Post-Quantum

Cryptography Conference

Quantum Key Distribution – What is done and what is to come

Quantum Key Distribution (QKD) systems promise to be a provably secure key transfer between two peers based on quantum effects that can meet the requirements for a quantum-secure communication in the post-quantum-threat era. For countries as well as for companies worldwide it is essential to keep track with the fast-changing developments on secure communication. The development and application of new cryptographic methods and key exchanges is immanent. We at Bundesdruckerei GmbH, owned by the German Federal Ministry of Finance, had the chance to examine and test several QKD systems and their peripherals within the Qu-Gov project. This talk will show the delimitation of QKD to PQC but also the potential use of a hybrid system and shares our experience with such QKD-systems regarding their performance, use in existing infrastructure, caveats and limits as well as open issues that we see as crucial.

Jan Klaußner

Senior Product Architect at Bundesdruckerei GmbH

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

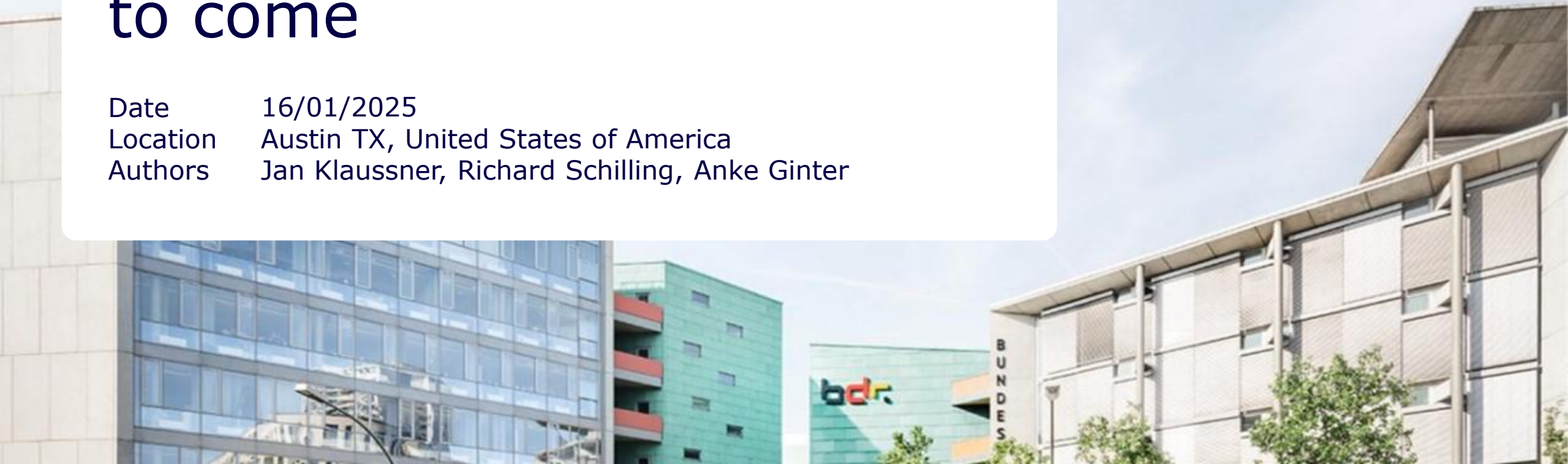
January 15 and 16, 2025 - Austin, TX (US) | Online

bundesdruckerei.

Quantum Key Distribution

What is done and what is to come

Date 16/01/2025
Location Austin TX, United States of America
Authors Jan Klaussner, Richard Schilling, Anke Ginter



bundesdruckerei.

