# TeleTrusT-EBCA "PKI-Workshop" 2023

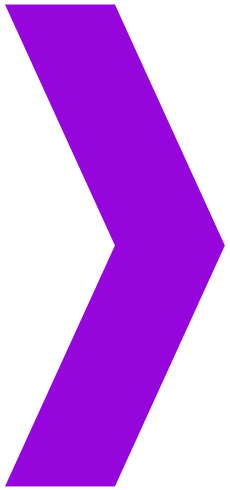
**Berlin, 21.09.2023**

# "A new hope: How Agile PKIs allow Efficient Migrations to new Algorithms"

**Jan Klaußner, D-Trust**

# 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 new competition for more PQC signatures



**High probability of…**

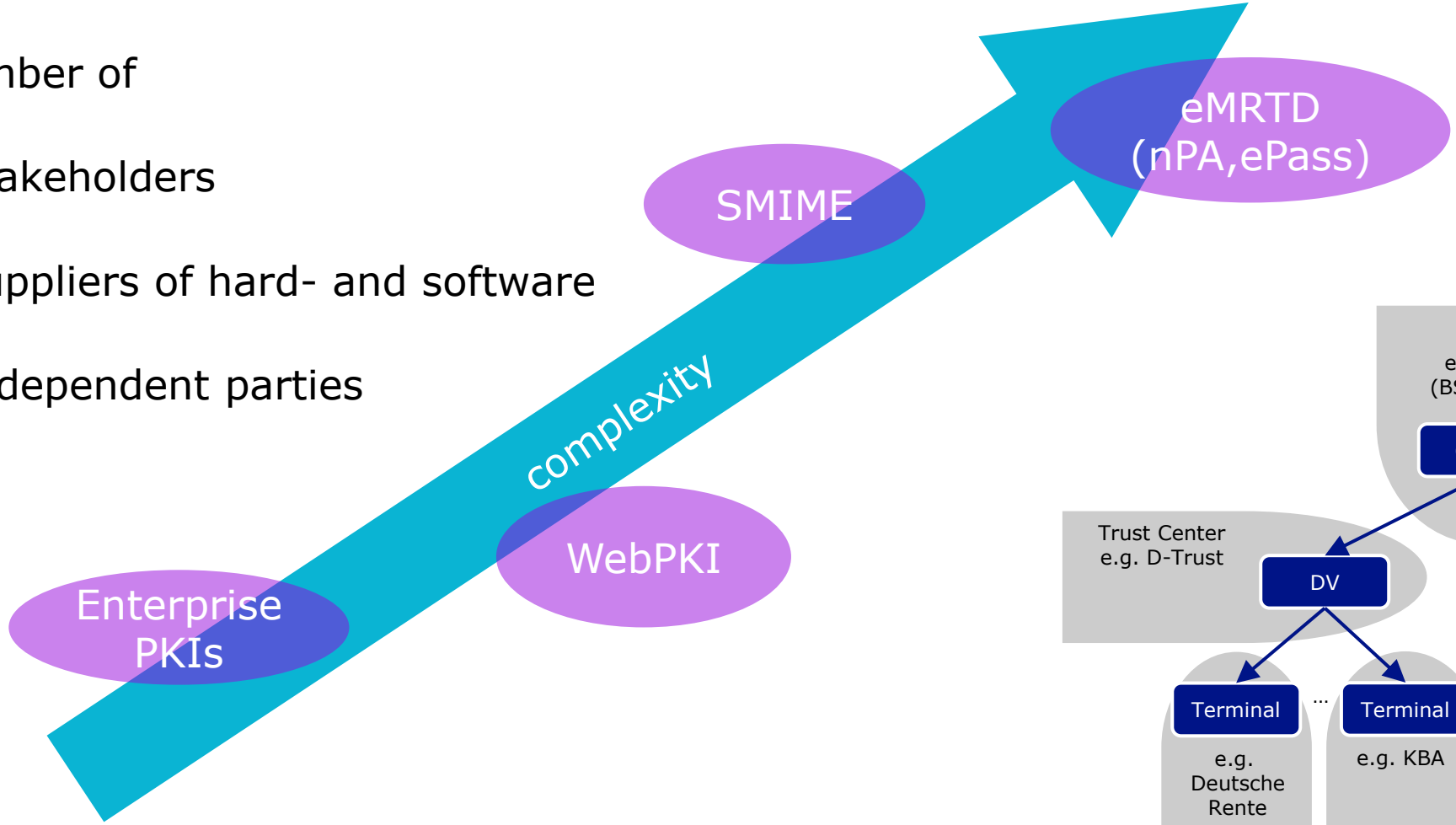
1. **need for short term switching of keys and algorithms**
2. **security gaps due to weak keys or algorithms**

