bundesdruckerei.

Why Agile PKI

PKI in the Age of PQC

Date	12.10.2023
Location	CA Day 2023, Vienna
Author	Dr. Kim Nguyen & Jan Klaussner

The NIST PQC Competition

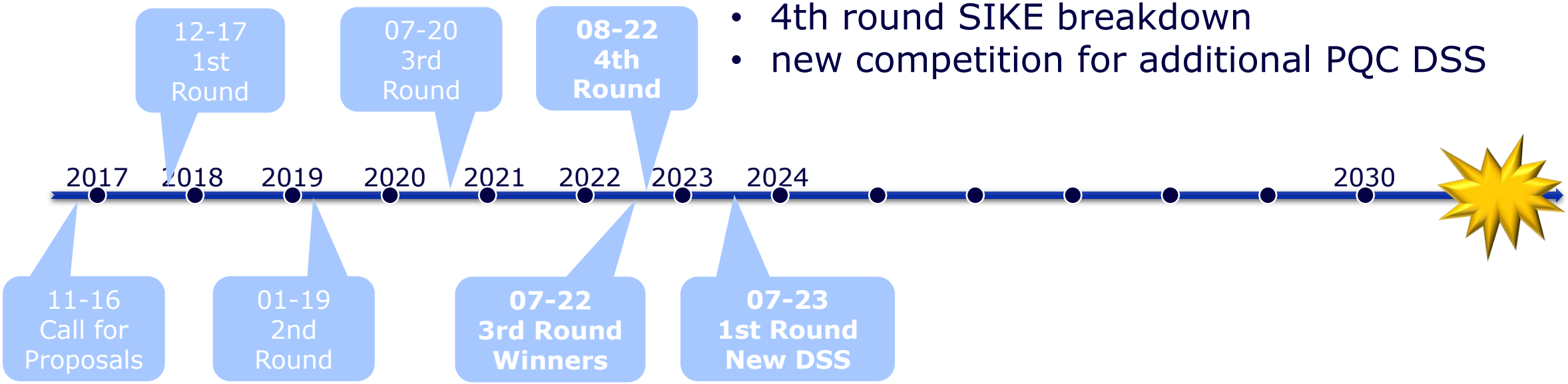
There ain't no easy way

- supposed final round
- 7 finalists, 8 alternates
- 2022 breakdown of finalist Rainbow

The NIST PQC Competition

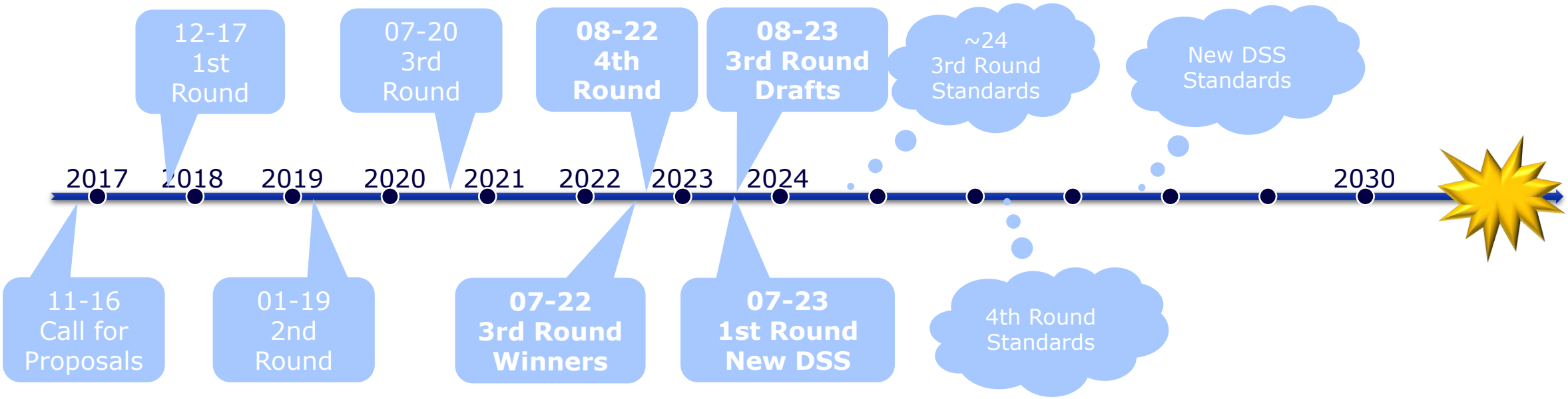
Surprise, surprise

- winners were announced (1 KEM, 3 DSS)
- 4 KEMs to 4th round
- 4th round SIKE breakdown
- new competition for additional PQC DSS



