ETSI/IQC Quantum Safe Cryptography Event

A New Hope: Efficient Migration Scenarios of PKIs to New Algorithms

Jan Klaußner

bundesdruckerei.

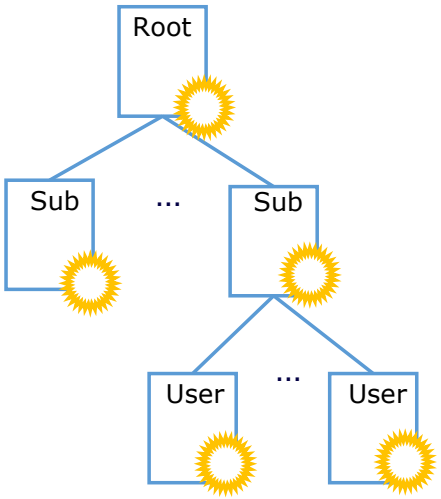
14/02/2023

Challenge for Open PKIs

Closed PKIs

- One stakeholder
- Controls all nodes

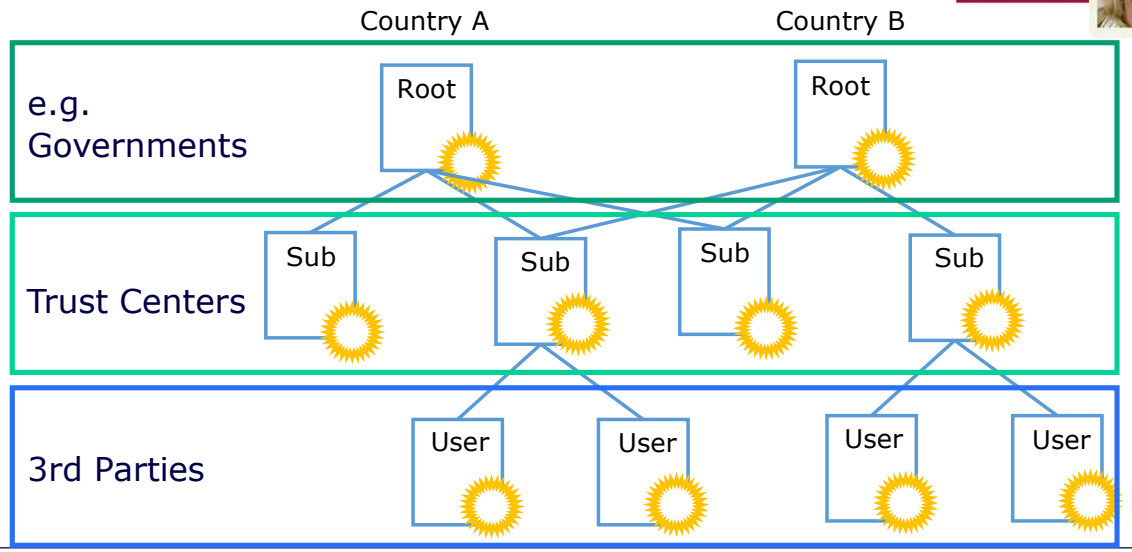
e.g. VPNs



Open PKIs

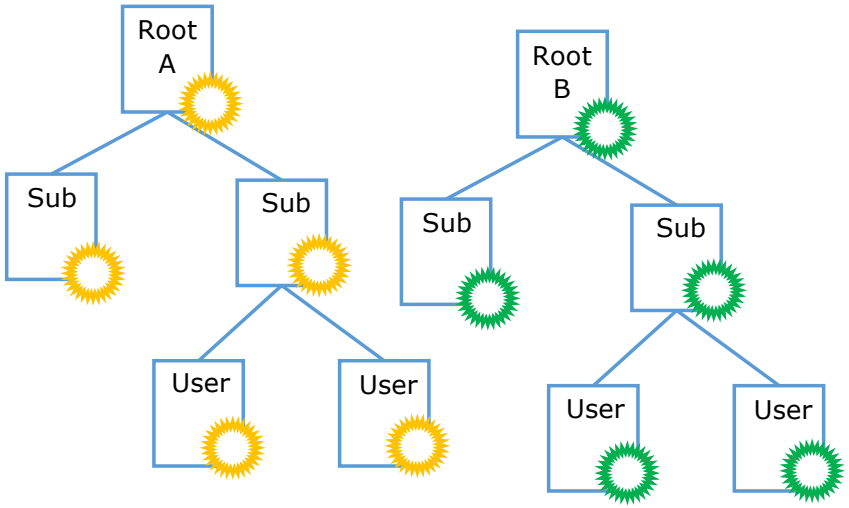
- Multiple Stakeholders
- Different Implementations
- Independent participants on nodes

