QKD@DT
DEUTSCHE TELEKOM’S SECURE FUTURE

EPIC online technology meeting on quantum communication & quantum key distribution
11th of November 2020

F. Wissel, M. Gunkel
Deutsche Telekom Technik GmbH, Darmstadt

EPIC
European Photonics
Industry Consortium

QKD inside

ERLEBEN, WAS VERBINDET.

OUR MISSION

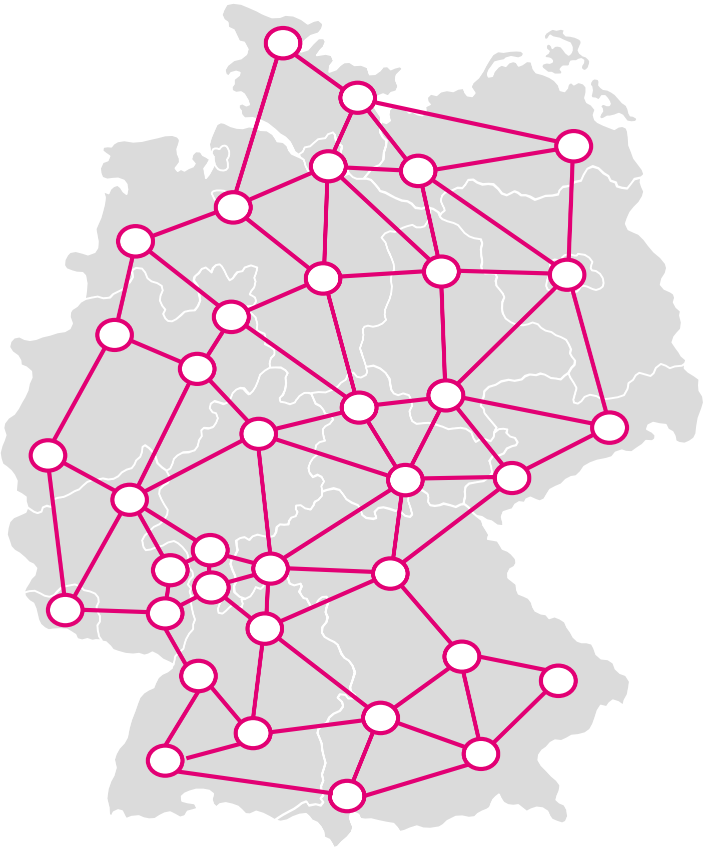
WE BUILD UP THE FUTURE QUANTUM COMMUNICATION INFRASTRUCTURE

OUR PROMISE
SECURITY FOR THE FUTURE

- Confidentiality
- Data Integrity
