Post-Quantum

Cryptography Conference

# CRQC and Signatures – no Problem?

**Jan Klaußner**
Senior Product Architect at D-Trust

# CRQC and Signatures

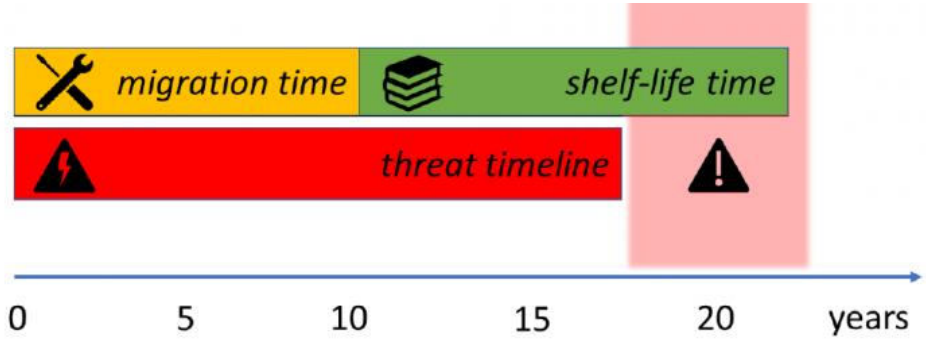
## No Problem?

Date: 08.11.2023
Location: Post-Quantum Cryptography Conference 2023
Author: Jan Klaußner

# Moscas Theorem and eIDAS

„A qualified electronic signature shall have the equivalent legal effect of a handwritten signature."

*eIDAS Regulation, articel 25 para. 2*




© 2021 Quantum Threat Timeline Report, Mosca/Piani, 01/2022

- retired algorithms or keys do not matter
- no obligation for archives, regular timestamping or re-signing

A Qualified electronic signature issued today is expected to be legally binding **forever**.

# Court case simulation

Disability pension claim

… electronic signature with outdated key length

➔ free consideration of evidence

*TransiDoc survey 2006*

© Image by rawpixel.com on Freepik

# PQC now!

# The PQC Signature Zoo

Simple replacement… does it work?

| Standard | Draft | New DSS |
|---|---|---|
| ♦ XMSS* | ▲ Dilithium | ▲ 7 |
| ♦ LMS* | ▲ Falcon | ● 6 |
| | ♦ Sphincs+ | ■ 1 |
| | | ✱ 10 |
| | | ❖ 7 |
| | | ◈ 4 |
| | | ⁂ 5 |

Probably not:

- Statefulnes
- Signature and Public Key Size
- Performance
- Trust in math

▲ Lattice
♦ Hash [* stateful]
● Code
■ Isogeny
✱ Multivariate
❖ MPC in the head
◈ Symmetric
⁂ other

# The Quicksand of PQC

- **breakups**
  - see SIKE, Rainbow
- **improvements**
  - see switch RSA PKCS1.5 to PSS
- **bugs**
  - see ROCA attack on RSA
  - see ECDSA „Psychic Signatures“
- **more PQC signatures**
  - NISTs new competition
- **New Quantum algorithms**

# The Quicksand of PQC

- **breakups**
  - see SIKE, Rainbow
- **improvements**
  - see switch RSA PKCS1.5 to PSS
- **bugs**
  - see ROCA attack on RSA
  - see ECDSA „Psychic Signatures“
- **more PQC signatures**
  - NISTs new competition
- **New Quantum algorithms**