e.g. German National ID



Classic Migration – Prepare and Switch

1 - Prepare new PKI

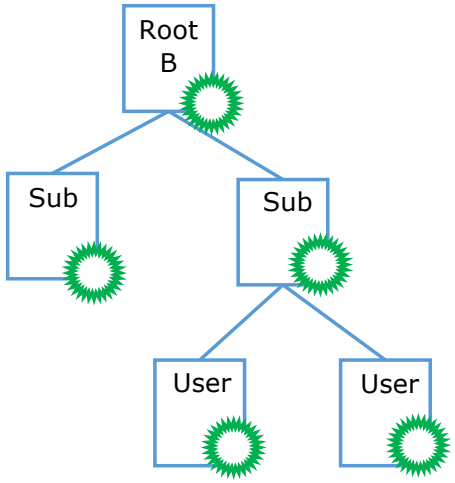


- Prepare all Certificates
- Prepare all Hardware and Software

– Takes long time until ready

Classic Migration – Prepare ad Switch

2 - Switch to new PKI on Flag Day



- Point of no Return

- chance of missed participants
- chance of missed support in HW/SW
- what if new (PQC) algorithm gets broken?

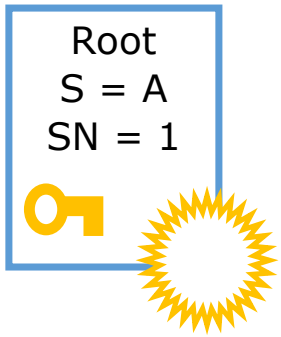
New Migration Method needed

- Classic method is hard even for Closed PKIs
- Usage and distribution of Open PKIs increases, so is their importance
- New PQC algorithms are not as mature and are up to surprises

New Method should provide…		.. by Tool
Stepwise migration	Allows stakeholders and participants to switch on own schedule	Root Key Update
Backwards compatibility	Allows uninterrupted Operation between old and new nodes	
Resilience against Cryptographic Event	Gives time to switch algorithm	Composite Keys