- Secure Authentication

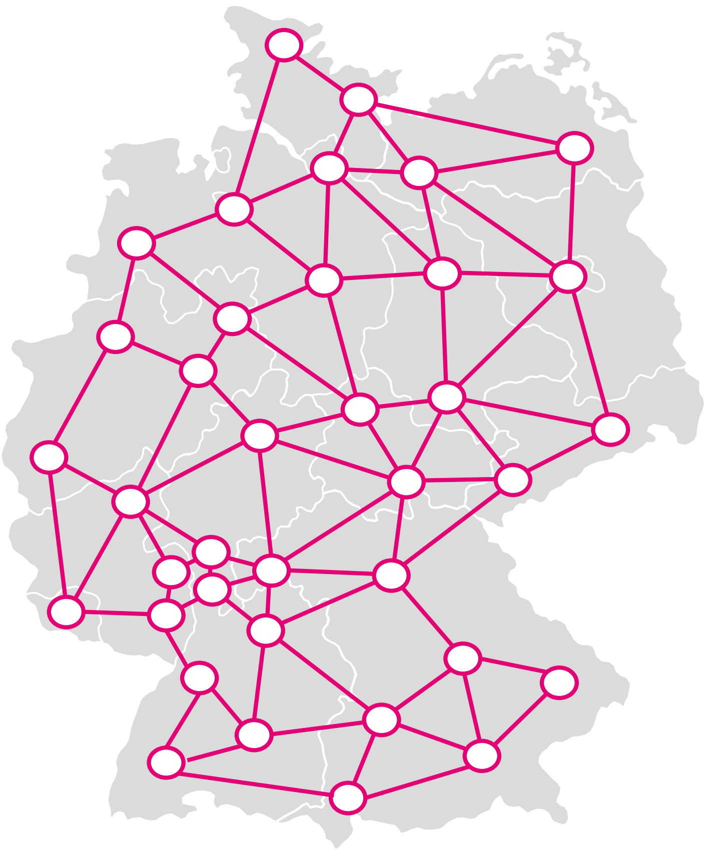
OUR GOAL

A SECURE COMMUNICATION PLATFORM



1. Protection of DT’s own network assets
2. Protection of governmental traffic and public agencies
3. Protection of critical infrastructure

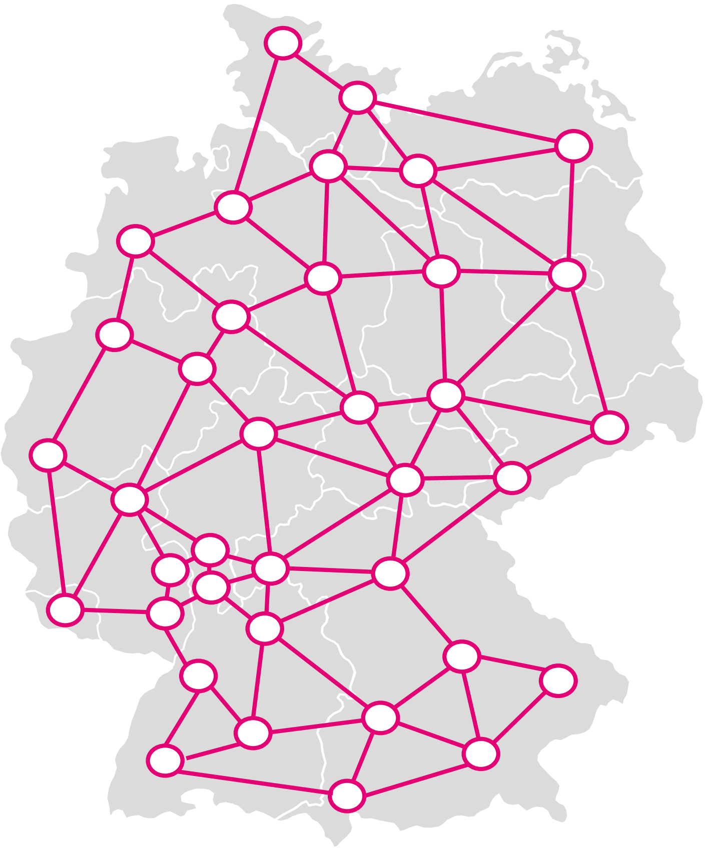
OUR GOAL
A SECURE COMMUNICATION PLATFORM



1. Protection of DT’s own network assets
2. Protection of governmental traffic and public agencies
3. Protection of critical infrastructure

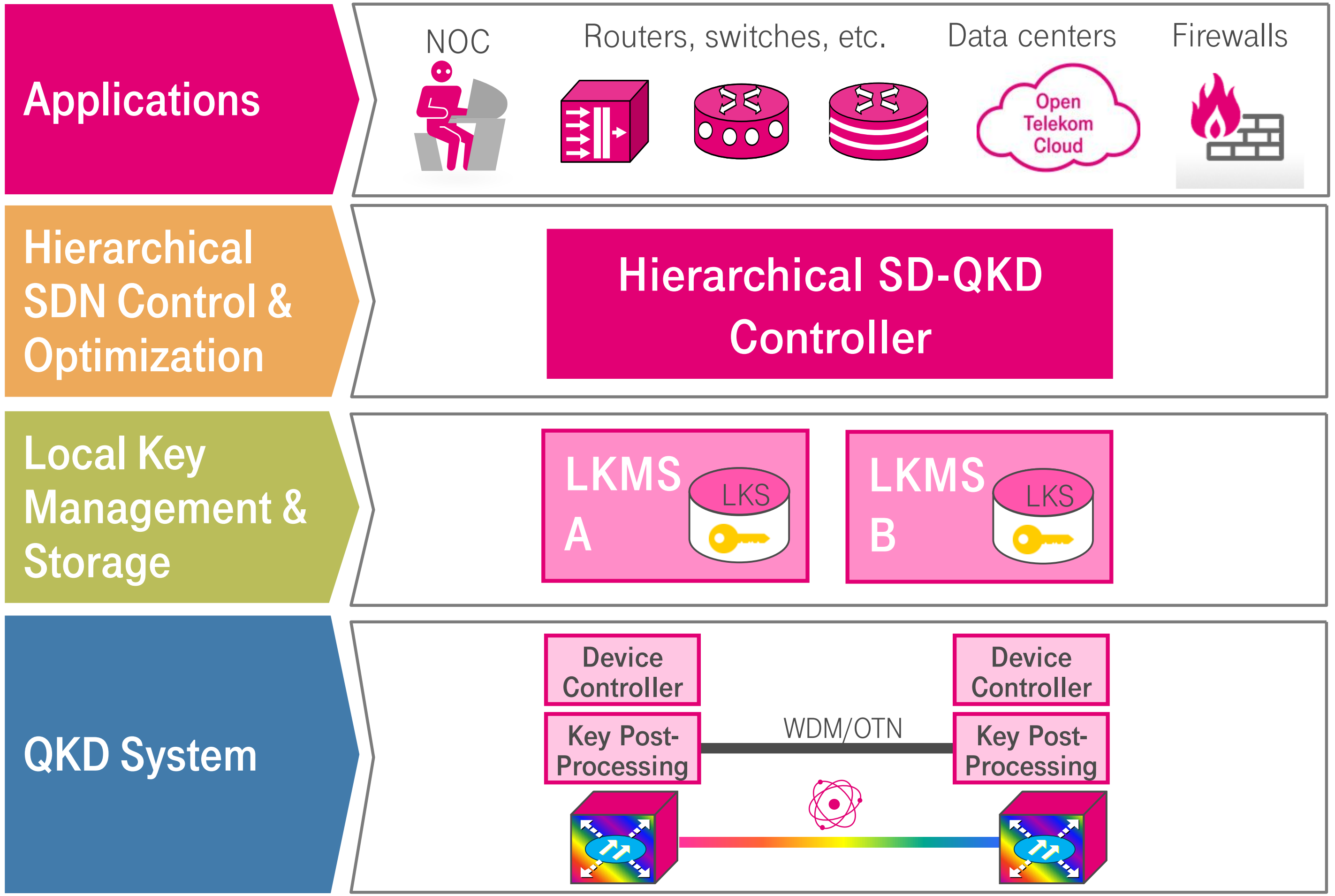
OUR GOAL

A SECURE COMMUNICATION PLATFORM

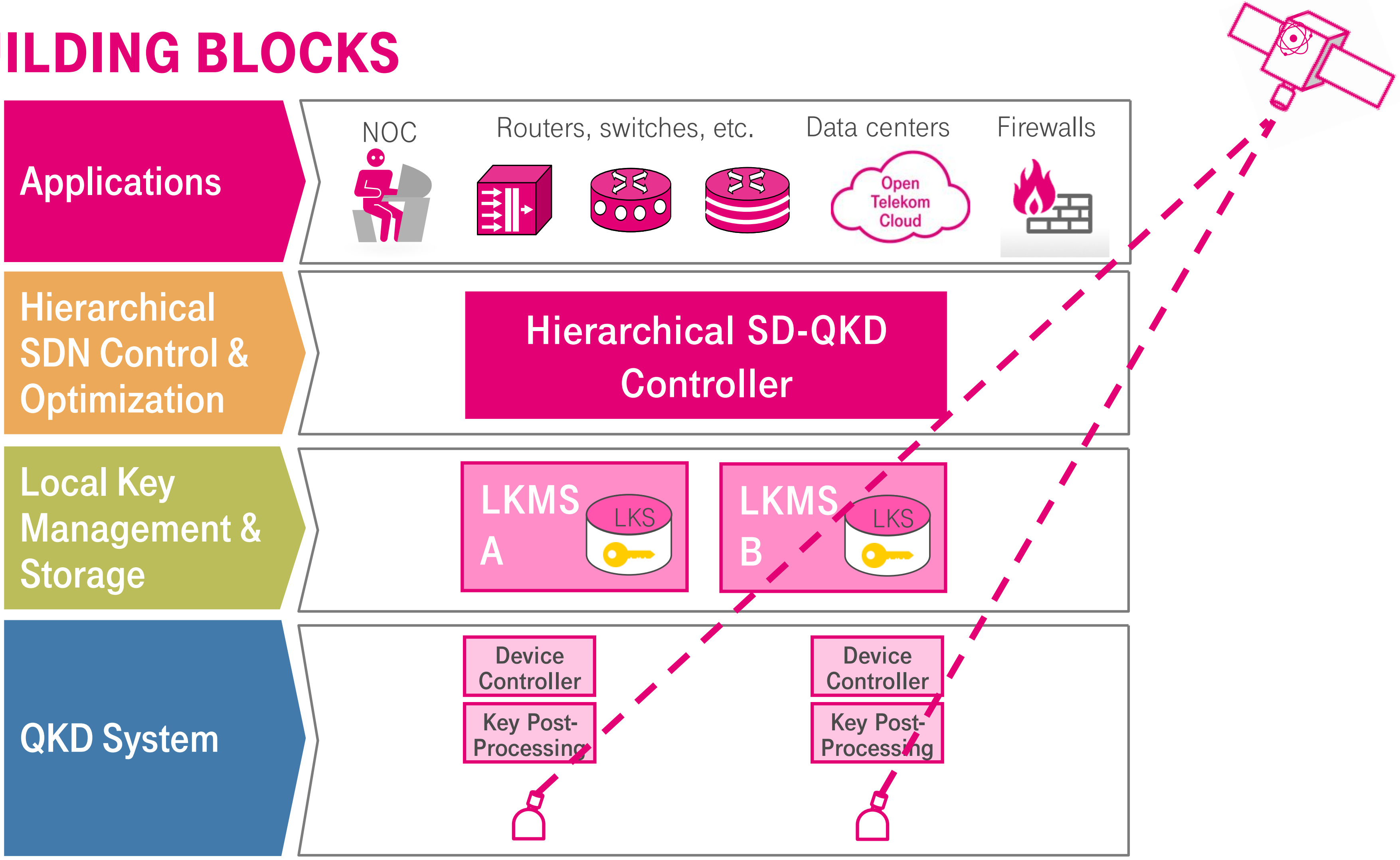


1. Protection of DT’s own network assets
2. Protection of governmental traffic and public agencies
3. Protection of critical infrastructure

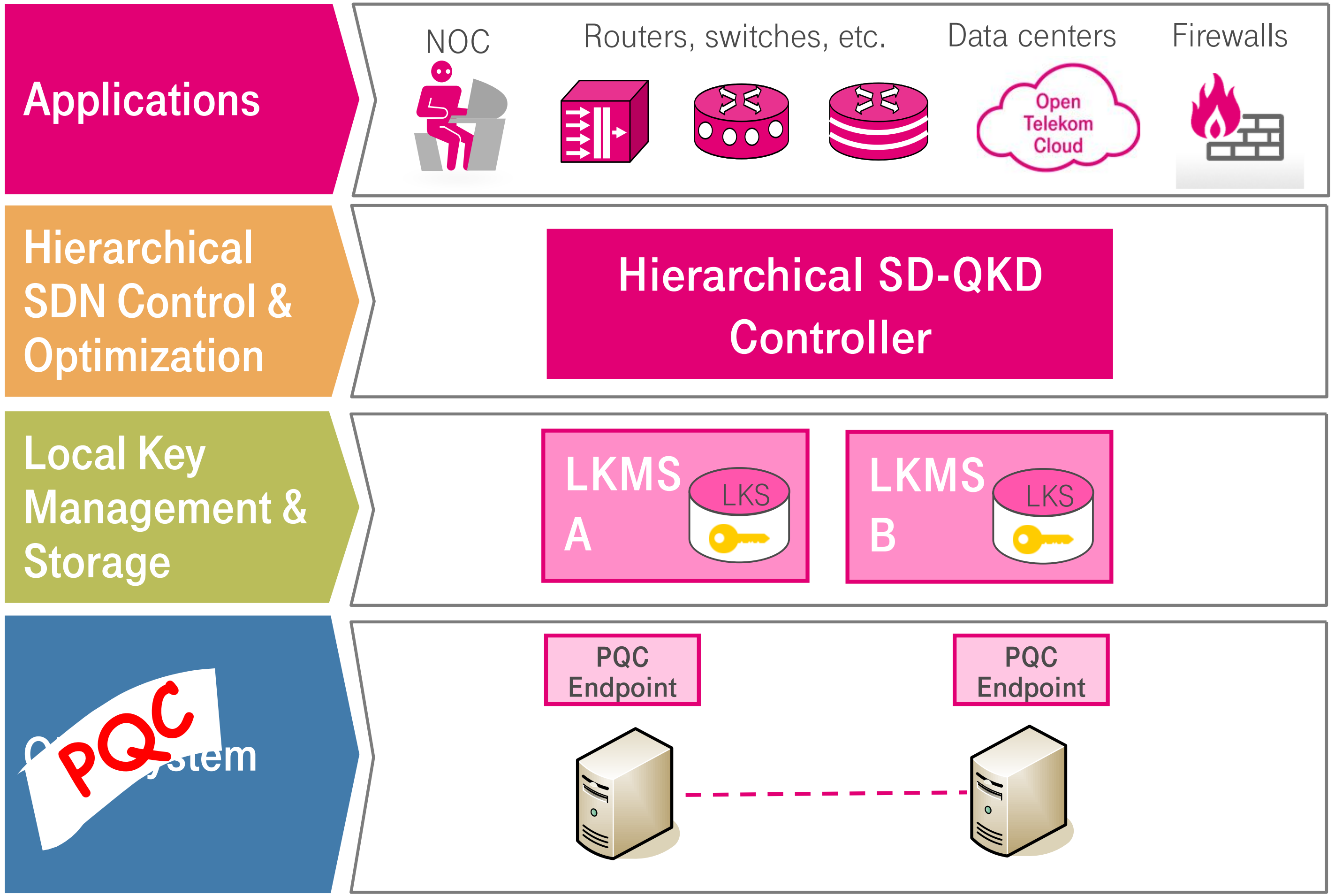
OUR ARCHITECTURE
MODULAR BUILDING BLOCKS



OUR ARCHITECTURE
MODULAR BUILDING BLOCKS



OUR ARCHITECTURE
MODULAR BUILDING BLOCKS



BEST OF BOTH WORLDS

DESIGN PRINCIPLES FOR CARRIER-GRADE QKD NETWORKS

Clear separation of QKD platform and key consuming devices/applications

- application traffic never directly forwarded inside the QKD plane
- no interrelation between QKD platform and state-of-the-art networking mechanisms
- QKD devices might use standard network infrastructure where/when beneficial

Minimally invasive intervention to existing network assets

- no additional QKD-specific protocol header extensions
- no impact on established networking protocols/paradigms

Smooth QKD integration

- coexistence with today’s crypto mechanisms and future PQC
- no further needless assumption about key usage (e.g. for encryption, authentication or integrity)
- key consumption by any devices at any layer between arbitrary endpoints
  (e.g. OTN-encryption, MACsec, IP-Sec or higher layers)

STANDARDIZATION & OPENNESS

- **No proprietary monolithic solution coming from one vendor only**

- ➢ **Modular building blocks are required!**
  - Only one exception: Alice and Bob modules which are directly interconnected are accepted and expected to come from the same vendor, i.e. no “black-link”-like interoperability at the photonic layer (perhaps in the long-run, but not today)
- ➢ **We need standardized interfaces!**
- ➢ **We need certification!**
- ➢ **We follow the Software-Defined Network (SDN) paradigm with a centralized control entity!**

SUMMARY

- **We are building the quantum secure network of the future**
- **QKD and PQC**
  - QKD for core and aggregation networks, PQC/QRA everywhere else (e.g. 5G antenna poles)
- **Use Cases**
  - Protection of DT‘s own network assets
  - Protection of governmental traffic and public agencies
  - Protection of critical infrastructure
- **QKD-Platform architecture**
  - Modular structure
  - No monolithic solution
- **What is needed**
  - Standardization
  - Certification
  - Speed

VIELEN DANK

FELIX.WISSEL@TELEKOM.DE
MATTHIAS.GUNKEL@TELEKOM.DE