The NIST PQC Competition

And it goes on…



State of PQC

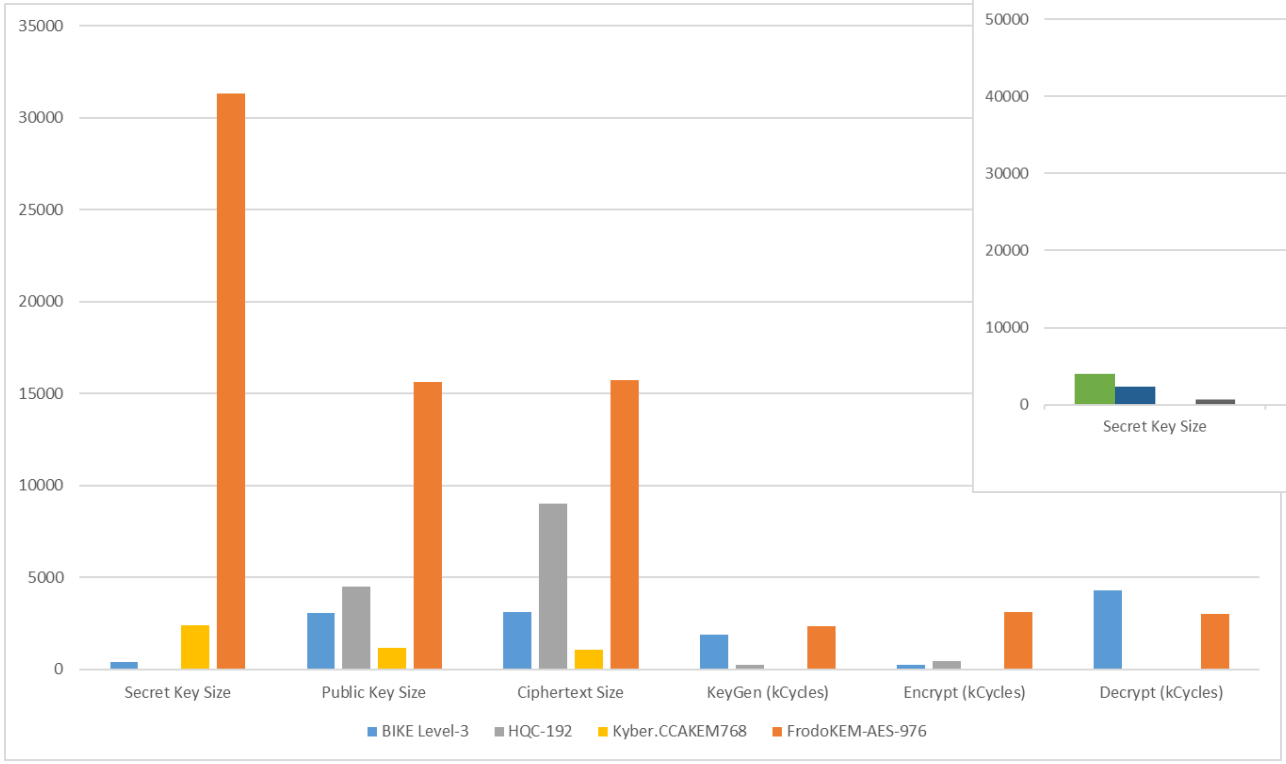
Lattices!