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

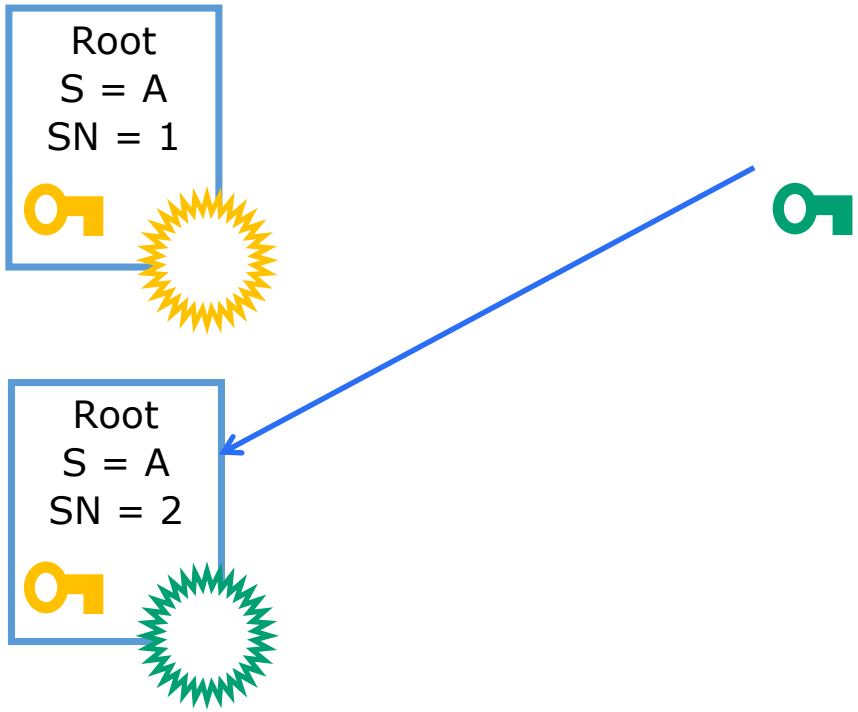


Cross Certificates with same SubjectName (S) and new Serial Number (SN)

1. Generate new key pair

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

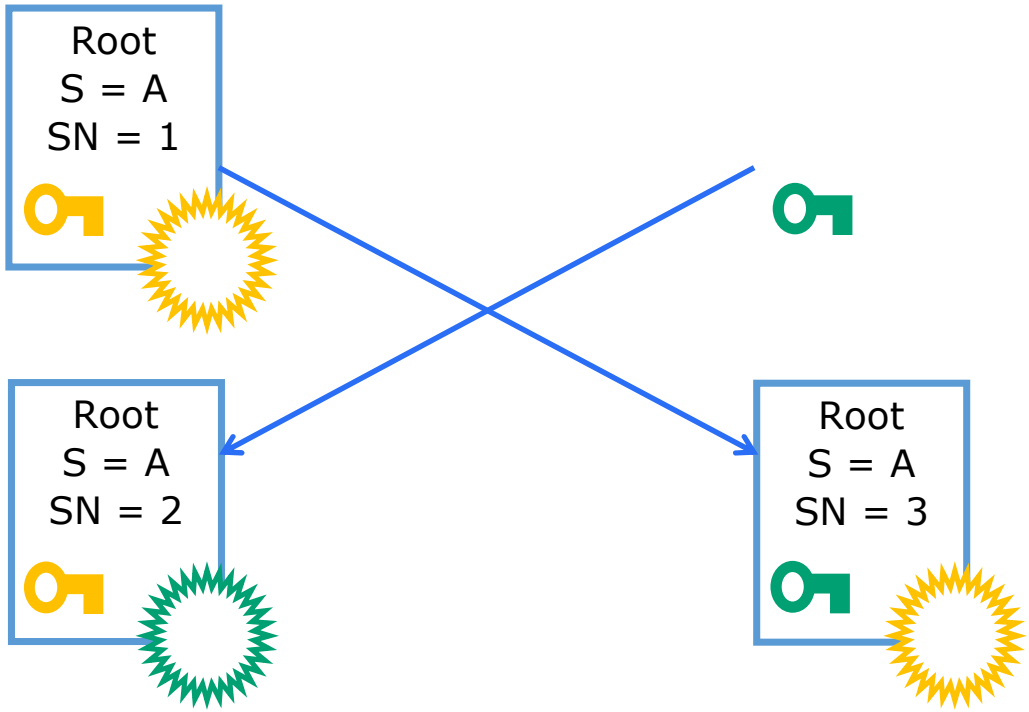


Cross Certification with same SubjectName (S) and new Serial Number (SN)

