How will Post Quantum Cryptographic effect Contactless Travel in Entry-Exit Solution?

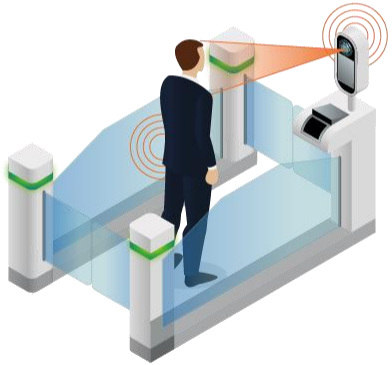
Lutz Richter
Mühlbauer Group

Current Situation

Current Seamless Travel

VERIFICATION

AUTHENTICATION

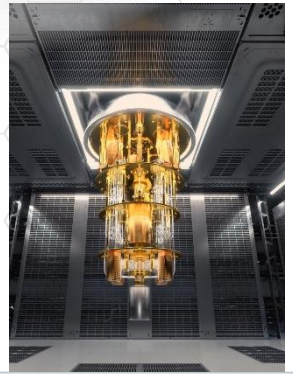


BOARDING

Challenges: Policy Contradictions

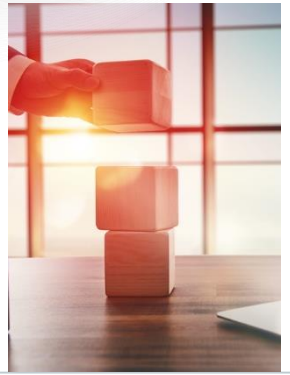
Challenges

POST QUANTUM CRYPTOGRAPHY