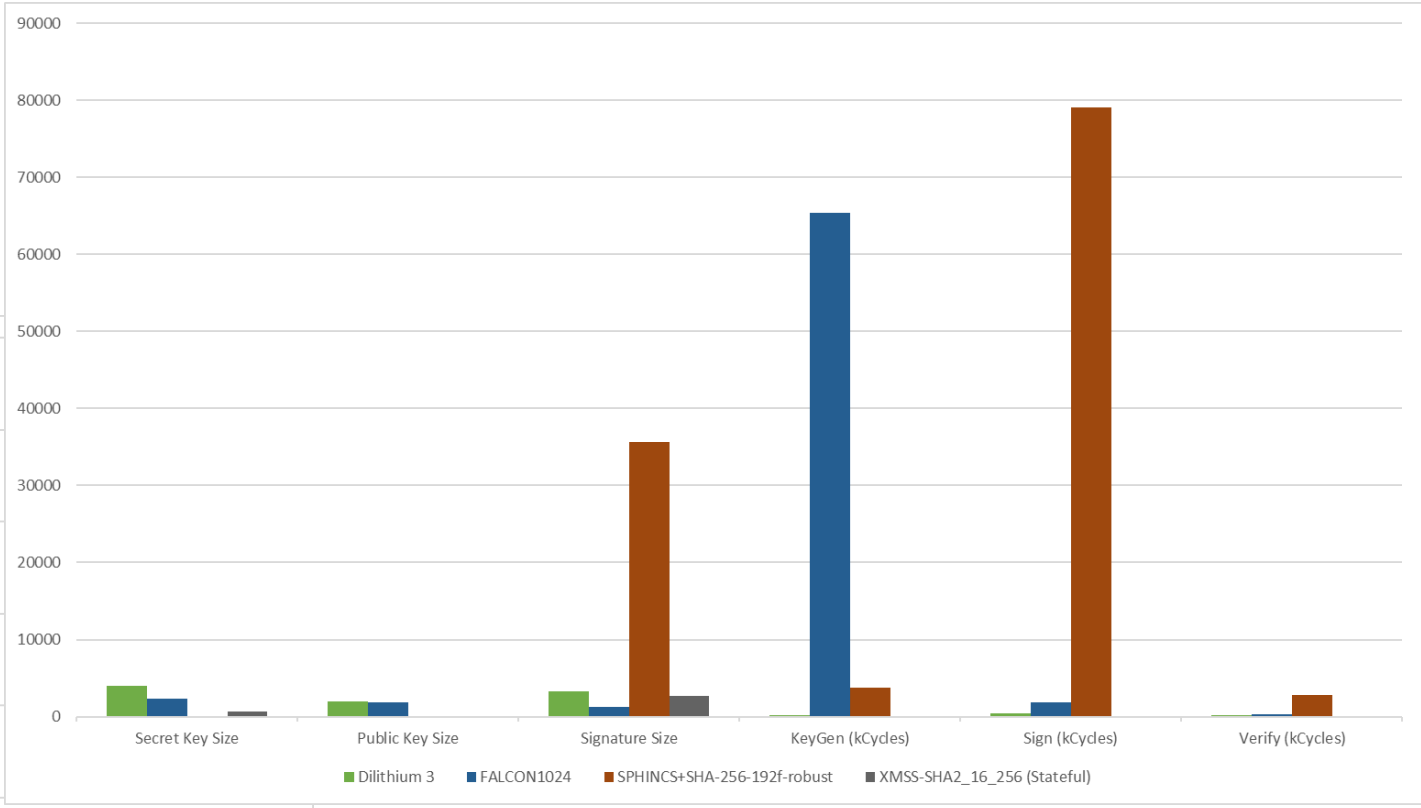
	Standard	Draft	4th round	Non-NIST	New DSS
KEM		▲ Kyber	● Bike ● HQC ● Classic McEliece	▲ FrodoKEM ▲ NTRU	
DSS	♦ XMSS ♦ LMS	▲ Dilithium ▲ Falcon ♦ Sphincs+			▲ 7 ● 6 ■ 1 ✱ 10 ❖ 7 ◈ 4 ⁂ 5

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

State of PQC

No one fits all
… and all worse than RSA/EC





PQCs – What can we expect?