1. Generate new key pair
2. Create OldWithNew

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

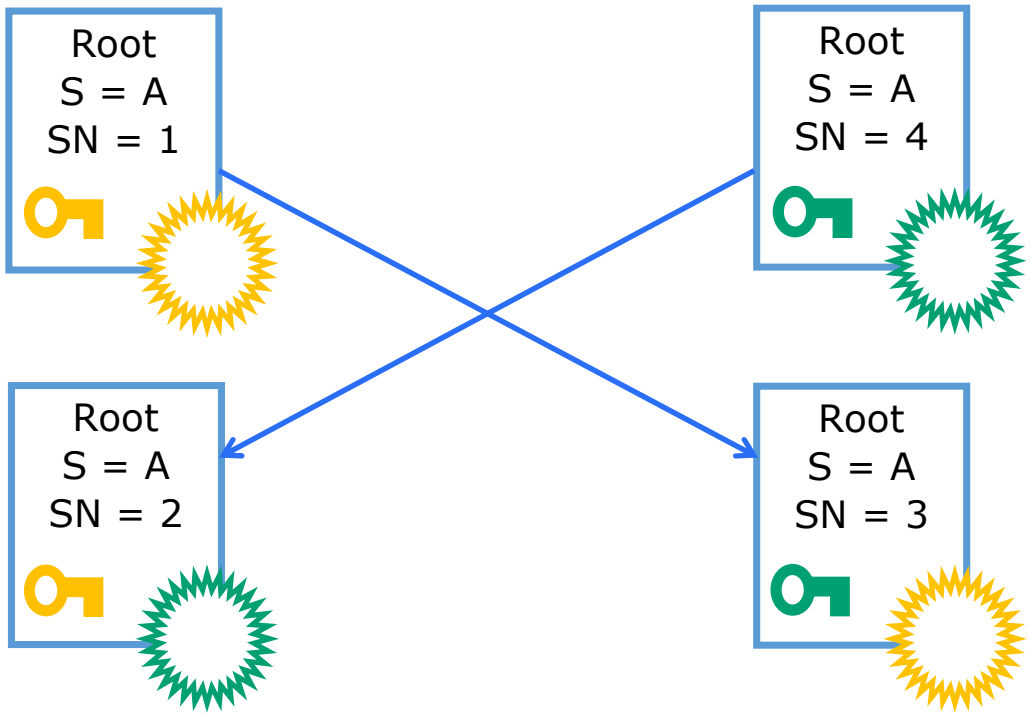


Cross Certification with same SubjectName (S) and new Serial Number (SN)

1. Generate new key pair
2. Create OldWithNew
3. Create NewWithOld

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

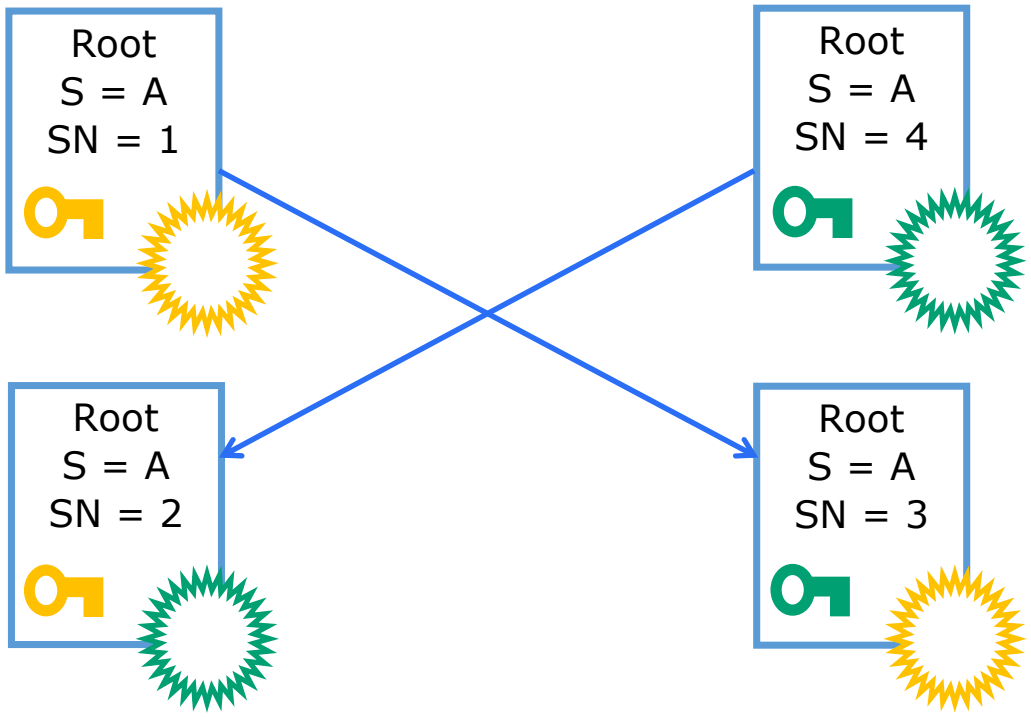


Cross Certification with same SubjectName (S) and new Serial Number (SN)