**A challenge for complex distributed systems.**

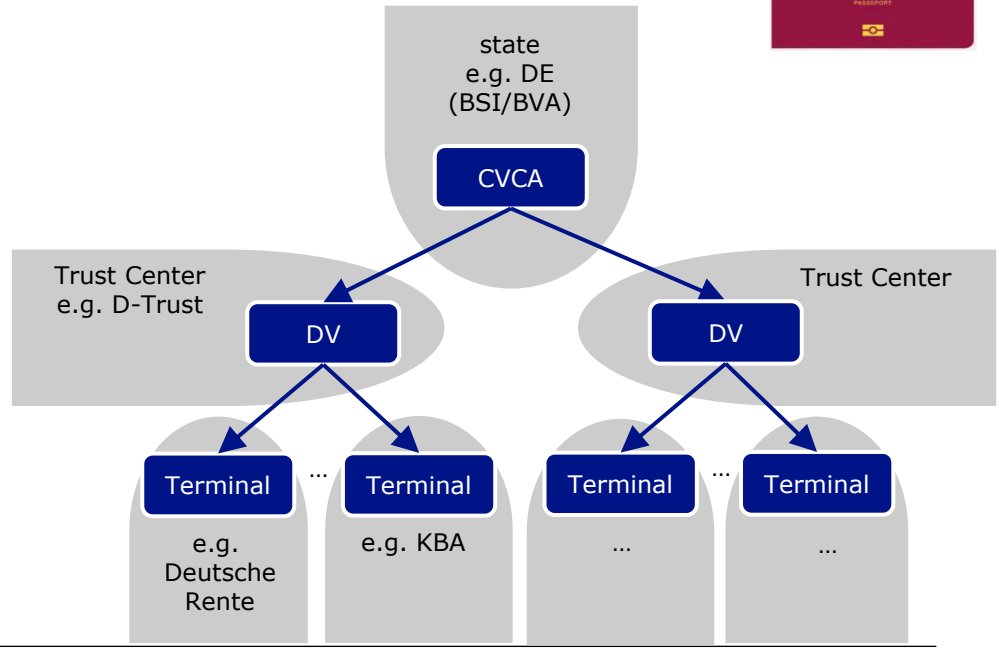
# Complexity of PKIs

number of

- stakeholders
- suppliers of hard- and software
- independent parties



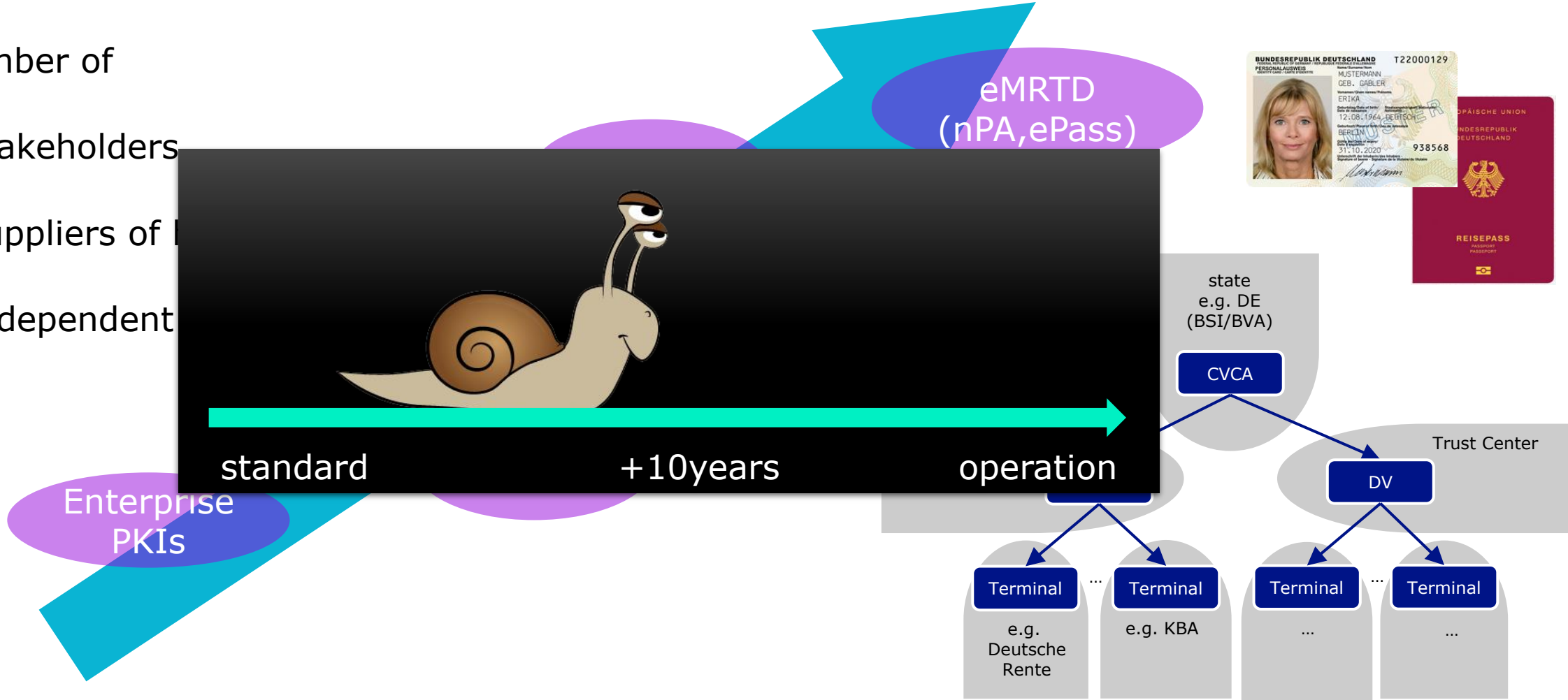




# Complexity of PKIs

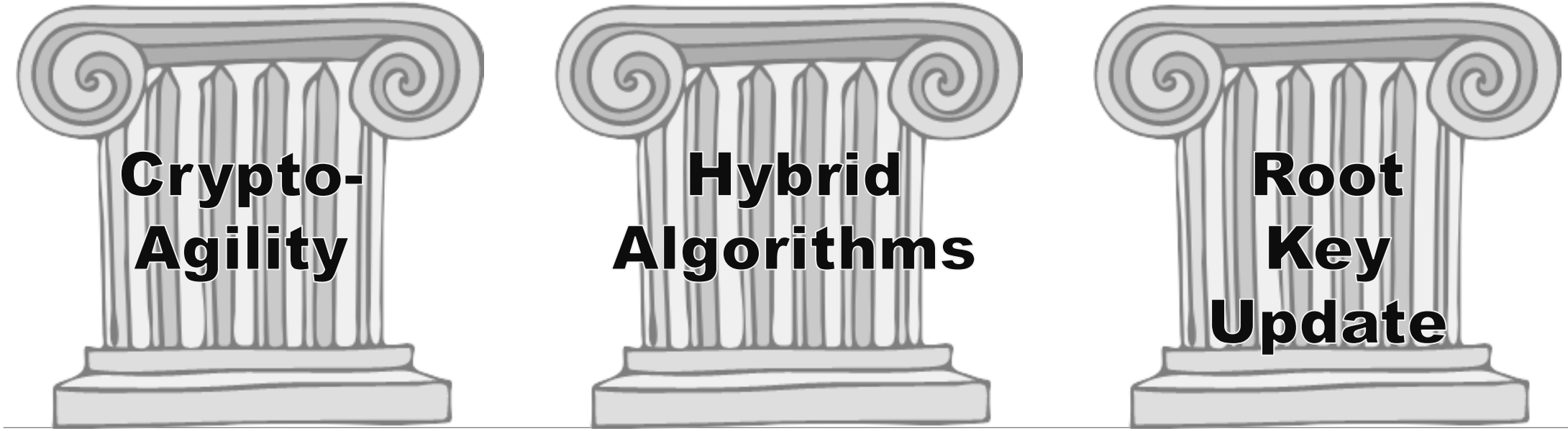
number of

- stakeholders
- suppliers of
- independent



# 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;

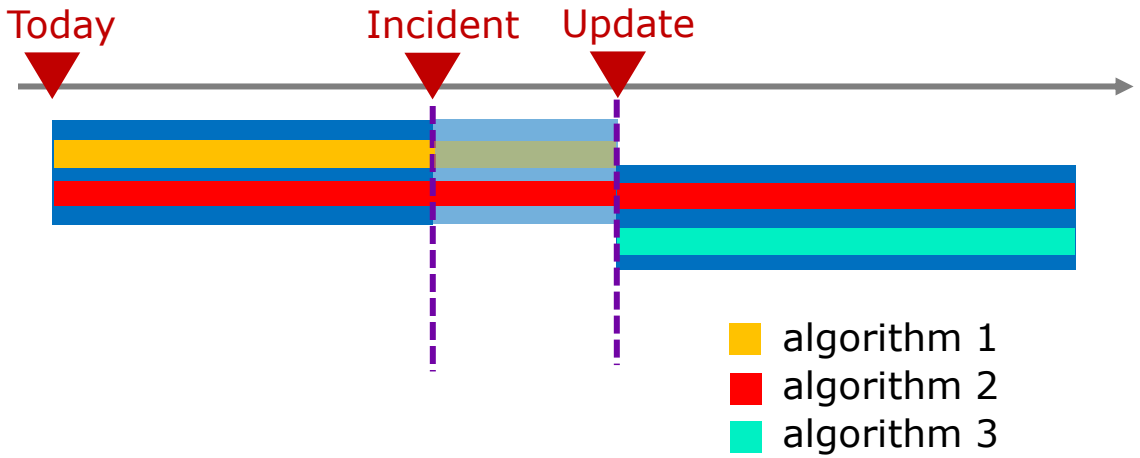
and (3) the ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete.

*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 Algorithms

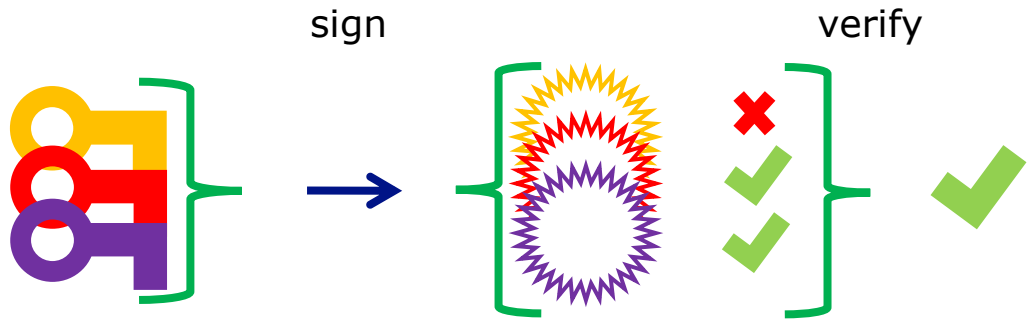
hybrid keys/algorithms

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




K-of-N construction

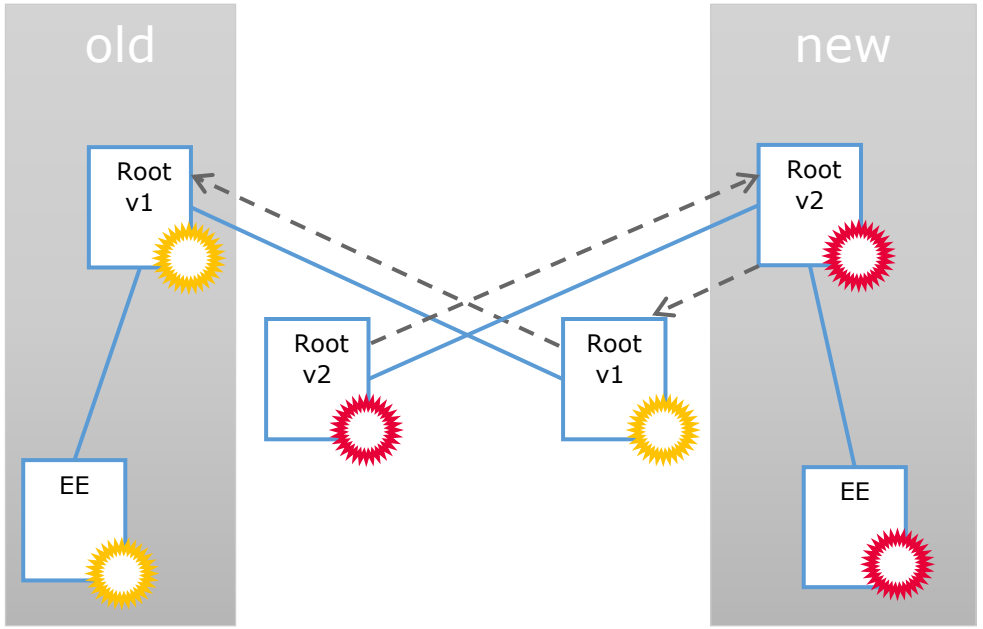
- only K of N signatures must verify
- provides backwards compatibility
- retains security in case of broken keys/algorithms



# Root Key Update

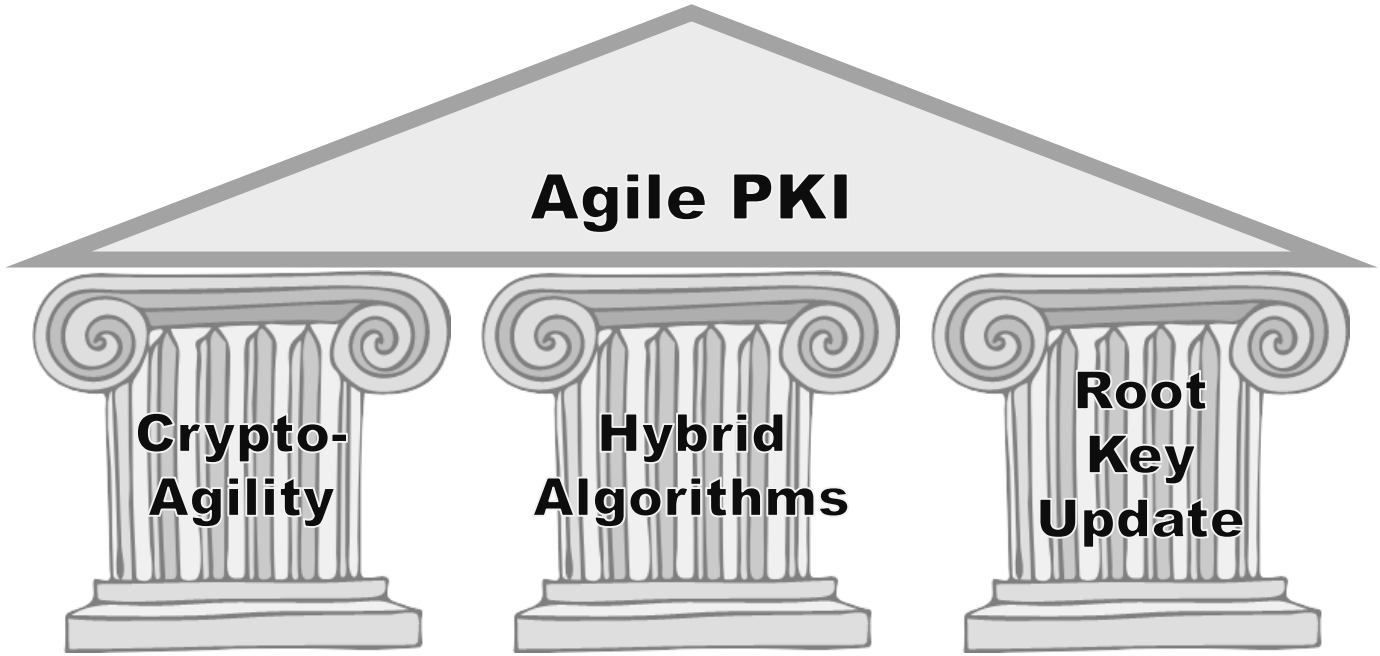
cross-certification of root certificates

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



# Conclusion

- agility for PKIs is possible
- standardization efforts
  - IETF, ISO
- Projects
  - FLOQI, QuGov, …



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

# Thank you!