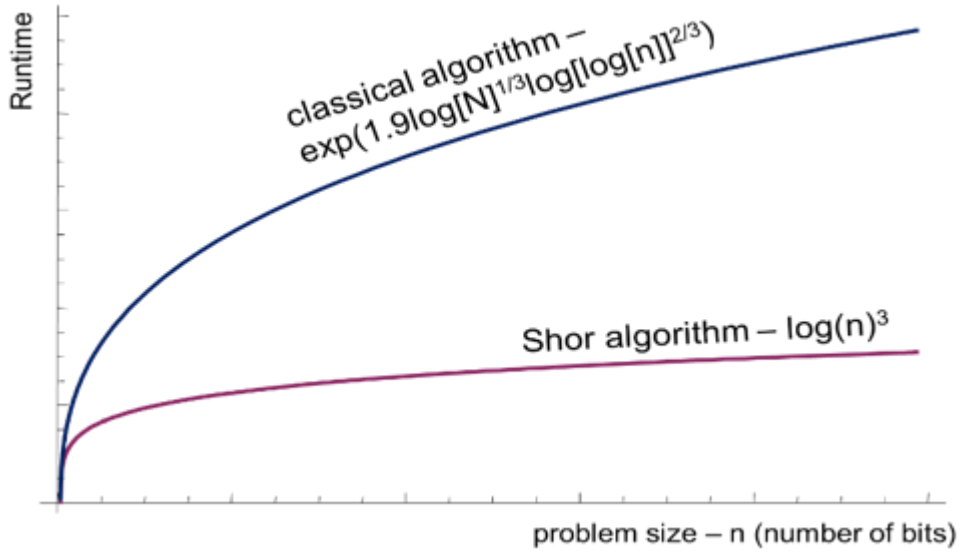
Security in the quantum era

Quantum technologies

- Principles are long known but access and usage new
- Highly disruptive and very dynamic development
- We need to prepare now – opportunity to shape future
- Quantum world is different – we need to thing different to see risk and benefits
- New approaches, research and development necessary

PQC as first step

- Methods based on mathematical assumptions
- Not enough experience with side channel and other attacks
- AI and quantum may change a lot
- Other security layers will be necessary



Dewes, A. 2014: Let's Build a Quantum Computer!

Functionality

Quantum Key Distribution

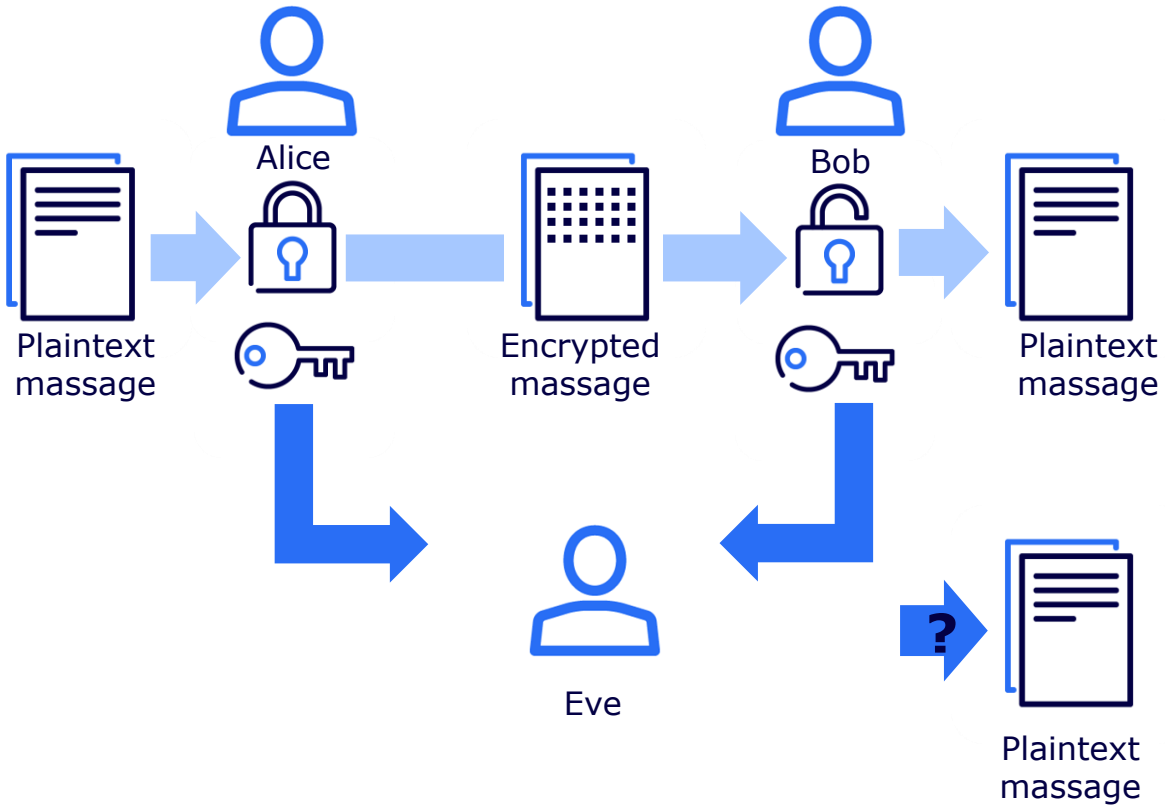
bundesdruckerei.