1. Generate new key pair
2. Create OldWithNew
3. Create NewWithOld
4. Create NewWithNew

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1



Cross Certification with same SubjectName (S) and new Serial Number (SN)

Further standards involved

- RFC 5652 – Validation of Public Key in Client
- RFC 5280 – PKI structure and Path Validation
- RFC 3280 – Authority Information Access

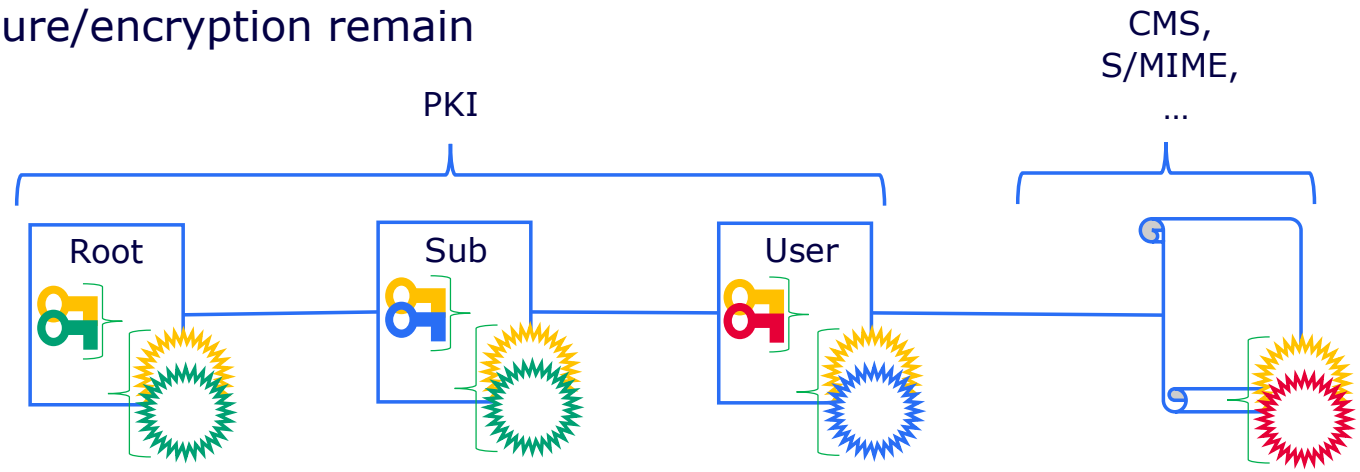
+ Old and new certificates share same PKI

+ Clients can Update themselves if needed

+ Old Root can be revoked by CRL

Composite Keys

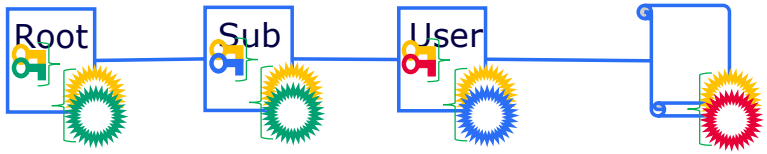
- Combines two or more different algorithms in one key
- No new certificate extensions needed
- all are used to sign or encrypt
- Breaking one still lets signature/encryption remain secure