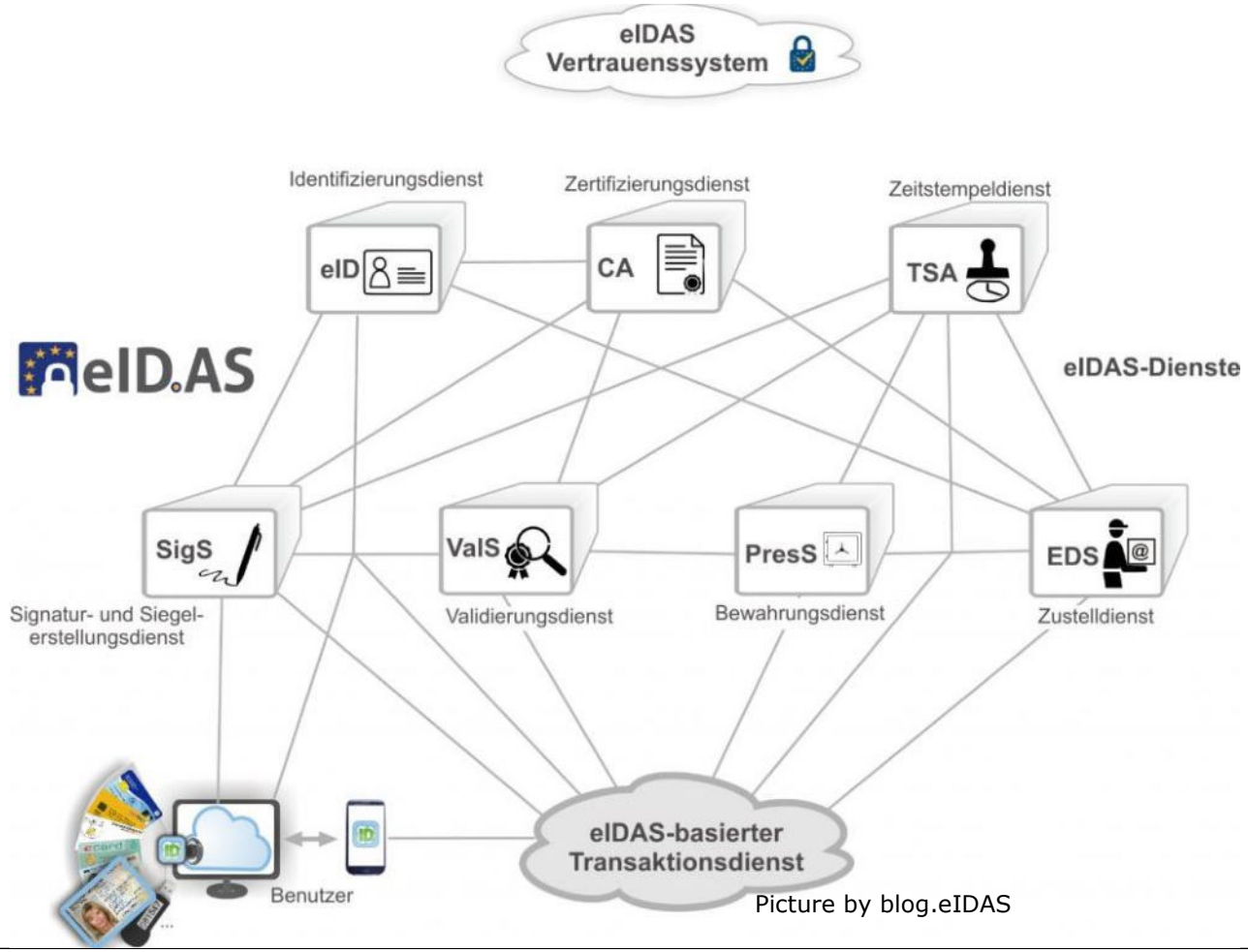
**short term switching**
of keys and algorithms