CYBER SECURITY

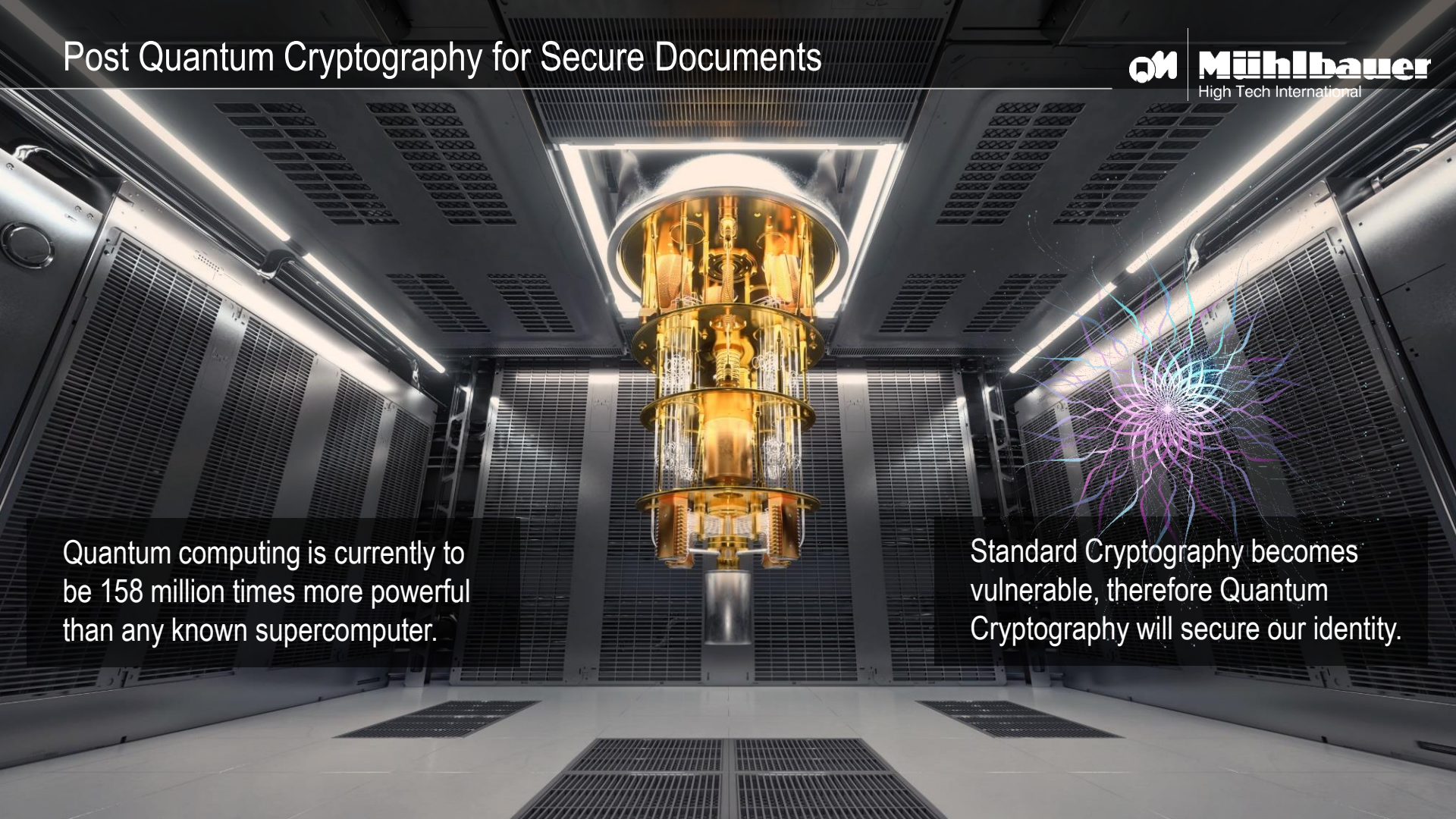
ARCHITECTURE GUIDELINES



SUSTAINABILITY

Post Quantum Cryptography for Secure Documents

Mühlbauer
High Tech International

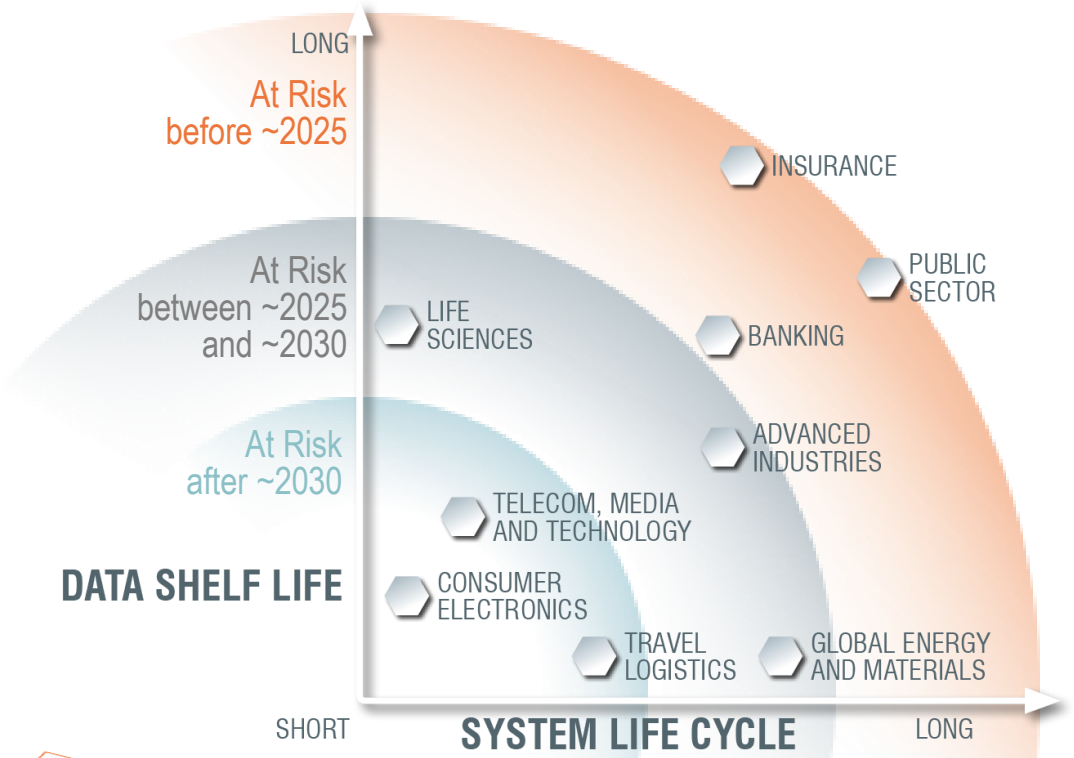


Quantum computing is currently to be 158 million times more powerful than any known supercomputer.

Standard Cryptography becomes vulnerable, therefore Quantum Cryptography will secure our identity.