Quantum Key Distribution (QKD)
Security based on physical principles

Task
- Generate and distribute secure keys
- Keys used for symmetric encryption

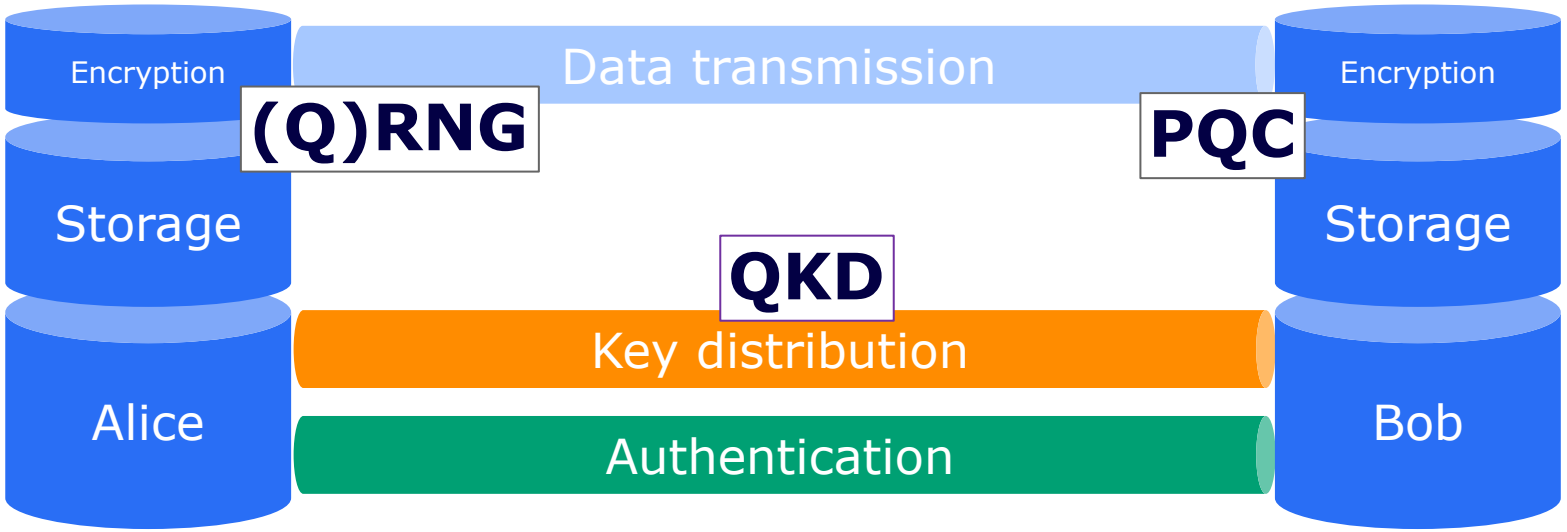
Idea of quantum states
- No perfect cloning of quantum states possible
- Eavesdropping will be noticed
- Security based on physical laws instead of mathematical assumptions

QKD is only one part of the whole chain
- Communication is a classical process
- PQC and crypto agility is needed additionally



bundesdruckerei.

QKD is only part of the chain



QKD for distributing secure symmetric keys

Data transmission is still a classical process

A classical authenticated channel needed -> ID Systems

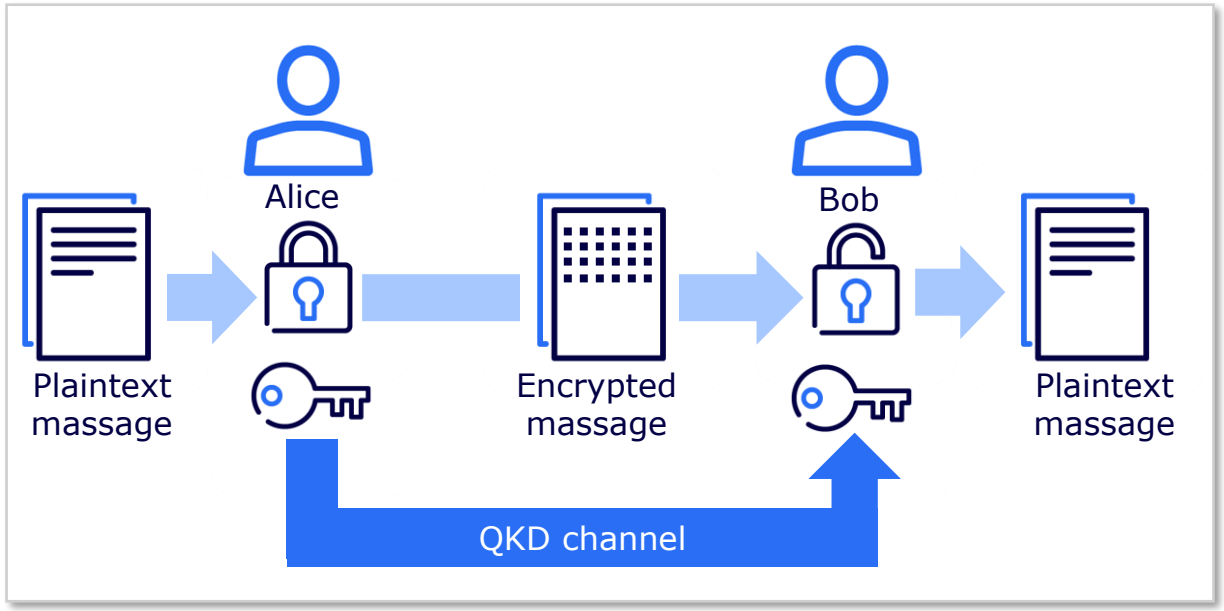
All other parts needed to be classically secured -> PQC, crypto agility

How to implement QKD?
Using quantum effects for security

Implementation of QKD protocols

- Additional quantum channel between Alice and Bob (optical fiber)
- Key material (bits) encoded into quantum states
- Use (Q)RNG for randomness for bits and encoding
- Distribute quantum states via optical fiber (photons)
- Classical post processing: Check error rate and discard non useful bits in protocol channel
- Remaining bits used for a secure key if error rate under threshold

Long time security: Key can not be calculated after procedure is finished



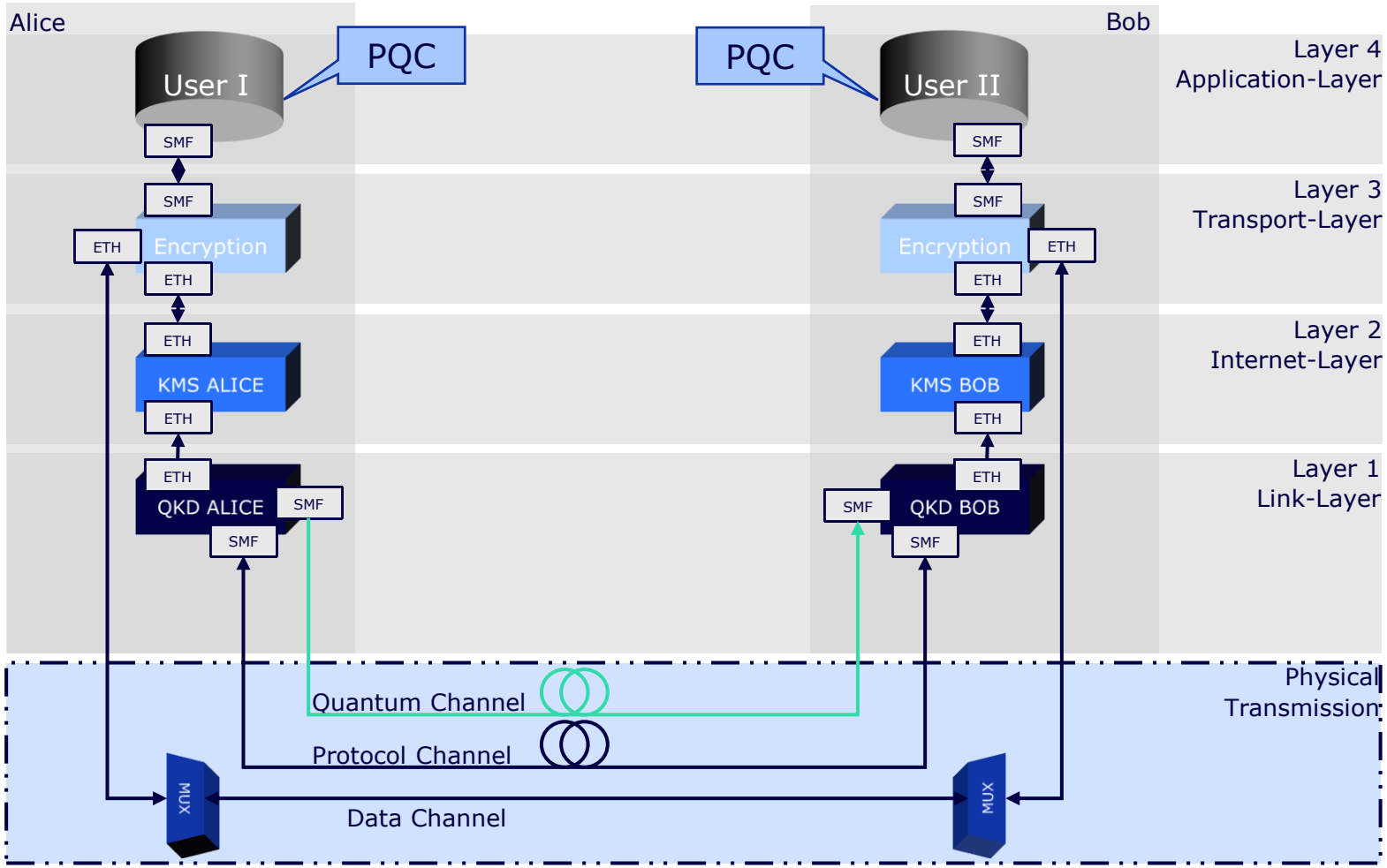
Network Integration

QKD in existing Infrastructures

Integration into Network Infrastructure

Requirements for the architecture:

- Interfaces compatible with QKD-standards (e.g., ETSI GS QKD 014)
- Optical fibres for connection
- QKD-Hardware: assigned sender and receiver



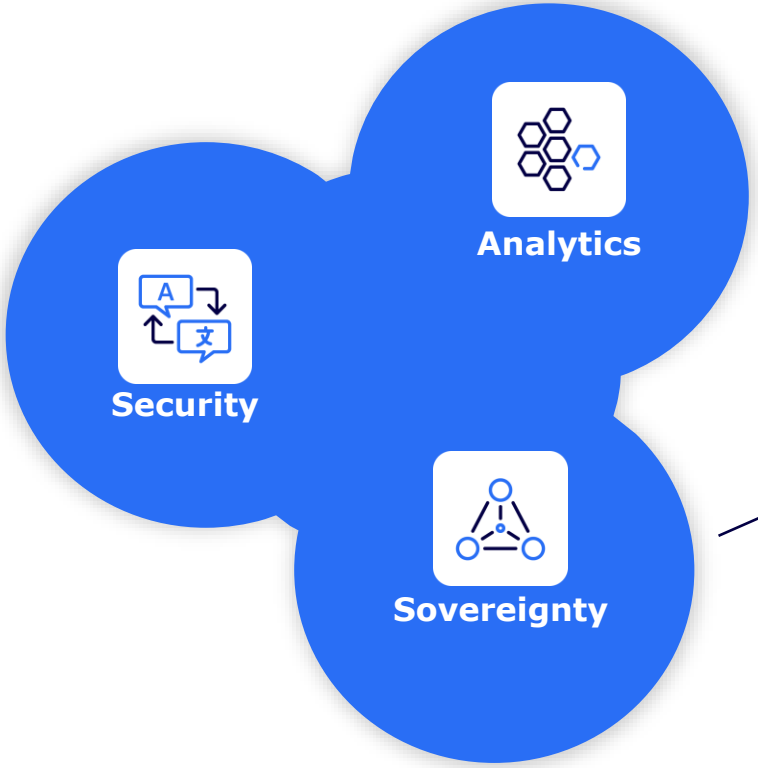
Legend:
SMF – Singlemode Fiber
ETH – Ethernet Port
KMS – Key Management System
(DE)MUX – (De)Multiplexer
⟷ - Physical Connection

QKD@bdr

Start Quantum Innovation

Qu-Gov: Start quantum innovation
Quantum technologies for federal administration

Bundesministerium der Finanzen & bdr.

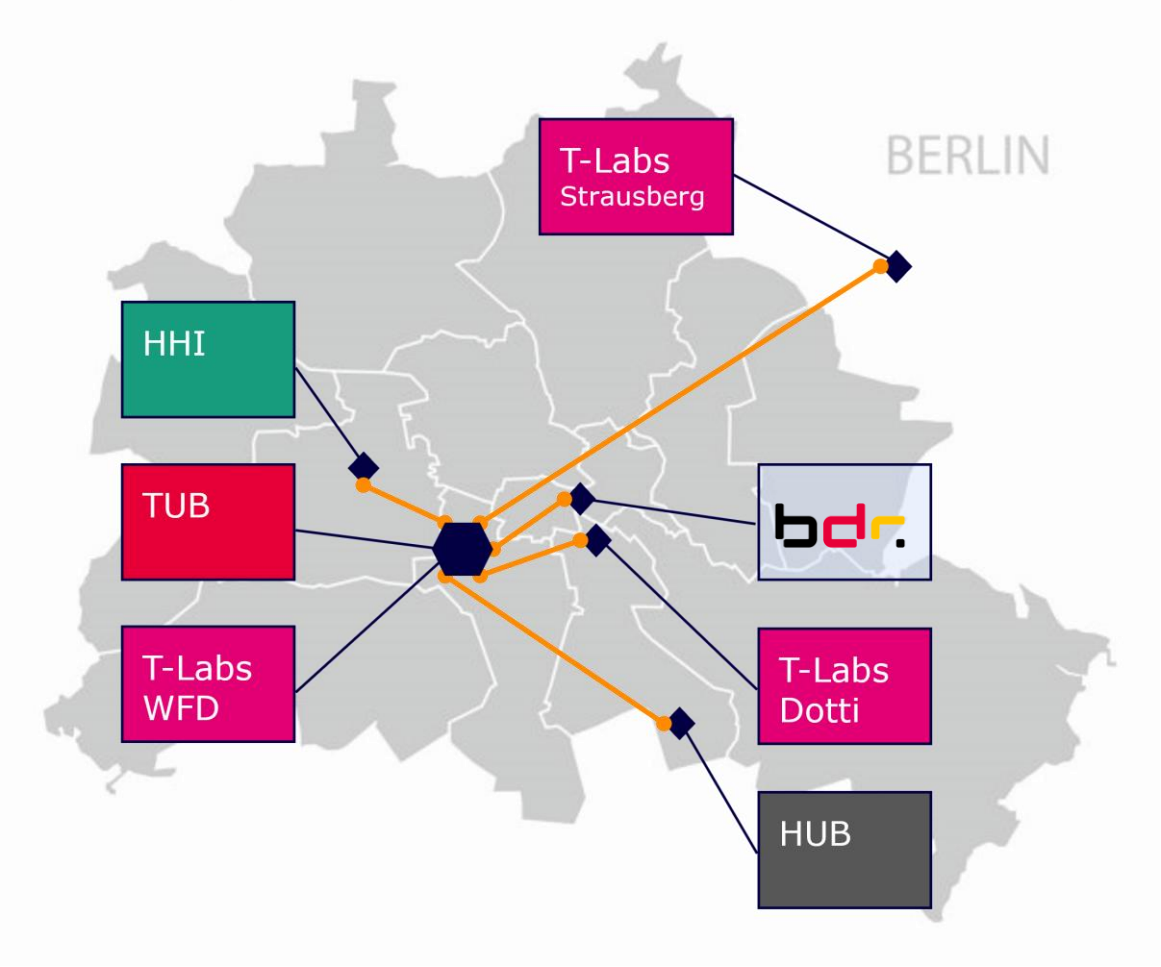


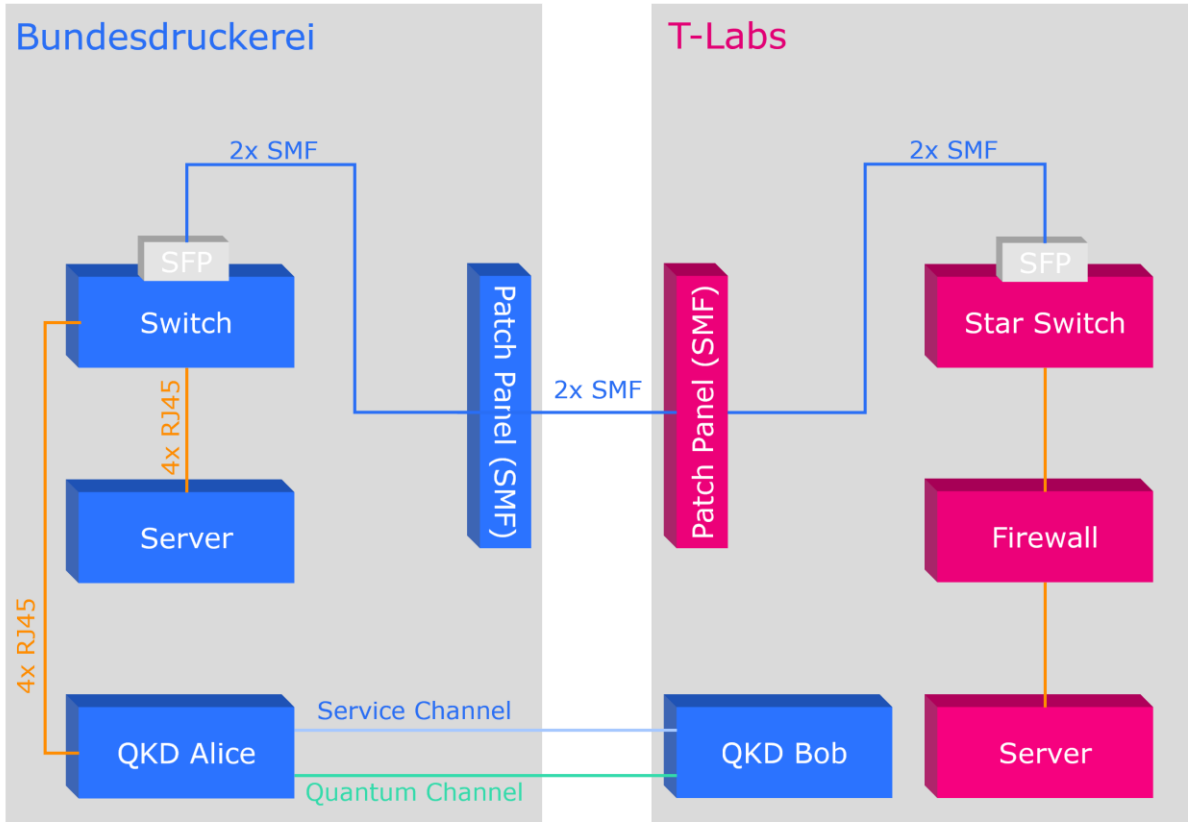
Security
- Crypto-agility / PQC
- Quantum Cryptography
- Quantum information
- Risks and benefits

Quantum Analytics
- QML and optimization
- Synthetic data
- Modelling complex systems e.g. customs and federal budget

Quantum Sovereignty
- Quantum cloud services
- Integration of quantum HW
- Upskill in quantum topics
- Development of use-cases

bdr QKD-Testbed in Berlin





Hybrid System

QKD + PQC

bundesdruckerei.

Hybrid System: QKD + PQC

QKD

- Key distribution of symmetric keys
- Eavesdropping will be detected
- Future-proof through physical encryption

PQC

- No additional hardware necessary
- Multiple algorithmic approaches
- „easy" to implement for existing infrastructure

Hybrid

- Security in Depth
- Symmetric key-exchange & PK-Infrastructure
- Fail-safe with mathematical and physical approach

Open Issues

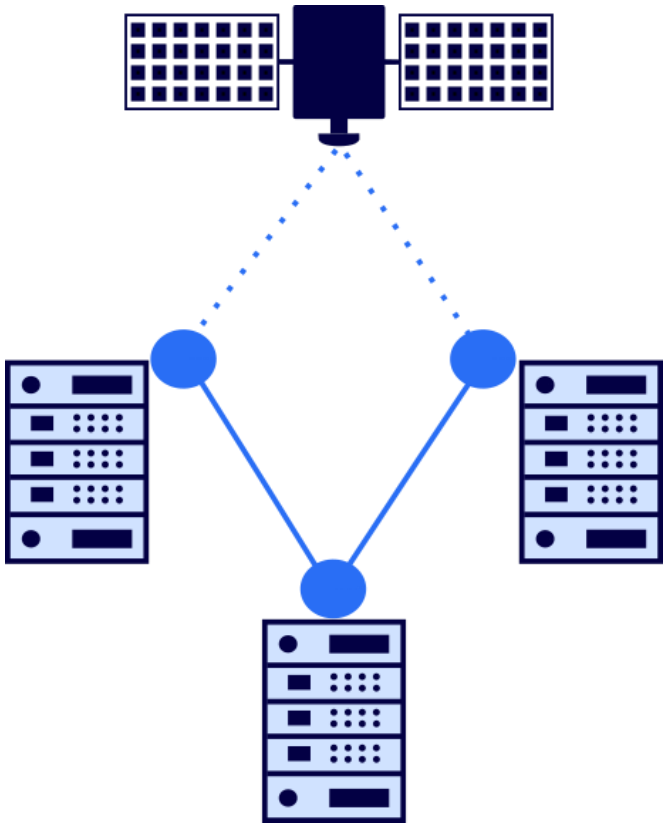
What is to come?

Quantum networks as a future vision
QKD is just the beginning

QKD is still in its infancy
- Only few separated testbeds
- Only small distances between nodes possible (100 km)
- Security proofs for real implementations still missing

QKD is just the beginning
- Connections for real networks with more participants
- Connecting future quantum computers
- Direct transfer of quantum data

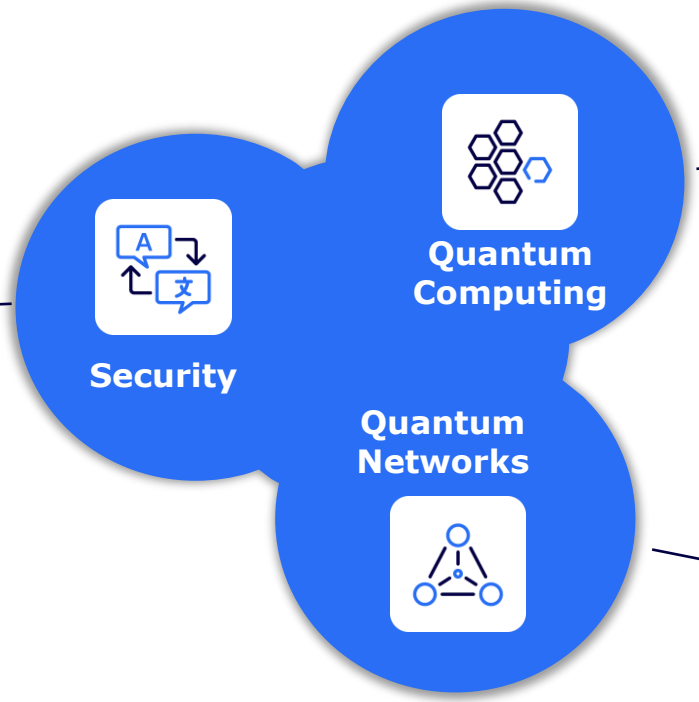
Security is the key
- Opportunity to include security from the start
- New approaches for securing ID and backend systems



bundesdruckerei.

Think security and technologies together

- Implement security from start
- Analyze risks and benefits
- Secure classical systems
- Cryptography needs to be agile
- Explore new security features



- Today: Small noisy quantum computers – very limited
- Highly dynamic development
- Unlocking potential will change a lot

- QKD is the beginning
- Establish infrastructure for quantum links
- Connecting quantum devices
- Transmission of quantum data as future vision

Combining technologies paints the full picture.

Think Quantum

Jan Klaussner

Bundesdruckerei GmbH
Department Innovations
E-Mail: jan.klaußner@bdr.de

Part of the Bundesdruckerei Group