**cover security gaps**
due to weak keys or algorithms

**Agility**

# The Quicksand of PQC and eIDAS

## Agility?




Picture by blog.eIDAS

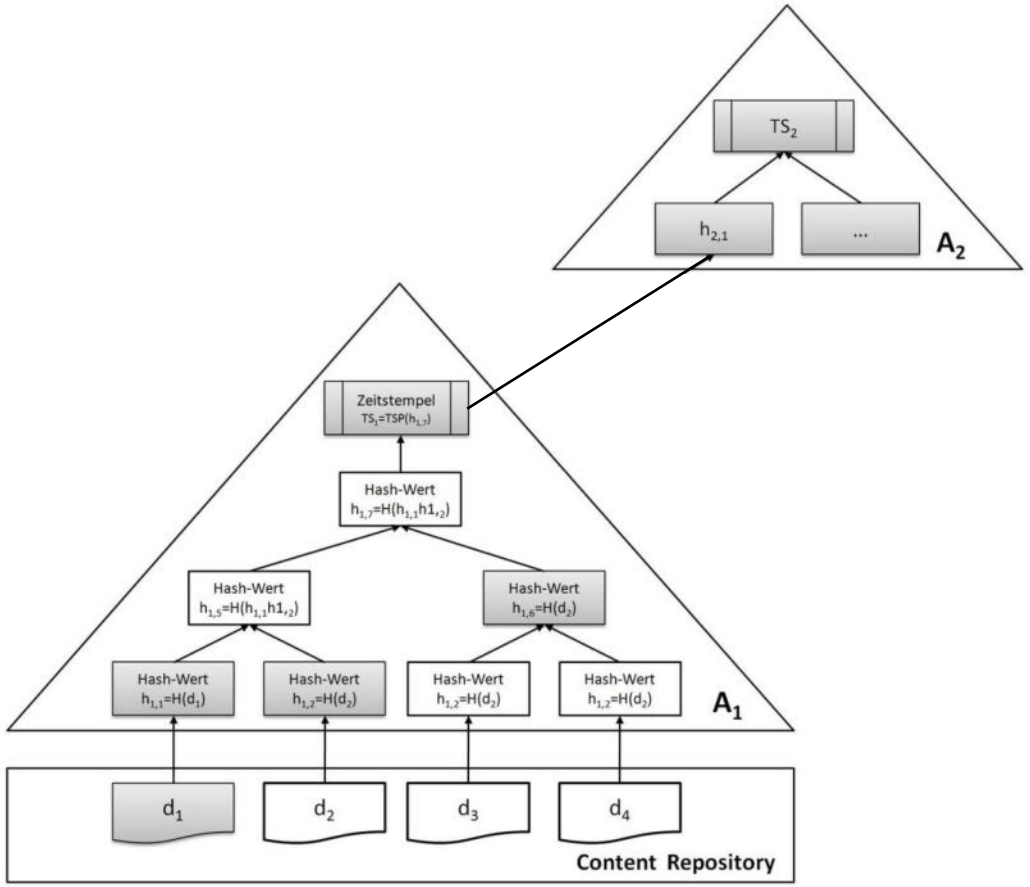
# Current Approach

- Timestamps
- AdES digital signatures
- ERS

Timestamps are not for free
Maybe two timestamps are required

Will hinder deployment of Digital Signatures

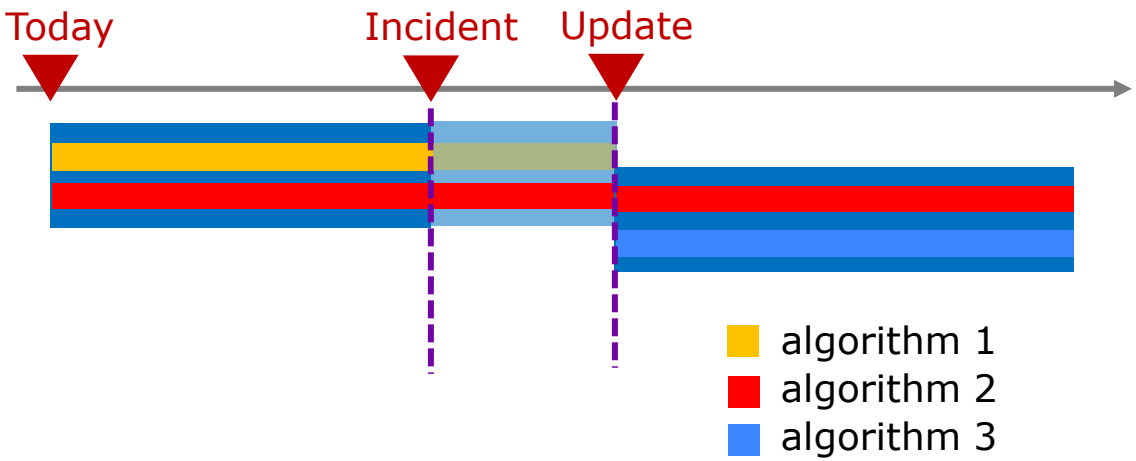
➔ Better make simple signatures last longer!