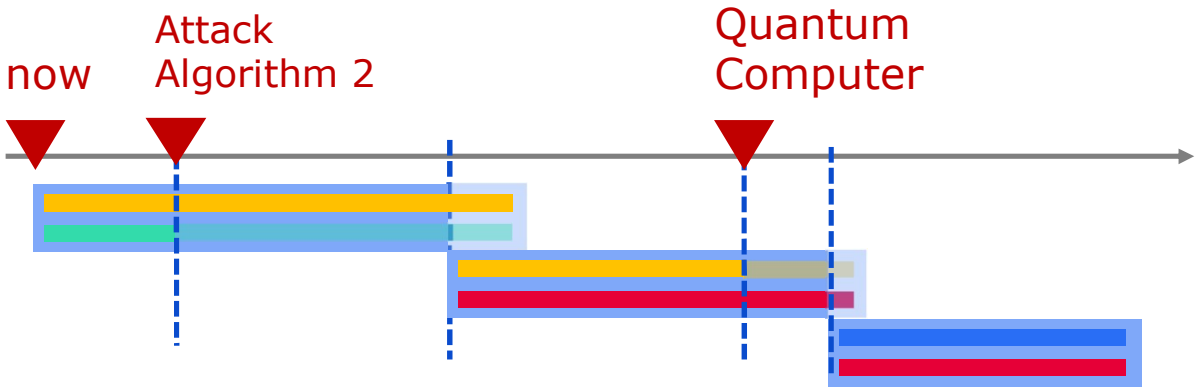


- Intelligent Composed Algorithms (ICA)
  https://eprint.iacr.org/2021/813.pdf
- Composite Keys, Signatures and KEMS
  https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-keys/
  https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs
  https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-kem

Composite Keys

- Combines two or more different algorithms in one key
- No new certificate extensions needed
- all are used to sign or encrypt
- Breaking one still lets signature/encryption remain secure

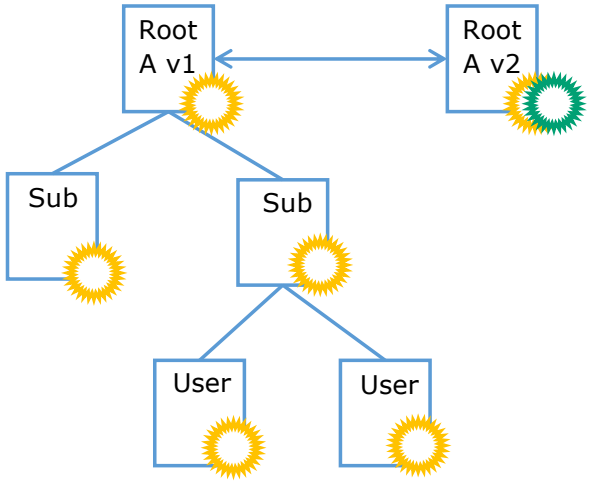




Algorithm 1 (e.g. classial)
Algorithm 2 (PQC)
Algorithm 3 (PQC)
Algorithm 4 (PQC)

