Migration von Agilen PKIen

Datum: 24.05.2023
Ort: OmniSecure 2023 Berlin
Verfasser: Frank Byszio-Wegner, Jan Klaußner

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

Juli 2020

KEM Finalists	▲ KYBER
	▲ NTRU
	▲ SABER
	● Classic McEliece
KEM Alternates	● Bike
	▲ FrodoKEM
	● HQC
	▲ NTRU Prime
	■ SIKE
DSS Finalists	▲ DILITHIUM
	▲ FALCON
	▰ Rainbow
DSS Alternates	▰ GeMSS
	◆ Picnic
	◆ SPHINCS+

▲ Gitter
■ Isogenie
● Code
◆ Hash
▰ Multivariate

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

Februar 2022

KEM Finalists	▲ KYBER
	▲ NTRU
	▲ SABER
	● Classic McEliece
KEM Alternates	● Bike
	▲ FrodoKEM
	● HQC
	▲ NTRU Prime
	■ SIKE
DSS Finalists	▲ DILITHIUM
	▲ FALCON
	~~▰ Rainbow~~
DSS Alternates	▰ GeMSS
	◆ Picnic
	◆ SPHINCS+

Paper 2022/214

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens, IBM Research - Zurich

Abstract

This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks

Quelle: https://eprint.iacr.org/2022/214

▲ Gitter
■ Isogenie
● Code
◆ Hash
▰ Multivariate

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

Juli 2022

KEM Winners	▲ KYBER
KEM 4th Round	● Bike
	● HQC
	● Classic McEliece
	■ SIKE
DSS Winners	▲ DILITHIUM
	▲ FALCON
	◆ SPHINCS+
DSS Neuer Call for Proposals	Juni 2024

▲ Gitter
■ Isogenie
● Code
◆ Hash
▰ Multivariate

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

Juli 2022

KEM Winners	▲ KYBER
KEM 4th Round	● Bike ● HQC ● Classic McEliece ■ ~~SIKE~~
DSS Winners	▲ DILITHIUM ▲ FALCON ◆ SPHINCS+
DSS Neuer Call for Proposals	Juni 2023

Paper 2022/975

An efficient key recovery attack on SIDH (preliminary version)

Wouter Castryck, KU Leuven
Thomas Decru, KU Leuven

Abstract

We present an efficient key recovery attack on the Supersingular Isogeny Diffie-Hellman protocol (SIDH), based on a "glue-and-split" theorem due to Kani. Our attack exploits the existence of a small non-scalar endomorphism

Quelle: https://eprint.iacr.org/2022/975

▲ Gitter
■ Isogenie
● Code
◆ Hash
▰ Multivariate

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

Mai 2023	
KEM Winners	▲ KYBER
KEM 4th Round	● Bike
	● HQC
	● Classic McEliece
DSS Winners	▲ DILITHIUM
	▲ FALCON
	◆ SPHINCS+
DSS Neuer Call for Proposals	Juni 2023

- Praktische Sicherheit noch nicht gut verstanden
- Implementierungsfehler
- Noch kein Test durch Quantenalgorithmus

-> mehr Angriffe erwartet

▲ Gitter
■ Isogenie
● Code
◆ Hash
▰ Multivariate

Sind sie sicher?

7 Jahre NIST PQC Wettbewerb…

- Praktische Sicherheit noch
  nicht gut verstanden

sfehler

urch
nus

wartet

Na und?

Dann tauschen wir sie einfach aus!