# Hybrid Scheme

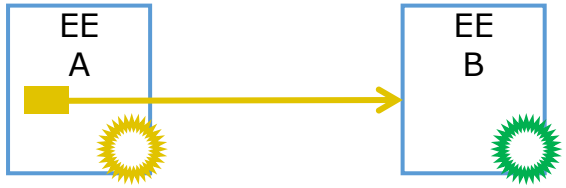
use two or more algorithms

- Combine traditional and/or PQ algorithms
- bridges security gap if one fails



# Related Certificates

Cryptographic linking of two certificates to same entity



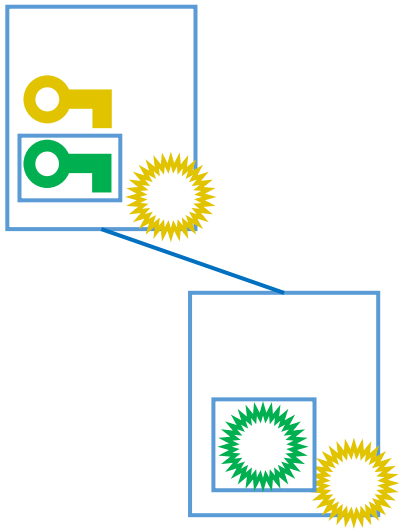

- non-critical X.509v3 extension
- CA validates reference an signs

| | | |
|---|---|---|
| Standard | ● | draft-ietf-lamps-cert-binding-for-multi-auth |
| No algorithm restriction | ✓ | |
| Protocol independent | ✘ | Only X.509 end entity certificates; handling of two PKIs needed |
| Security implication | ✘ | Usage of related keys out of scope; only one way relation |
| Backward compatibility | ✓ | Non-critical extensions are ignored if unknown |
| Forward compatibility | ✘ | |

# Isara Catalyst Extension

Additional key and signature in certificate

- X.509v3 extension
- also for CSRs and CRLs

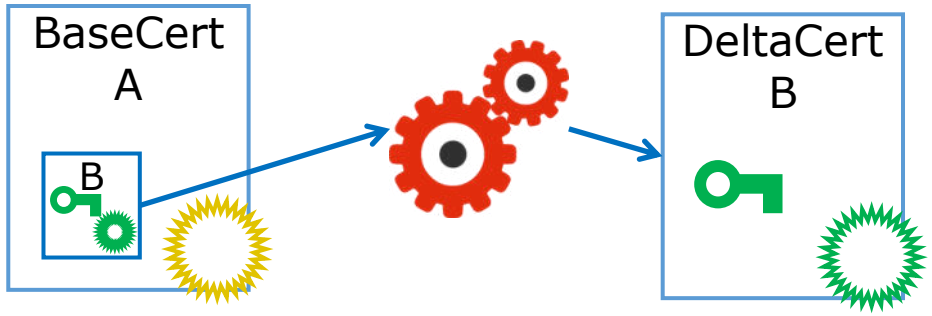


| | | |
|---|---|---|
| Standard | ✓ | ITU-T X.509 (10/2019) \| ISO/IEC 9594-8 |
| No algorithm restriction | ✗ | Only one extension |
| Protocol independent | ✗ | Only X.509 signatures and certificates |
| Security implication | ✗<br>✓ | Non-critical extension has unclear security<br>Critical extension provides complete security |
| Backward compatibility | ✓<br>✗ | Non-critical extension is ignored if unknown<br>Critical extension is rejected |
| Forward compatibility | ✗ | |

# Chameleon Certificates

Reconstruction of additional certificate from Base certificate

- Non-critical X.509v3 extension

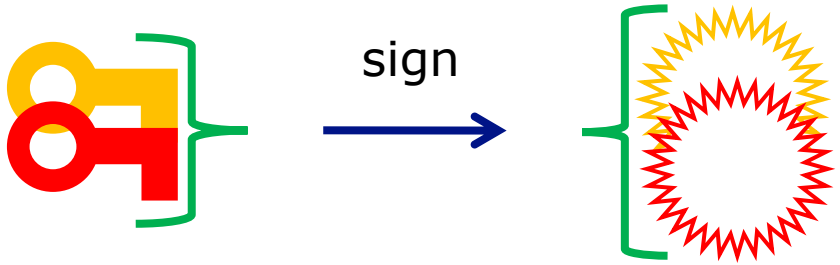



| | | |
|---|---|---|
| Standard | ✘ | draft-bonnell-lamps-chameleon-certs |
| No algorithm restriction | ✘ | Only one extension |
| Protocol independent | ● | Only X.509 signatures and certificates; handling of two PKIs needed |
| Security implication | ✘ | Non-critical extension has unclear security |
| Backward compatibility | ✓ | Non-critical extension is ignored if unknown |
| Forward compatibility | ✘ | |

# Composite Signatures

Algorithm composes Keys and signatures

- Two component algorithms
- Explicit specification of pairs
- Key pair and signature are
- Both must validate (AND construction)