Post Quantum Algorithms selected by NIST

Risk of Quantum Powered Attack by Industry



Encryption: **CRYSTALS-Kyber**

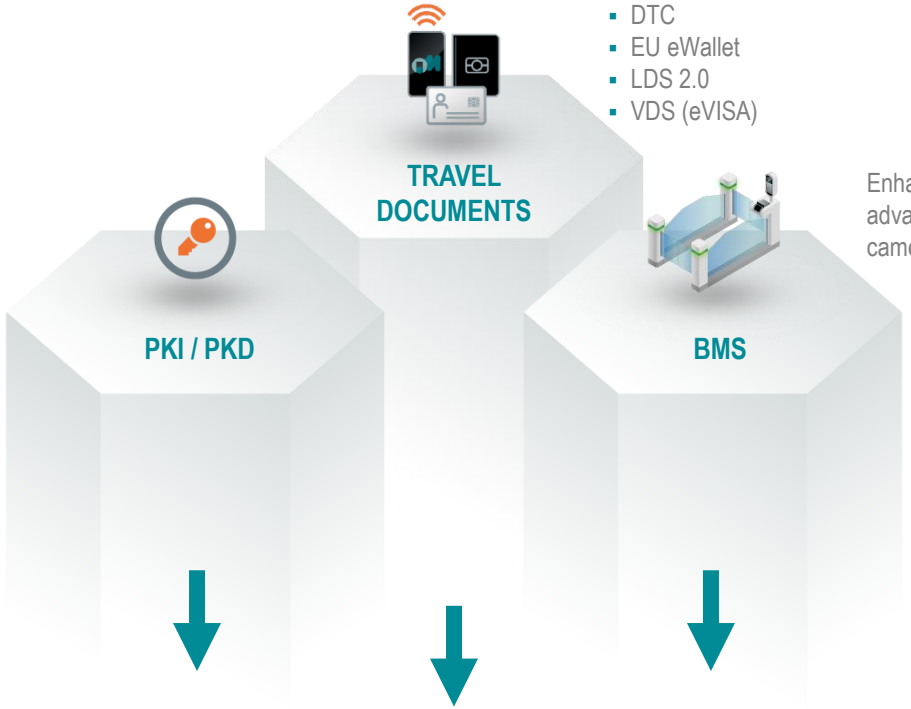
Digital Signature: **CRYSTALS-Dilithium, FALCON** and **SPHINCS+**

according to www.cryptomathic.com

Solution Concept

Essential Immigration Components

Immigration Pillars



- DTC
- EU eWallet
- LDS 2.0
- VDS (eVISA)

Enhanced with advanced biometric cameras & readers

Integrated to Contactless Travel System (Airline/Airport)
as recommended by IATA

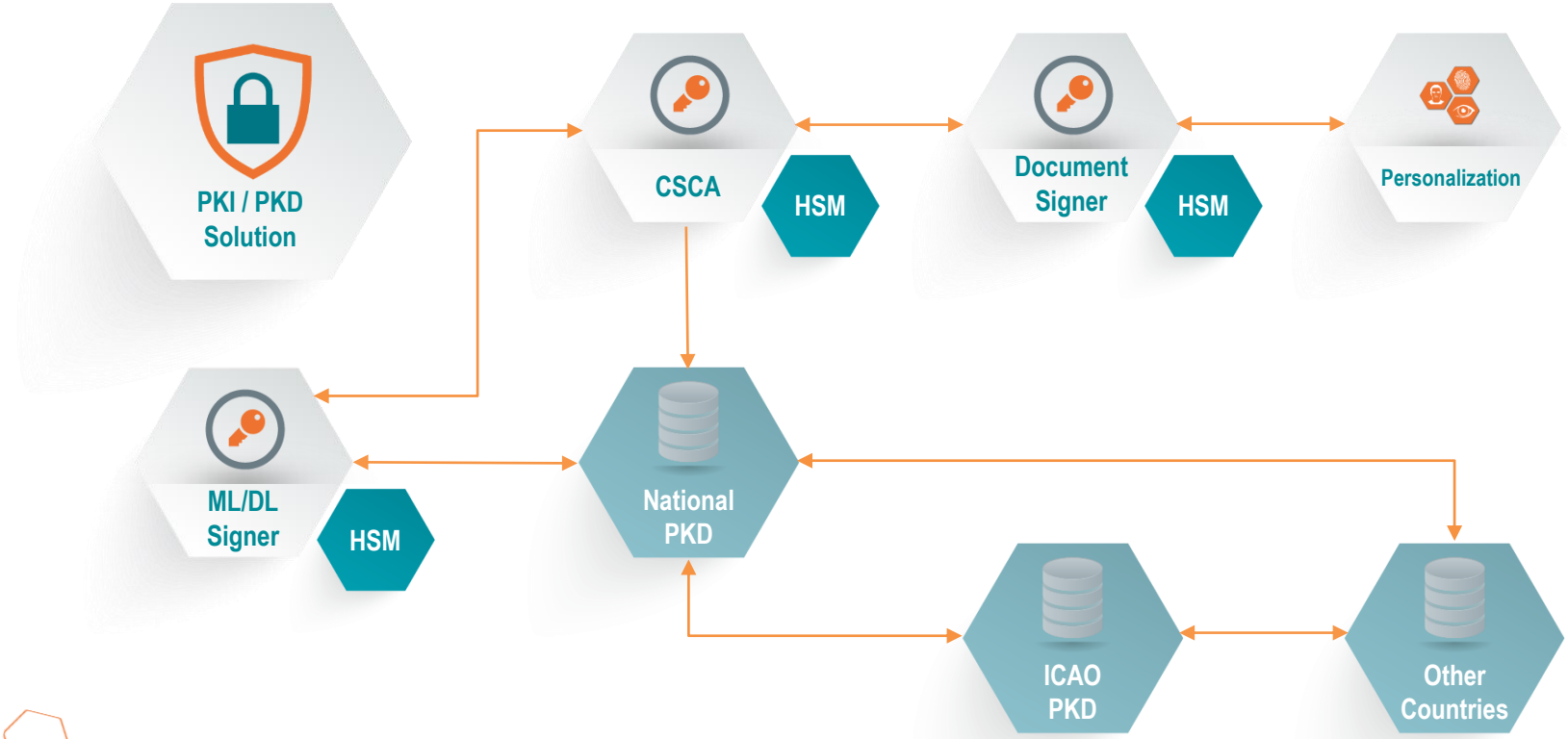
Diversity of Travel Documents

ISO 18013-5
ISO 23220

DTC
LDS 2.0

Trusted eServices
eIDAS

Public Key Infrastructure / Public Key Directory



Seamless Travel: Next Chapter

Summery

- Upgrade digital and mobile Documents with PQC proven Chip and Secure Element
- Upgrade Personalization systems from Machine to issuing systems to support PQC
- Upgrade PKI including Inspectionssystems mainly with new generation of HSM
- Upgrade use algorithm for secure communications between involved system components
- Plan a new proejct from now which shall run over next 10 years to be ready for PQC

Mühlbauer
High Tech International

Thank you for your attention.