Neuer Call for Proposals

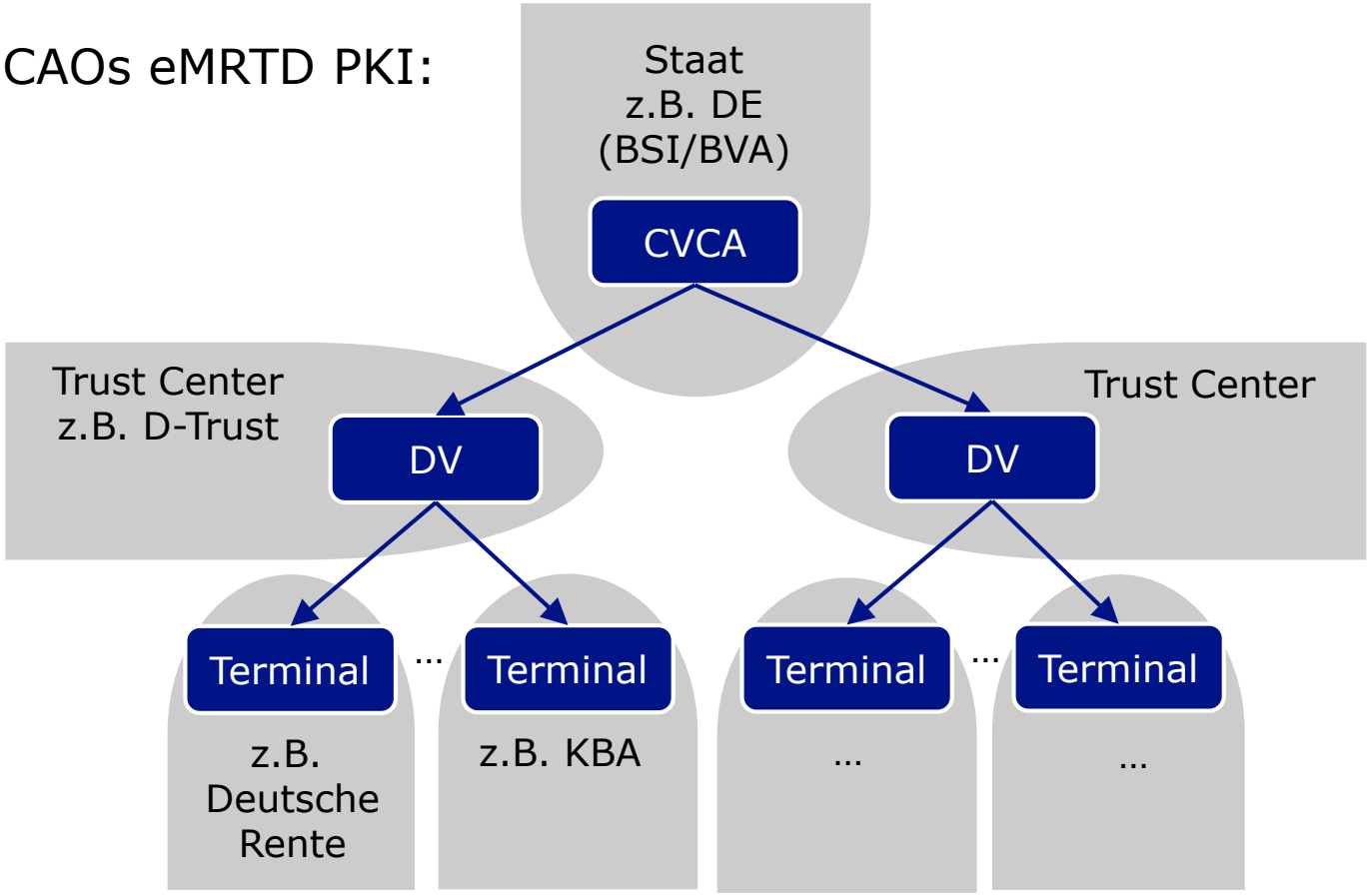
Juni 2023

- Gitter
- Isogenie
- Code
- Hash
- Multivariate

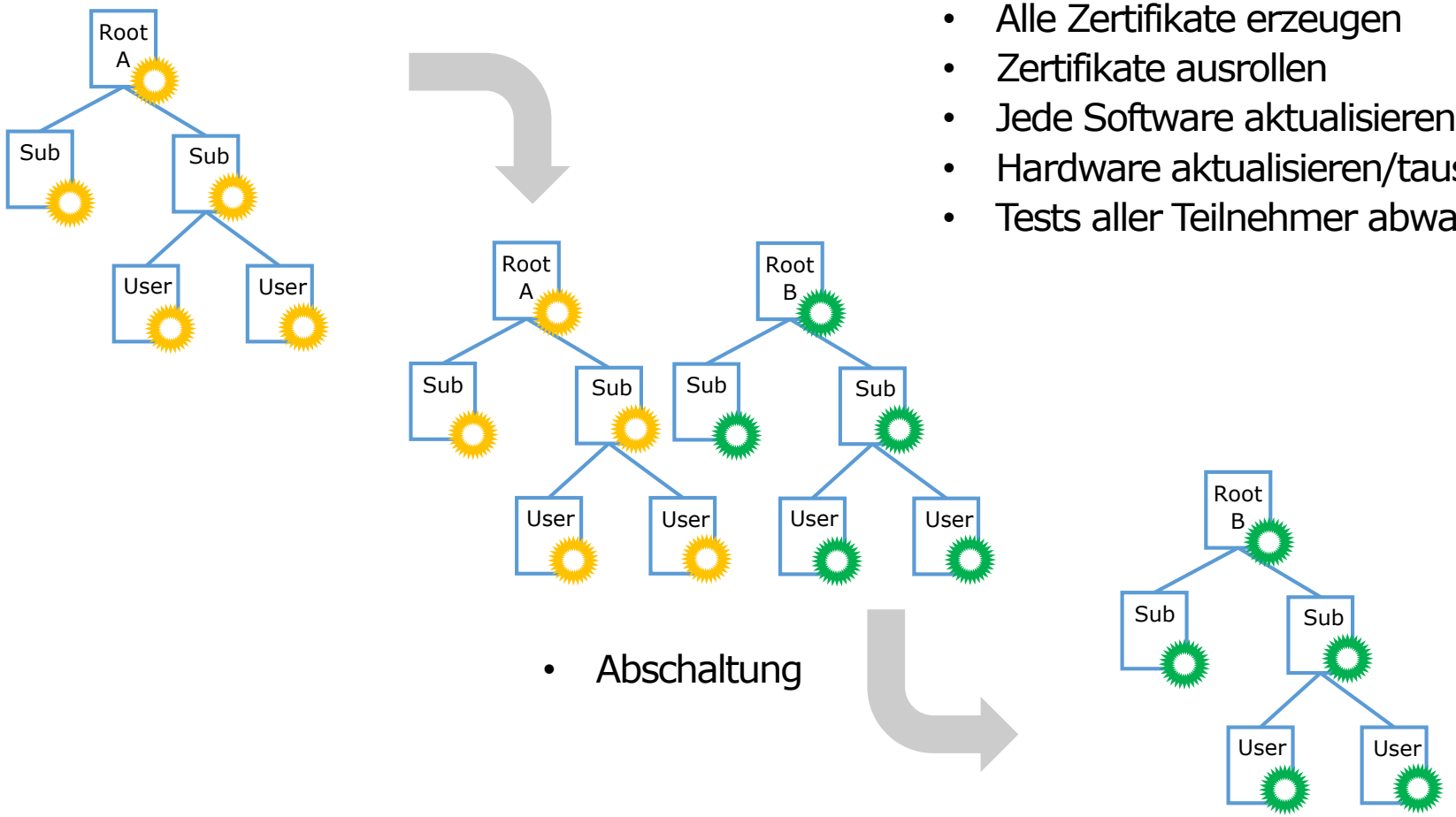
Offene Public-Key-Infrastrukturen

- Mehrere Stakeholder
- Verschiedene Zulieferer von Hard- und Software
- Unabhängige Teilnehmer

ICAOs eMRTD PKI:



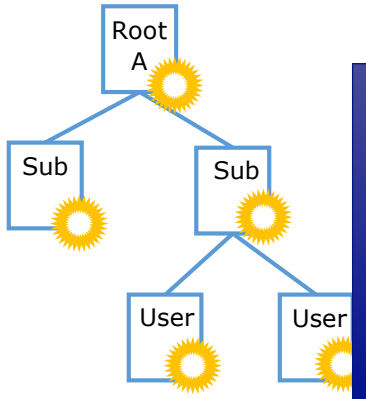
PKI Migration - bisher



- Alle Zertifikate erzeugen
- Zertifikate ausrollen
- Jede Software aktualisieren
- Hardware aktualisieren/tauschen
- Tests aller Teilnehmer abwarten

- Abschaltung

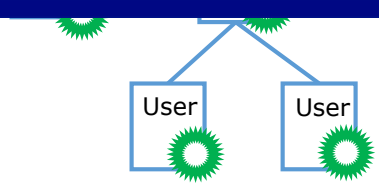
PKI Migration - bisher



- Alle Zertifikate erzeugen
- Abschaltung

- Lange Übergangszeit (15 Jahre)
- Sicherheitsvorfall in offener PKI risikoreich und teuer
- Bedeutung und Ausbreitung offener PKIen steigt
- Neue Algorithmen sind noch in Bewährung, doch die Zeit läuft ab

Neuer Ansatz wird gebraucht



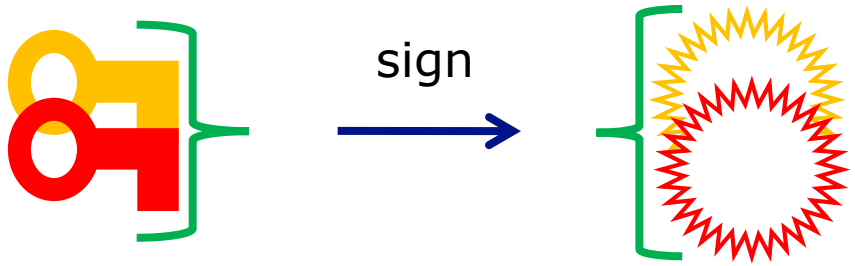
Die Agile PKI

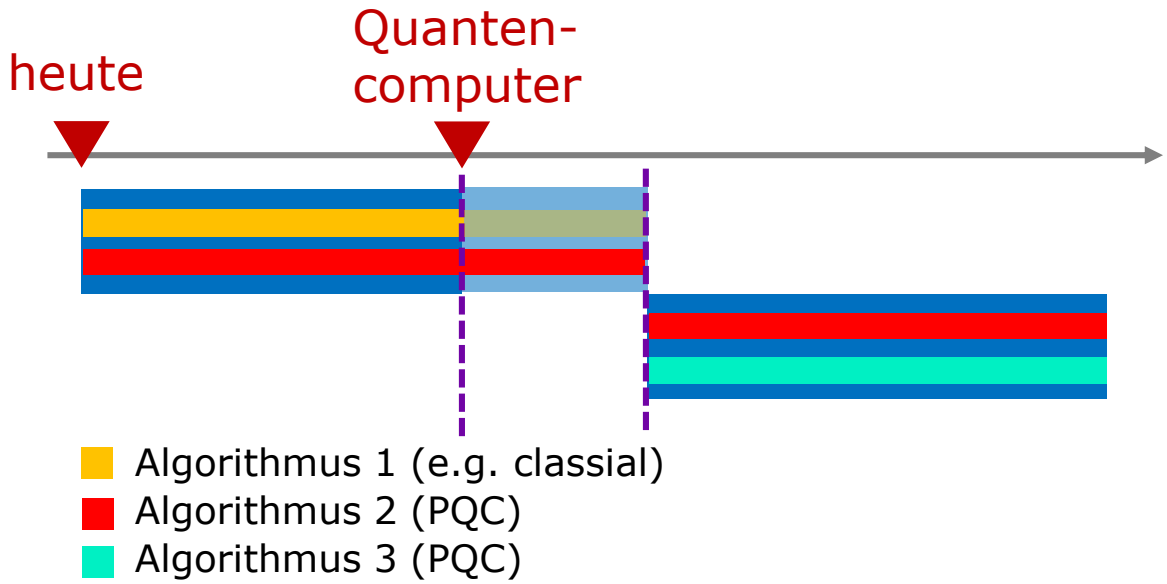
Agilität		**… durch**
Unabhängige Migration	Erlaubt Teilnehmern den Wechsel mit eigenem Zeitplan	Root Key Update
Rückwärts-kompatibiltät	Unterbrechungsfreier Betrieb mit neuen und alten Knoten	
Resilienz gegenüber Kryptographischen Schwachstellen	Erweitert Zeitfenster zum Algorithmenwechsel	Composite Keys

Composite Keys

- Kombiniert mindestens zwei Algorithmen in einem Schlüssel
- Benötigt keine neuen Datenelemente in Zertifikaten/ Protokollen/Dokumenten
- Alle kombinierten Algorithmen werden zum Signieren oder Verschlüsseln benutzt

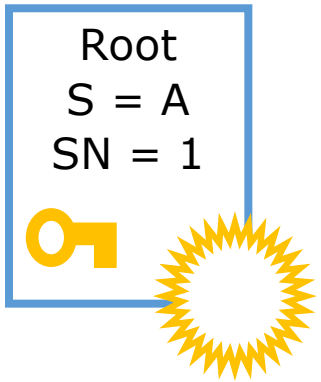
➢ Signatur/Schlüsseltext bleibt sicher auch wenn ein Algorithmus/Schlüssels gebrochen wurde





Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

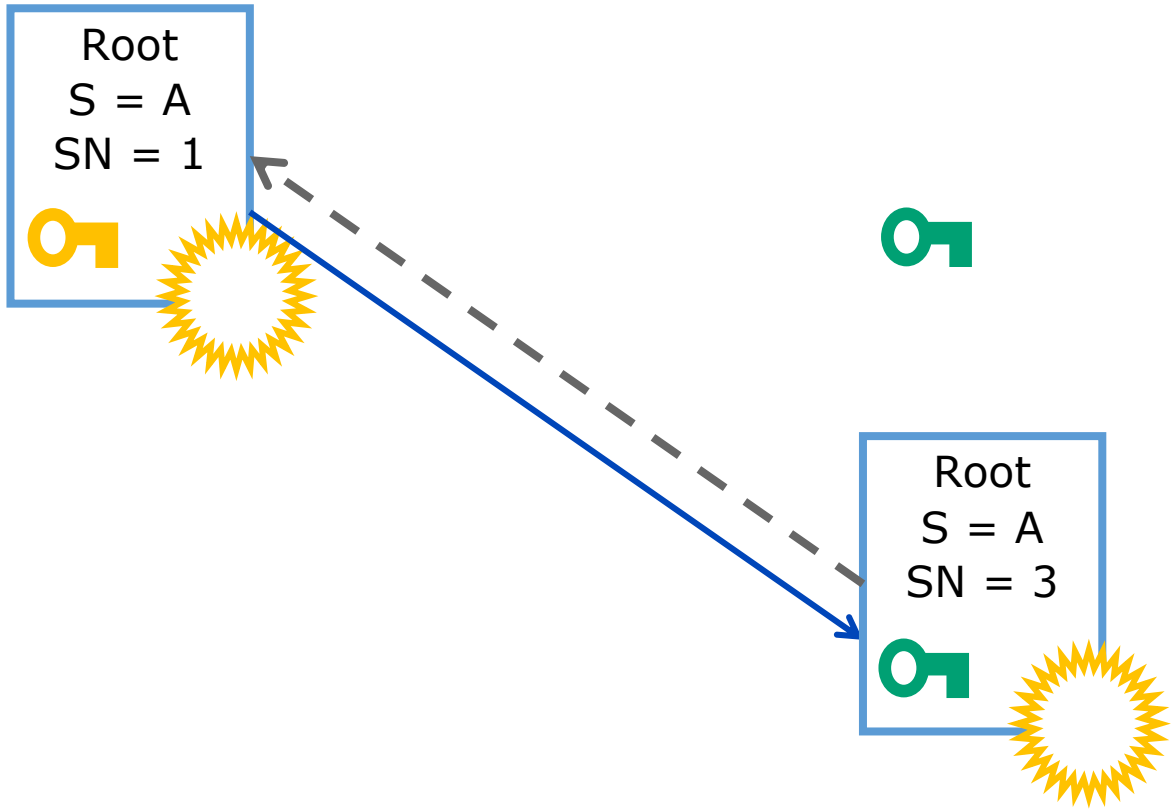


Erzeugung von Cross Certificates mit gleichem SubjectName (S) und neuer Seriennummer (SN)

1. Neues Schlüsselpaar generieren

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

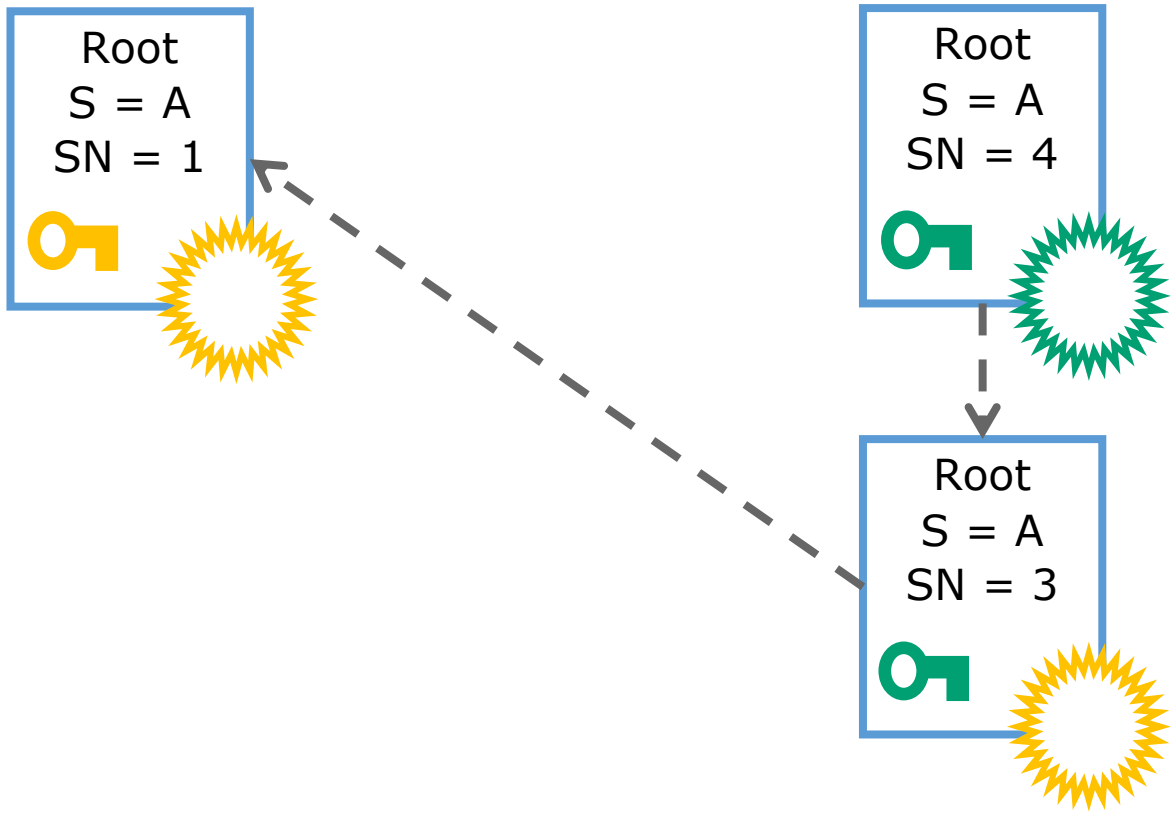


Erzeugung von Cross Certificates mit gleichem SubjectName (S) und neuer Seriennummer (SN)

1. Neues Schlüsselpaar generieren
2. Erzeuge NewWithOld Zertifikat
   – Link zu OldWithOld

Root Key Update

RFC-4210 (Certificate Management Protocol) 4.4.1

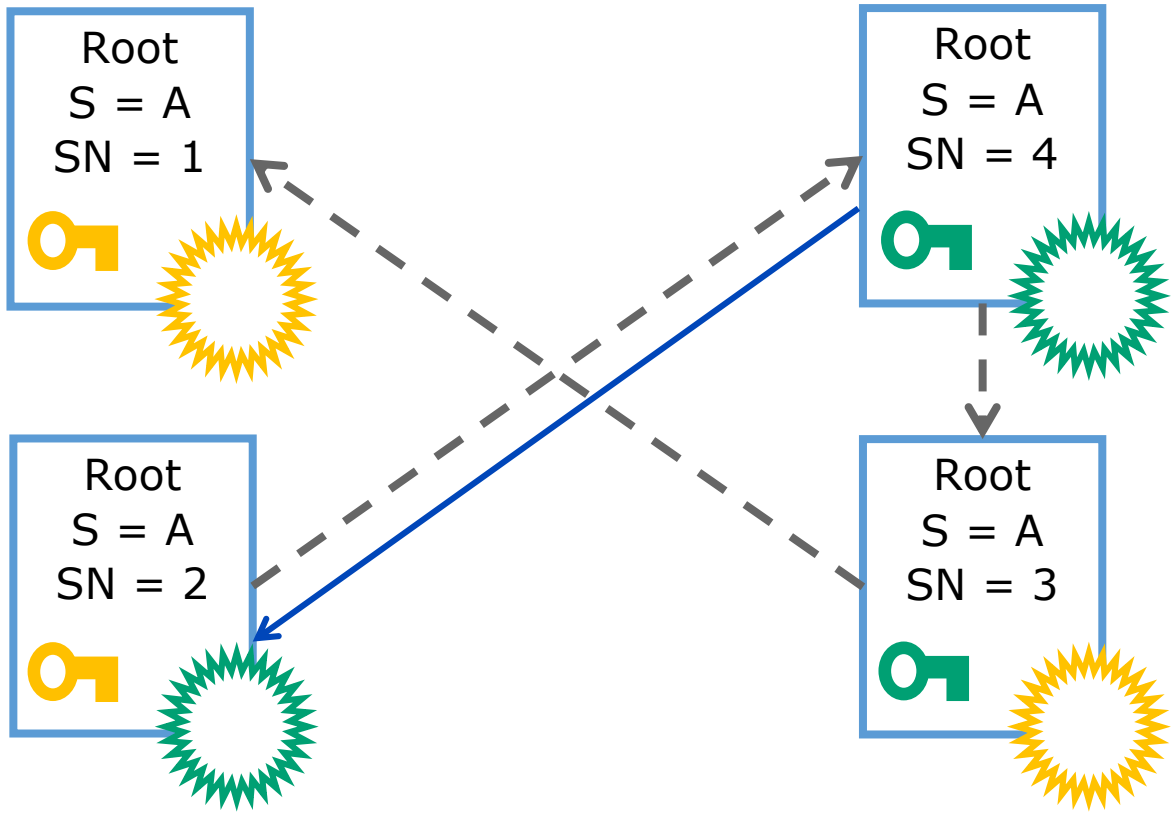


Erzeugung von Cross Certificates mit gleichem SubjectName (S) und neuer Seriennummer (SN)

1. Neues Schlüsselpaar generieren
2. Erzeuge NewWithOld Zertifikat
   – Link zu OldWithOld
3. Erzeuge NewWithNew Zertifikat
   - Link zu NewWithOld

Root Key Update

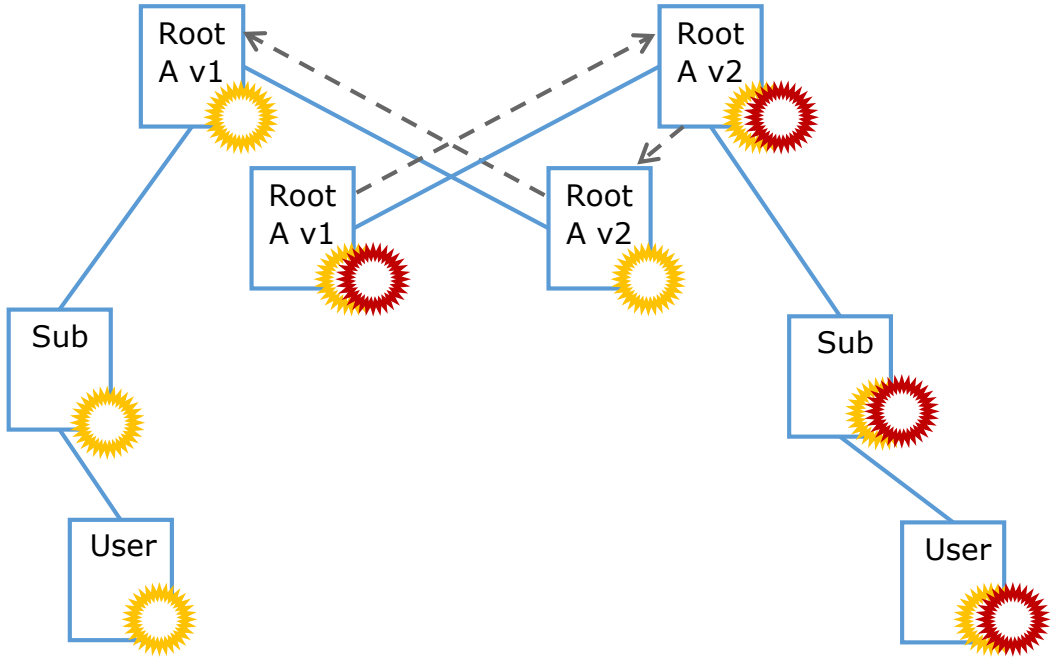
RFC-4210 (Certificate Management Protocol) 4.4.1



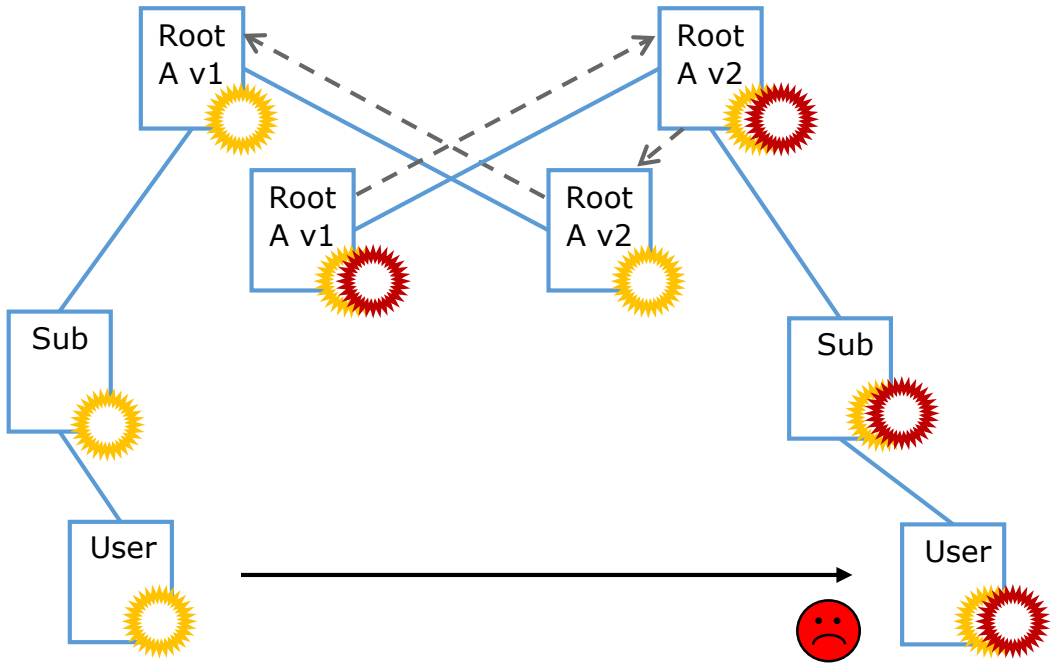
Erzeugung von Cross Certificates mit gleichem SubjectName (S) und neuer Seriennummer (SN)

1. Neues Schlüsselpaar generieren
2. Erzeuge NewWithOld Zertifikat
   – Link zu OldWithOld
3. Erzeuge NewWithNew Zertifikat
   - Link zu NewWithOld
4. Erzeuge OldWithNew Zertifikat
   - Link zu NewWithNew

Die Agile PKI



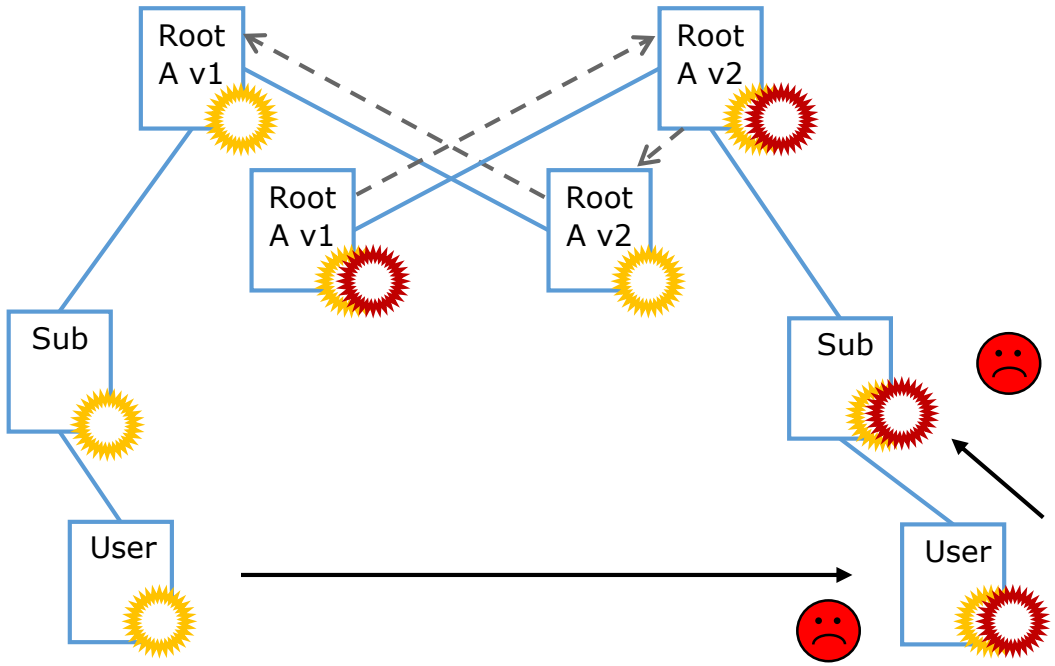
Die Agile PKI



User v1 prüft Zertifikat v2

1. Unvertraute Signatur, prüfe SubCA

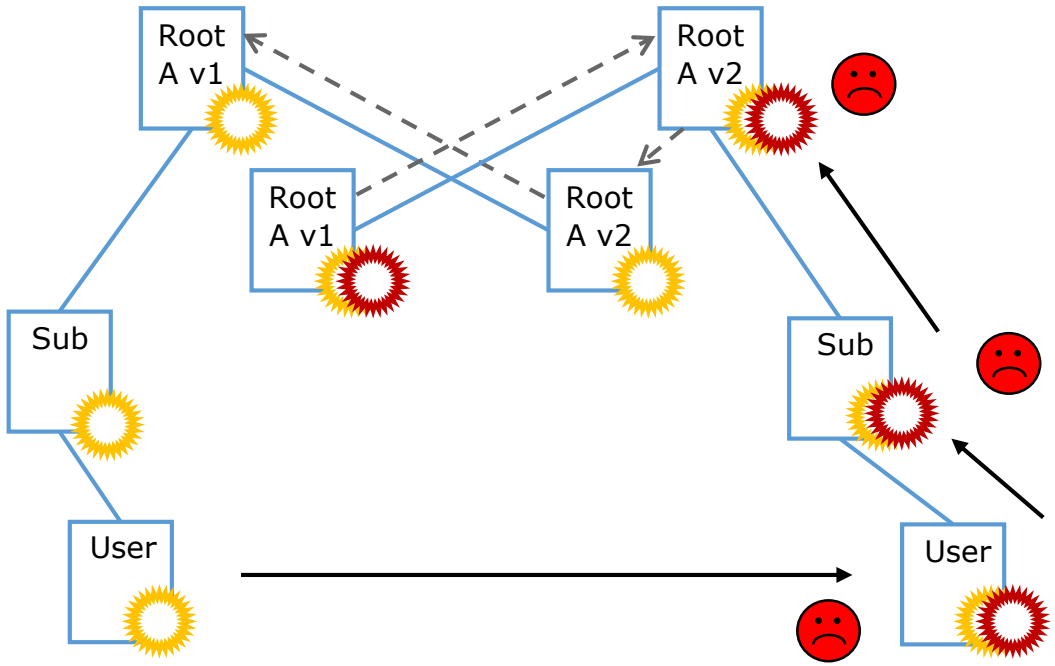
Die Agile PKI



User v1 prüft Zertifikat v2

1. Unvertraute Signatur, prüfe SubCA
2. Unvertraute Signatur, prüfe Root

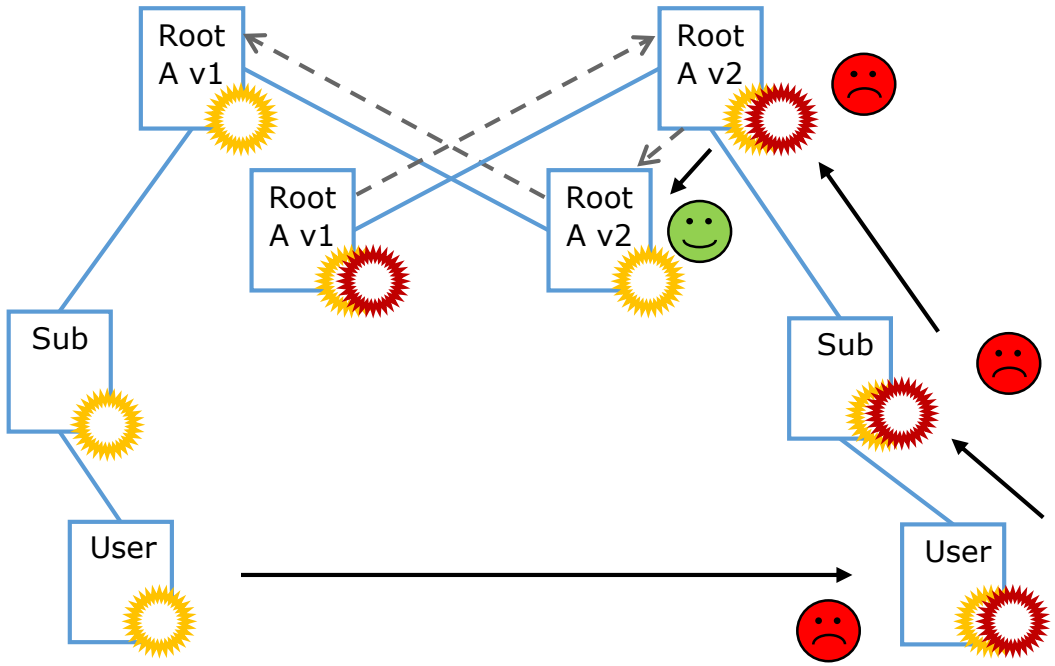
Die Agile PKI



User v1 prüft Zertifikat v2

1. Unvertraute Signatur, prüfe SubCA
2. Unvertraute Signatur, prüfe Root
3. Unvertraute Root, prüfe Crosszertfikat

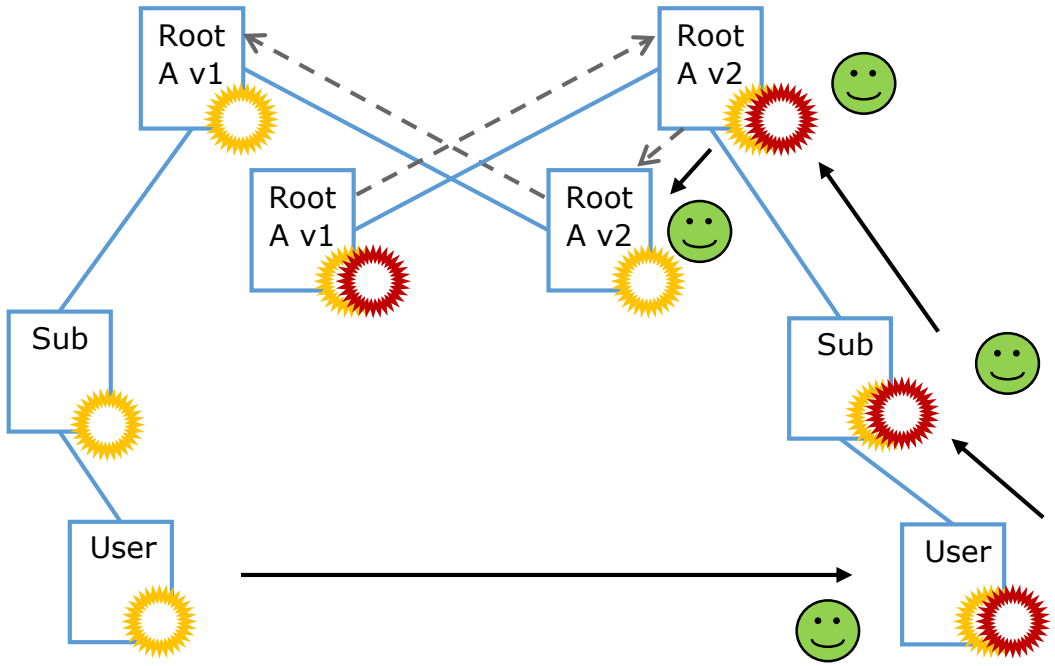
Die Agile PKI



User v1 prüft Zertifikat v2

1. Unvertraute Signatur, prüfe SubCA
2. Unvertraute Signatur, prüfe Root
3. Unvertraute Root, prüfe Crosszertfikat
4. Vertraute Signatur

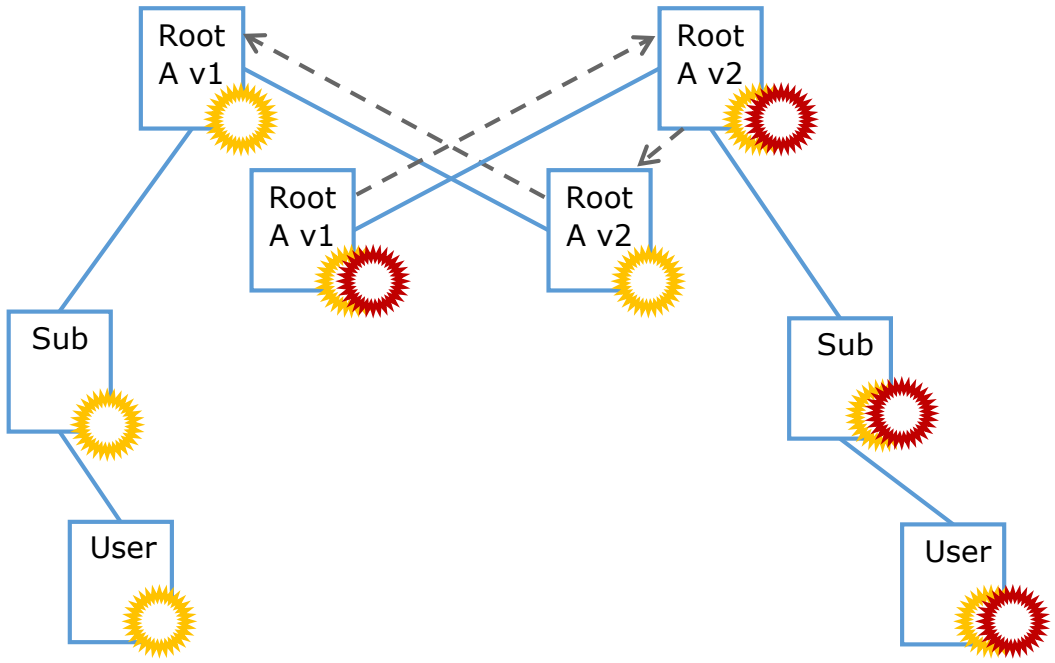
Die Agile PKI



User v1 prüft Zertifikat v2

1. Unvertraute Signatur, prüfe SubCA
2. Unvertraute Signatur, prüfe Root
3. Unvertraute Root, prüfe Crosszertfikat
4. Vertraute Signatur
5. Installiere Root v2

Die Agile PKI



- Resilienz gegen Schwachstellen in einzelnen Algorithmen oder Implementierungen
- Unabhängige Migration
- Automatische Installation
- Unterbrechungsfreier Betrieb während der Migration
- Test neuer Algorithmen ohne Betriebsstörung

Ausblick

Root Key Update

- Standard seit 2005
- Unterstützung mangelhaft

Composite Keys

- Standardisierung von Composite Keys in Arbeit (IETF)
- Implementierung von Composite Keys teilweise erfolgt (BouncyCastle, Botan)

Jan Klaußner
Senior Product Architect
Email: jan.klaussner@d-trust.net
Telefon: +49 (0) 151 5600 1986

Vielen Dank!