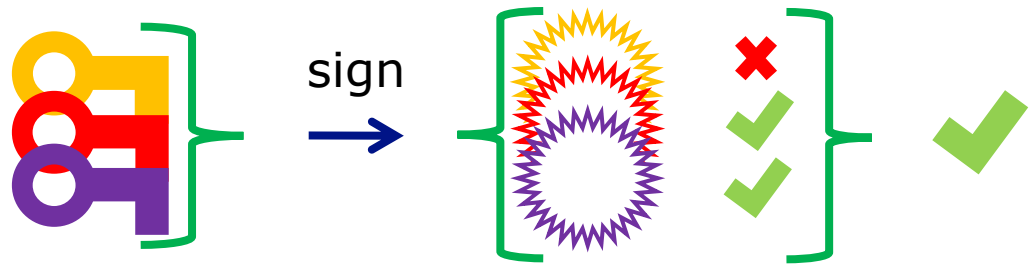



| | | |
|---|---|---|
| Standard | ✘ | draft-ounsworth-pq-composite-sigs |
| No algorithm restriction | ● | Limited predefined pairs, additional definitions possible |
| Protocol independent | ✓ | Transparent to other protocols (X.509, CMS, …) |
| Security implication | ✓ | |
| Backward compatibility | ✘ | |
| Forward compatibility | ✘ | |

# K-of-N Signatures

Algorithm composes keys and signatures

- N component algorithms allowed
- All component signatures are created
- Only K need to validate
- Generic construction



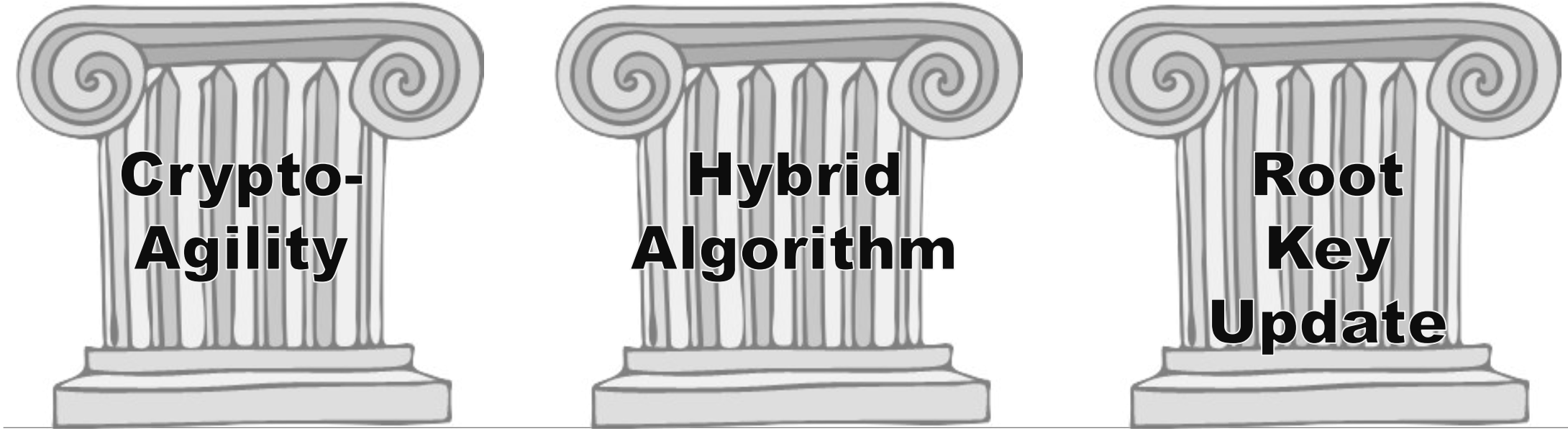

| | | |
|---|---|---|
| Standard | ✘ | draft-pala-klaussner-composite-kofn |
| No algorithm restriction | ✓ | Generic construction allows algorithm combination up to user |
| Protocol independent | ✓ | Transparent to other protocols (X.509, CMS, …) |
| Security implication | ✓ | |
| Backward compatibility | ✘ | |
| Forward compatibility | ✓ | Unknown components are ignored |

# The Hybrid Schemes Zoo

| | Related Certificates | Isara Catalyst | Chameleon Certificates | Composite Signatures | K-of-N Signatures |
|---|---|---|---|---|---|
| Standard | ● | ✓ | ✗ | ✗ | ✗ |
| No algorithm restriction | ✓ | ✗ | ✗ | ● | ✓ |
| Protocol independent | ✗ | ✗ | ✗ | ✓ | ✓ |
| Security implication | ✗ | ✗<br>✓ | ✗ | ✓ | ✓ |
| Backward compatibility | ✓ | ✓<br>✗ | ✓ | ✗ | ✗ |
| Forward compatibility | ✗ | ✗ | ✗ | ✗ | ✓ |

# The Agile PKI

*Automated, flexible processes for PKIs to support switching of keys and algorithms without interruption of security and operation.*



# Crypto-Agility

(1) the ability for machines to **select their security algorithms** in real time and based on their combined security functions;

(2) the ability to **add new cryptographic features or algorithms** to existing hardware or software, resulting in new, stronger security features;

and (3) the ability to gracefully **retire cryptographic systems** that have become either vulnerable or obsolete.