Agile PKI Migration

1 - Root Key Update

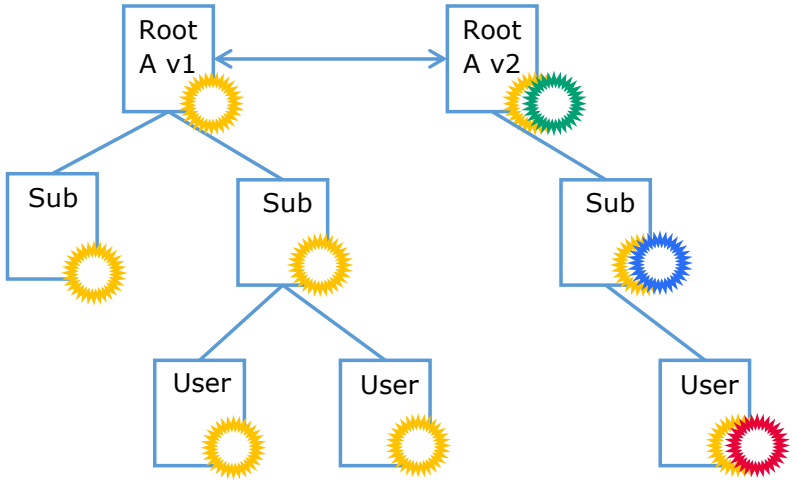


+ Already standardized, rarely used

+ Old and new certificates share same PKI

Agile PKI Migration

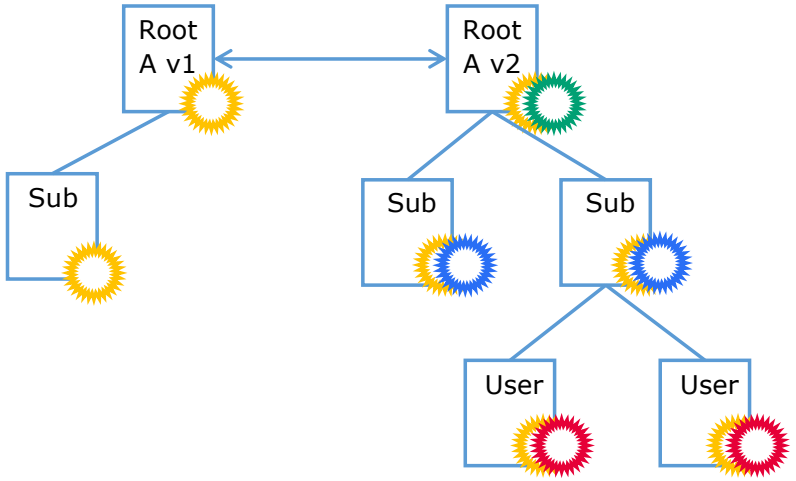
2 – Start Certificate Deployment



+ Test New Certificates without discarding old
+ Not all participants need to adopt at once

Agile PKI Migration

3 – Stepwise Revoke Certificates via CRL

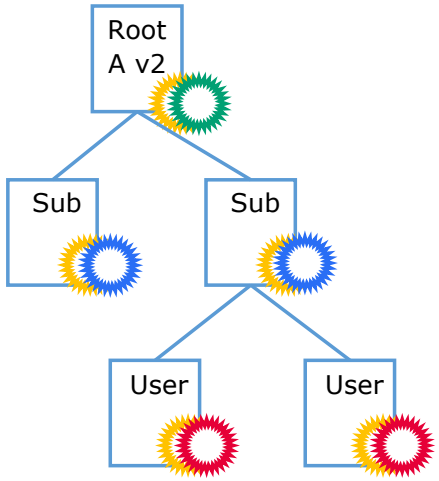


+ Test New Certificates without discarding old

+ Not all participants need to adopt at once

Agile PKI Migration

4 – Revoke old Root via CRL



+ With Composite Keys the PKI can operate even if one algorithm is broken

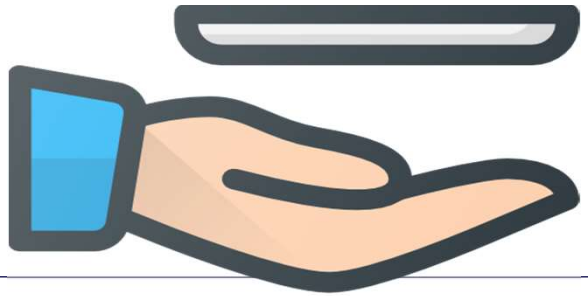
+ Repeat if needed

A New Hope

Summary

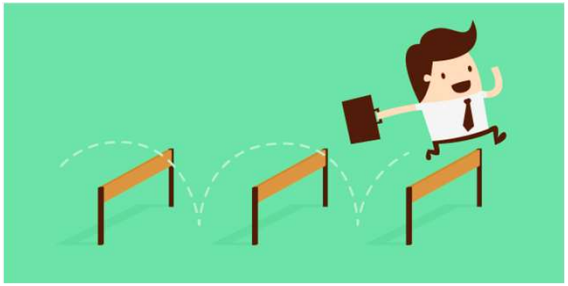
Agile PKI Migration provides

- Cryptoagilty for PKIs
- Stepwise Migration
- Frictionless Operation on Transition to new Root and Node Certificates



Obstacles to overcome

- Encourage Support of RFC-4210 Root Key Update
- Standardisation and Support of Composite Keys



- **FLOQI** (www.floqi.org)
  Concept and Demonstrator

Thank you.

Jan Klaußner

Bundesdruckerei GmbH
Senior Product Architect
E-Mail: jan.klaussner@bdr.de
Mobile: +49 (0) 151 5600 1986

Part of the Bundesdruckerei Group