- security issues
  - see SIKE, Rainbow
- improvements
  - see switch RSA PKCS1.5 to PSS
- bugs
  - see ROCA attack on RSA
  - see ECDSA „Psychic Signatures“
- more PQCs
  - NISTs 4th round an new competition for more PQC signatures

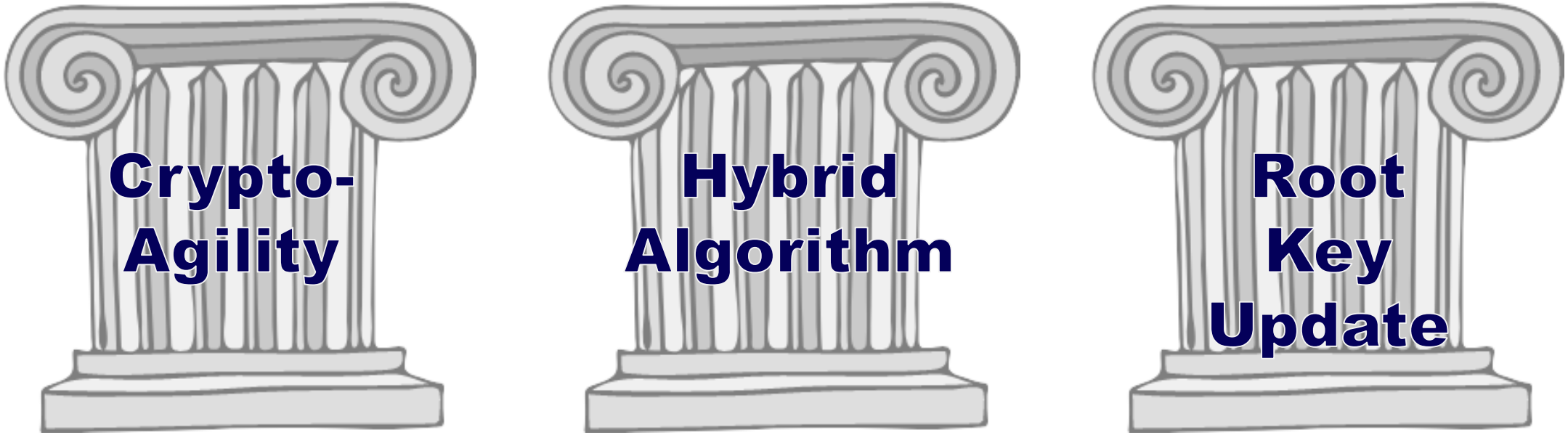
High probability of…

1. **need for short term switching of keys and algorithms**
2. **security gaps due to weak keys or algorithms**

A challenge for complex distributed systems.

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;

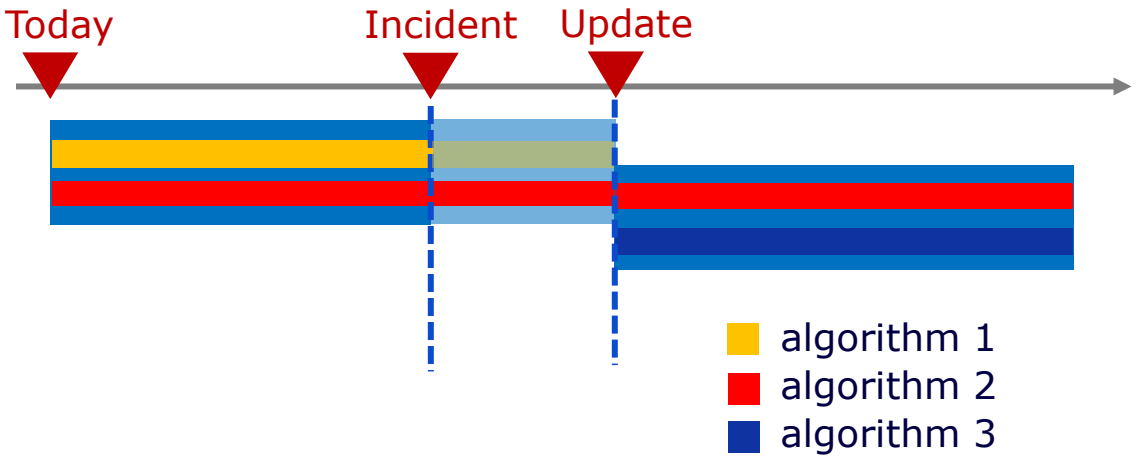
and (3) the ability to gracefully **retire cryptographic systems** that have become either vulnerable or obsolete.

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

Hybrid Algorithm: Intelligent Composed Algorithm

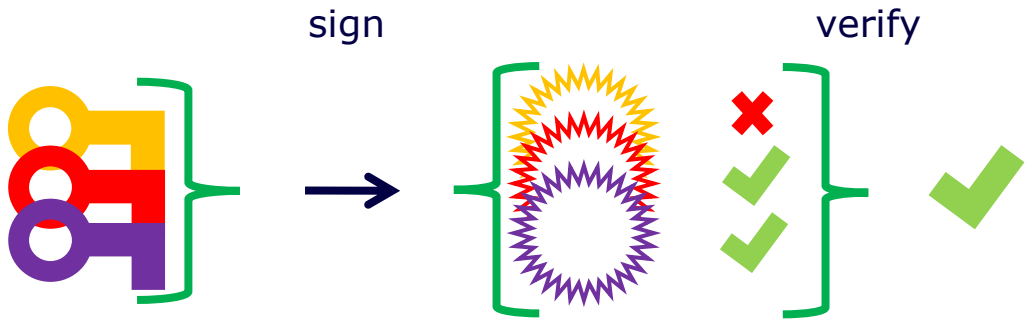
hybrid keys/algorithm

- bridges security gap if one fails
- works for keys and algorithms
- universal: requires no change to protocols



K-of-N construction

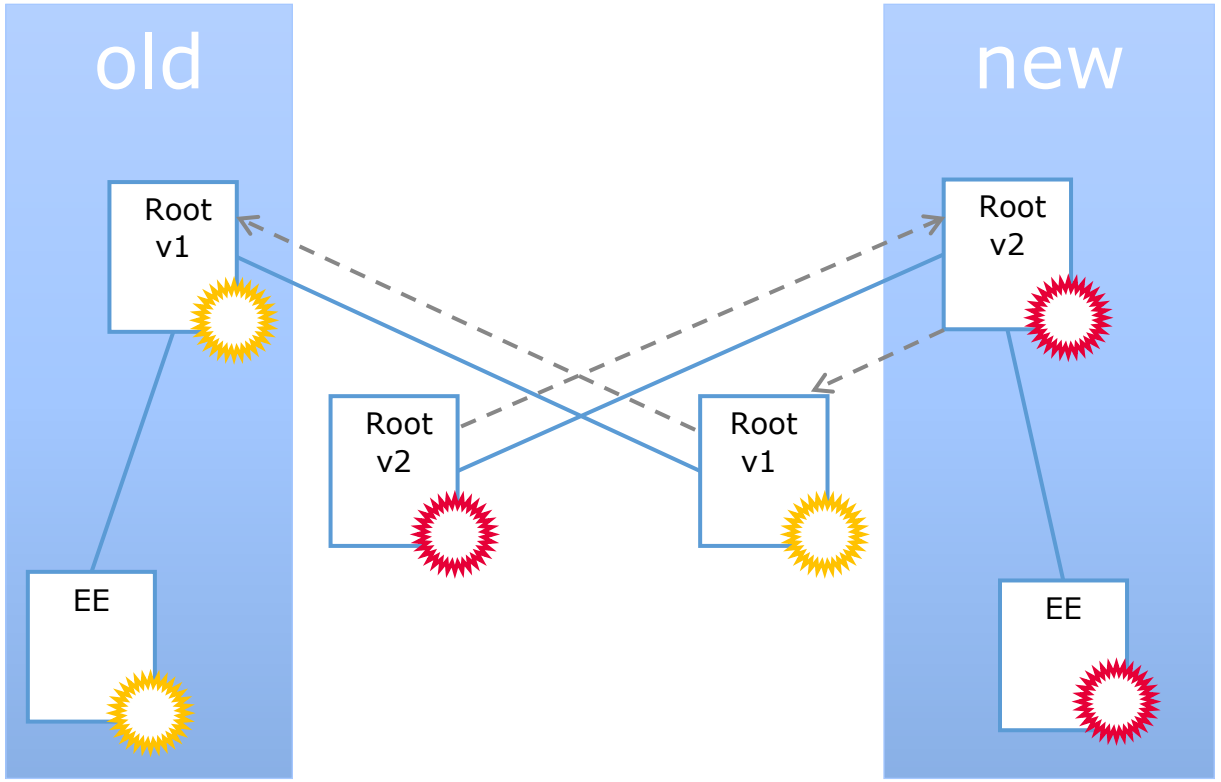
- only K of N signatures must verify
- provides backwards compatibility
- retains security in case of broken keys/algorithms



Root Key Update

cross-certification of root certificates

- forward compatibility:
  old clients trust new root
- automated migration:
  install new root



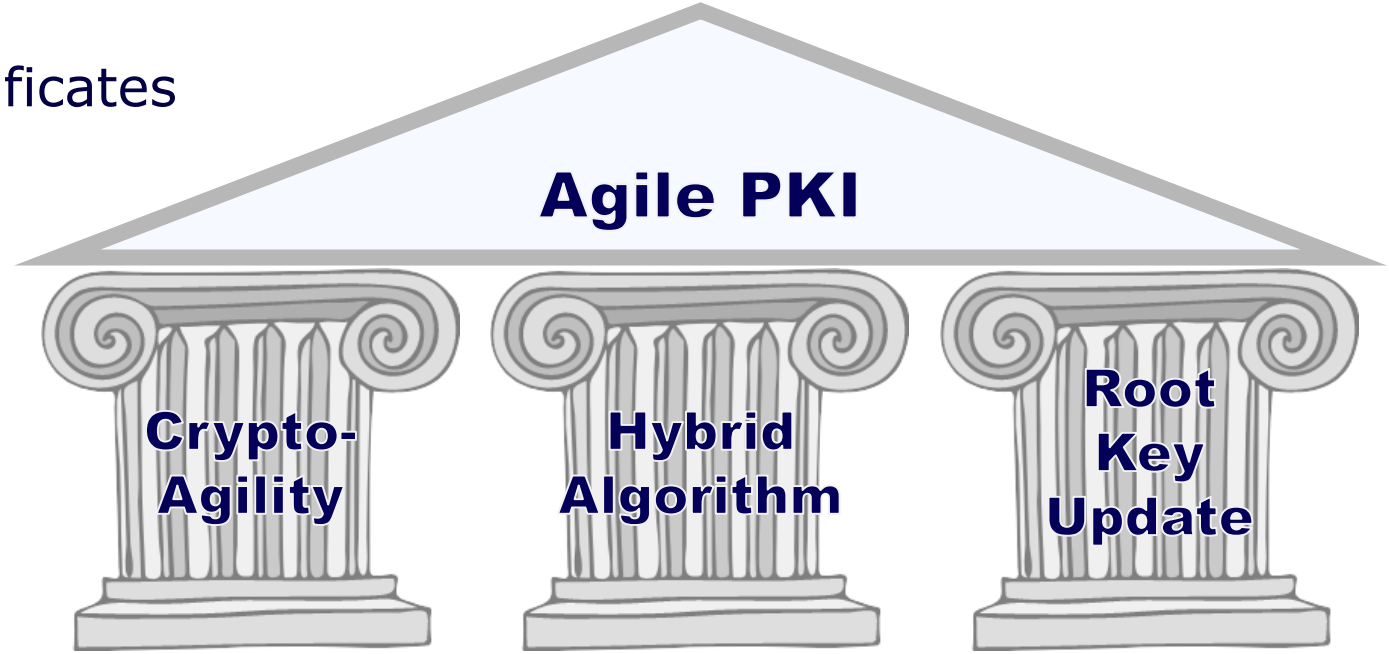
Conclusion

- Agile PKI protects against uncertainties of PQC age

- Hybrid Algorithm
  - more efficient than Parallel PKIs
  - more universal than Hybrid Certificates

- Standardization on the way
  - IETF, ISO

- Projects
  - FLOQI, QuGov, …



Thank you.

Dr. Kim Nguyen

D-Trust GmbH/
Bundesdruckerei GmbH
E-Mail: kim.nguyen@bdr.de

Jan Klaussner

D-Trust GmbH/
Bundesdruckerei GmbH
E-Mail: jan.klaussner@bdr.de

Part of the Bundesdruckerei Group