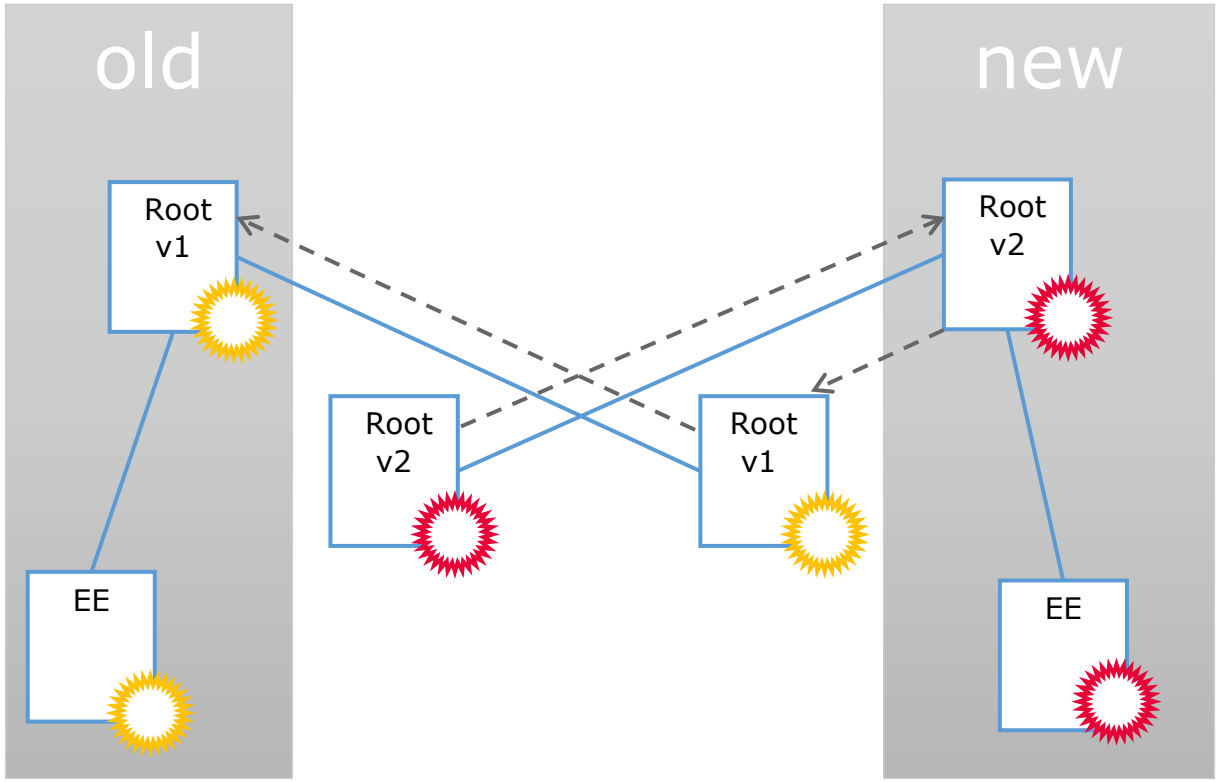
*Source: McKay in Anne Frances Johnson and Lynette I. Millett (Eds.). 2017. Cryptographic Agility and Interoperability: Proceedings of a Workshop. The National Academies Press, Washington, DC. https://doi.org/10.17226/24636*

# Root Key Update

cross-certification of root certificates

- forward compatibility:
  old clients trust new root

- automated migration:
  install new root



# Key takeaway points

- Todays digital signatures have legal effect beyond CRQC
- No drop in replacement of traditional algorithms
- Agile PKI needed
  - Hybrid Algorithms
  - Crypto agile system components
  - Root key update

**Jan Klaußner**
Senior Product Architect
Email: jan.klaussner@bdr.de
Mobile: + 49 (0) 151 5600 1986

# Thank You.

# Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia