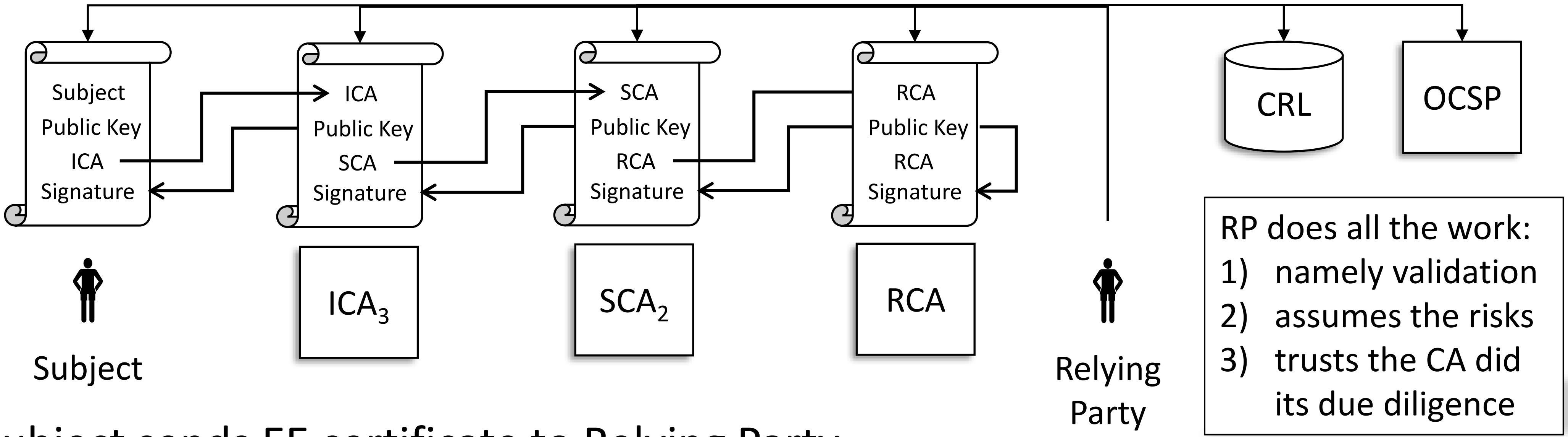
Registration Authority

RA$_1$ RA$_2$ RA$_3$ RA$_4$ RA$_5$

RA interfaces with subjects

Subjects Subjects Subjects Subjects Subjects

Addendum: Certificate Validation



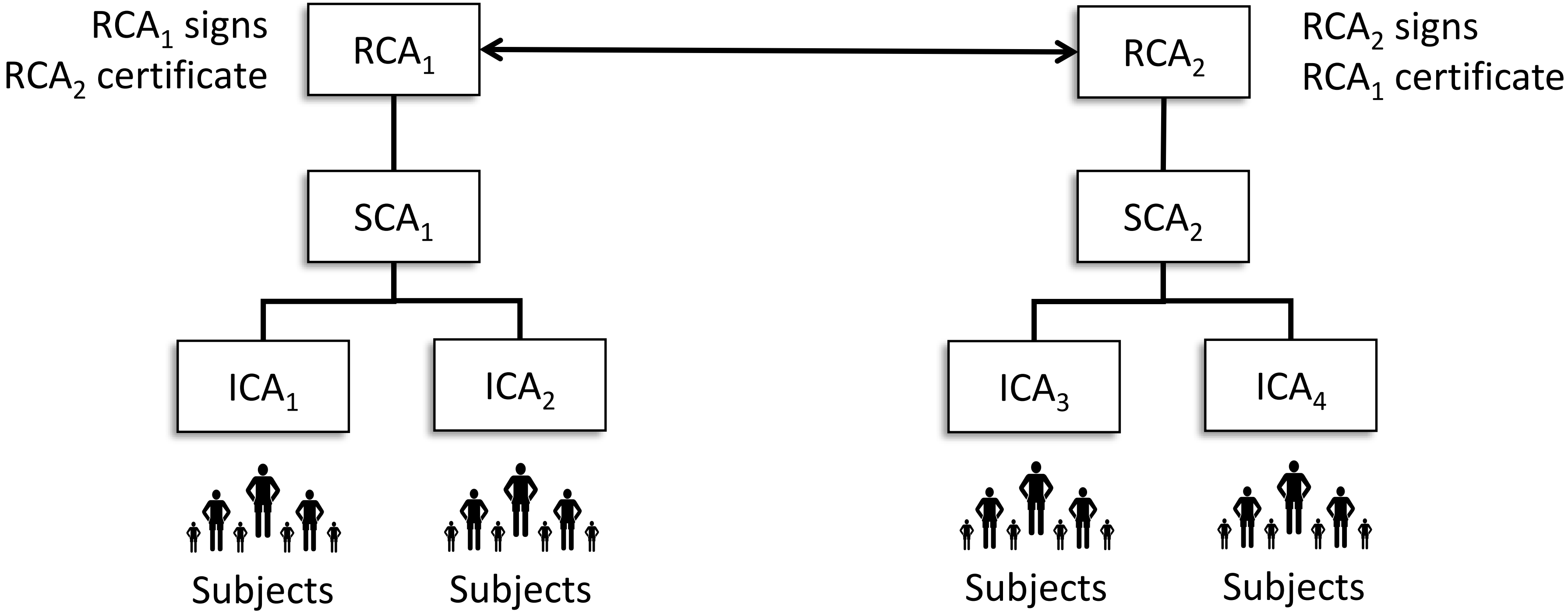
RP does all the work:

1) namely validation
2) assumes the risks
3) trusts the CA did its due diligence

- Subject sends EE certificate to Relying Party
- Relying Party validates the certificate chain to trust the EE public key
  1) Reconstructs the certificate chain
  2) Checks validity of each certificate
  3) Checks signature of each corticate
  4) Checks revocation status of each certificate

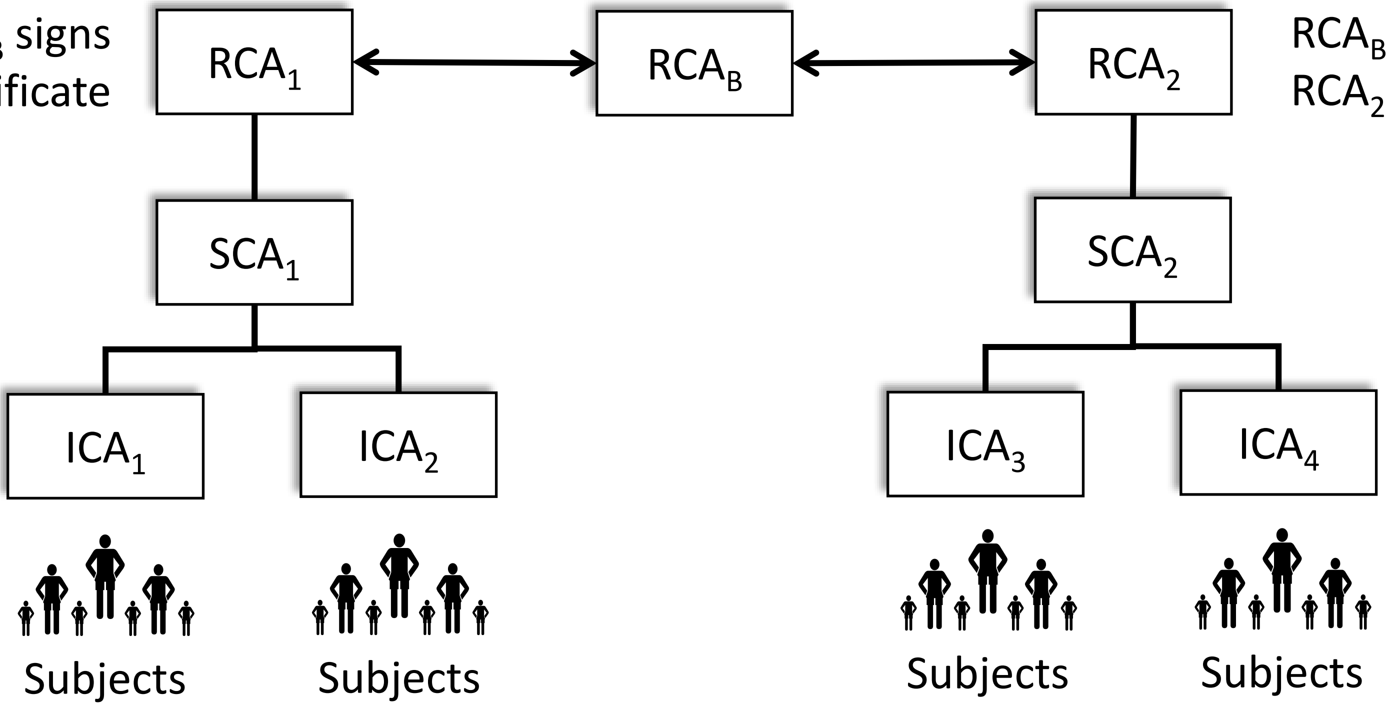
Note: reconstructing certificate chain can be tricky when interconnecting PKI

Addendum: PKI Cross-Certification



- Cross-certification makes sense when there are only a few PKI
- EE certificate signed by ICA$_1$ can be validated by relying party trusting RCA$_2$
- EE certificate signed by ICA$_4$ can be validated by relying party trusting RCA$_1$

Addendum: PKI Bridge

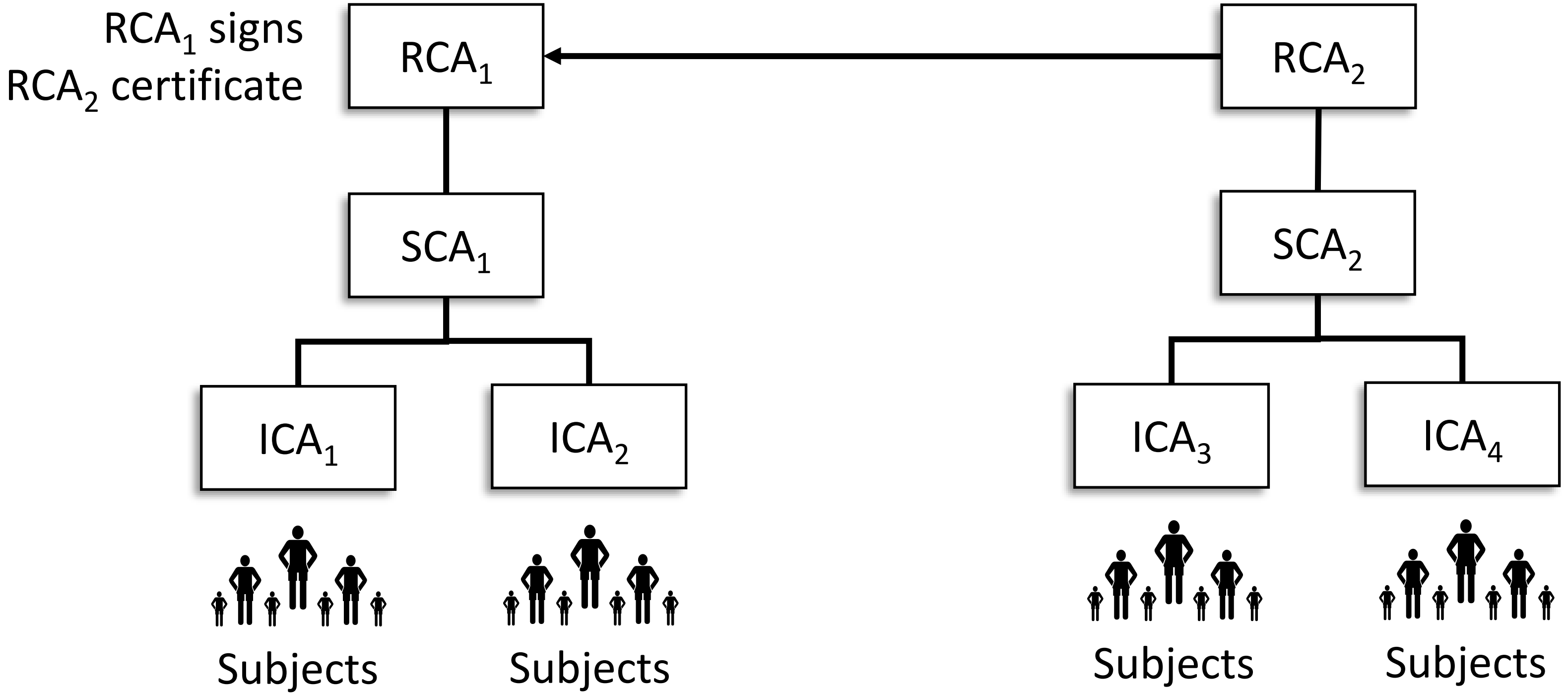


RCA$_B$ signs RCA$_1$ certificate

RCA$_B$ signs RCA$_2$ certificate

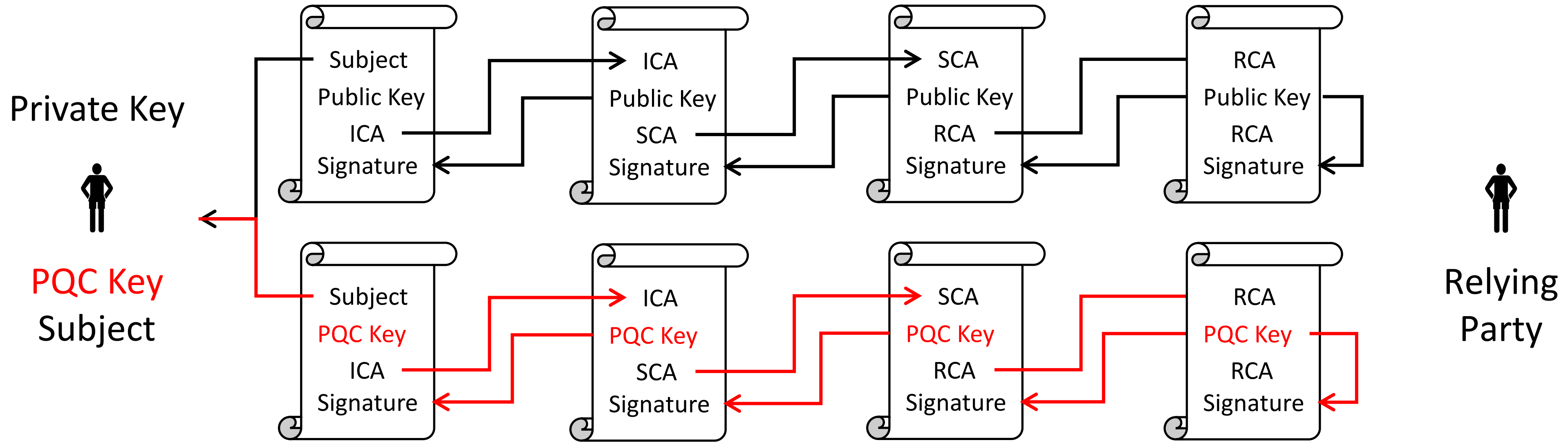
- Bridge RCA$_8$ makes sense when there are many PKI
- EE certificate signed by ICA$_1$ can be validated by relying party trusting RCA$_2$
- EE certificate signed by ICA$_4$ can be validated by relying party trusting RCA$_1$

Addendum: PKI Subordinate CA



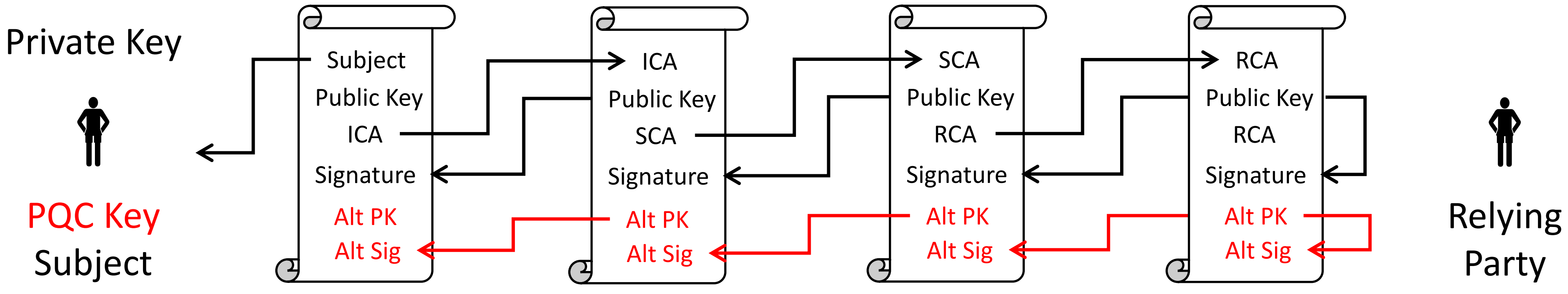
- *Subsidiary* makes sense when there are few PKI with one-way trust
- EE certificate signed by ICA_4 can be validated by relying party trusting RCA_1

Addendum: X.509 certificates



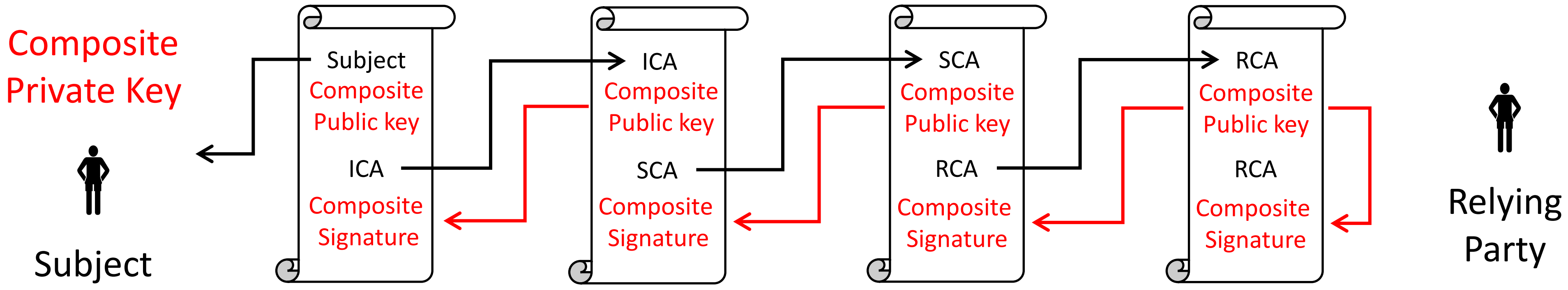
- Subject sends relevant certificate(s) to Relying Party
  - When is subject PQC-ready?
- Relying Party validates certificate chain
  - When is relying party PQC ready?

Addendum: X.509 *hybrid* certificates



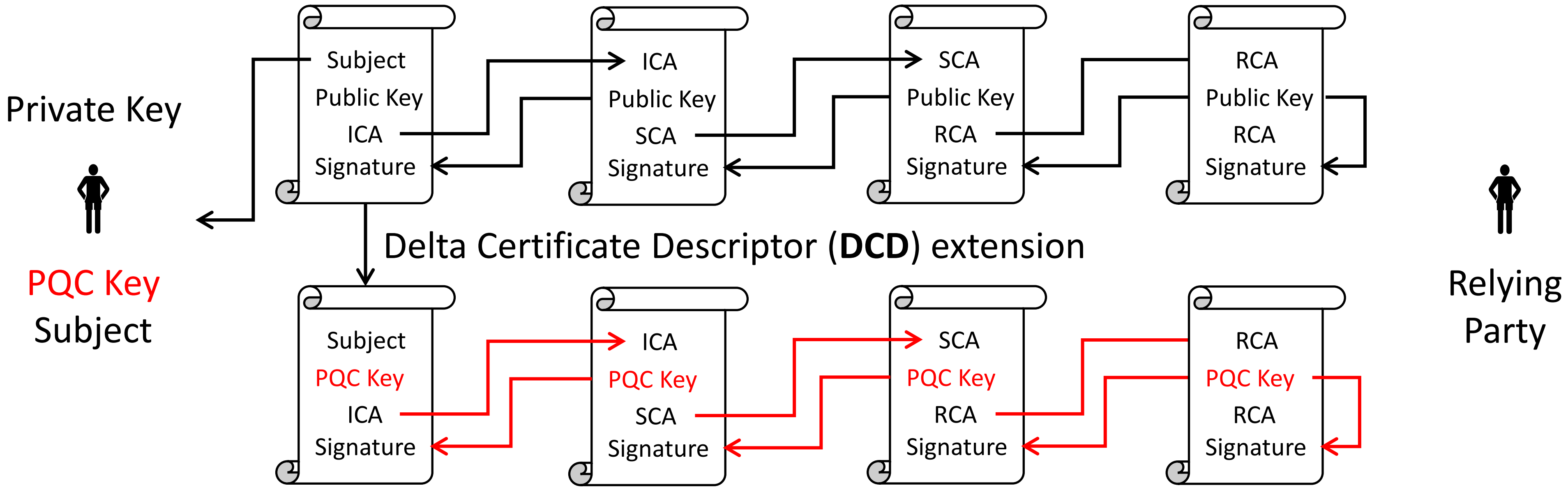
- Subject sends certificate(s) to Relying Party
  - *Native fields* legacy algorithm and signature
  - *Alt extensions* PQC algorithm and signature
- Relying Party validates certificate chain
  - Uses native fields when not PQC ready
  - Uses alt extensions when PQC ready

Addendum: X.509 *composite* certificates



- Composite keys consist of two or more asymmetric algorithms
  - Composite signatures are generated using *composite private* keys
  - Composite signatures are verified using *composition public* keys
- Subject sends *composite* certificate(s) to Relying Party
  - Subject supports *composite public keys* and *composite private keys*
- Relying Party validates certificate chain
  - When is Relying Party ready to support *composite public keys* and *composite signatures*?

Addendum: X.509 *chameleon* certificates



- Subject sends certificate(s) with DCD extension to Relying Party
- Relying Party validates certificate chain
  - Legacy certificate chain when not-PQC ready
  - PQC certificate chain when PQC-ready