

QKD @ DT: DEMOQUANDT

THE QUANTUM COMMUNICATION TESTBED FOR GERMANY

European Conference on
Optical Communication 2022

O. Nikiforov, M. Gunkel, F. Wissel, D. Giemsa

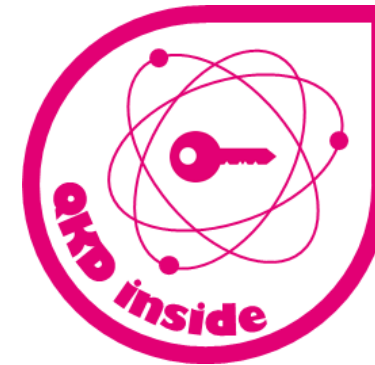
Deutsche Telekom Technik GmbH, Darmstadt



ERLEBEN, WAS VERBINDET.

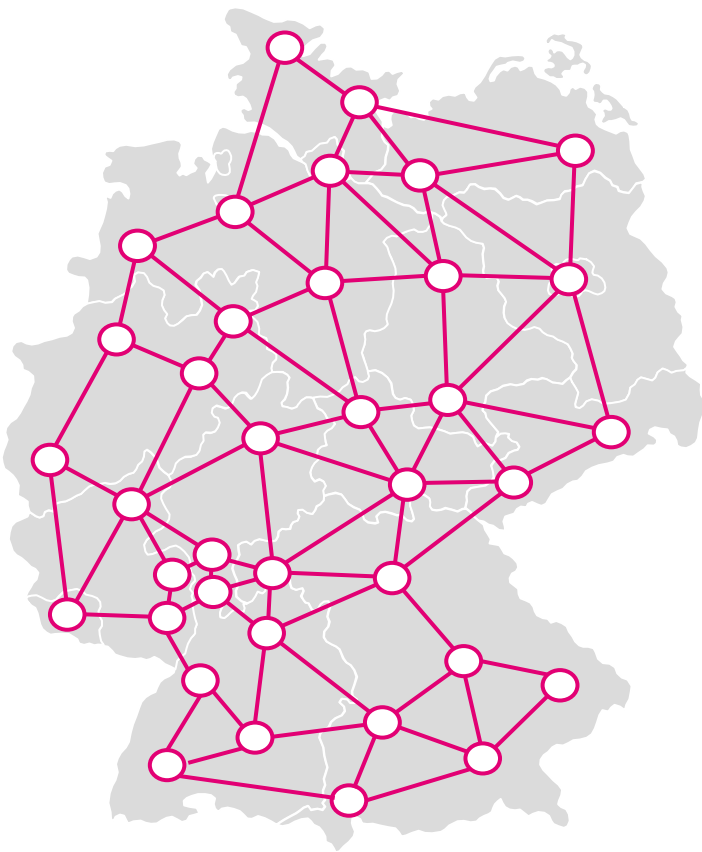
QKD @ DT: OUR PROMISE SECURITY FOR THE FUTURE

- Confidentiality
- Data Integrity
- Secure Authentication



QKD @ DT: OUR GOAL

GERMANY'S SECURE COMMUNICATION PLATFORM



Protection of governmental traffic and public agencies
 Protection of DT's own network assets as critical infrastructure
 Protection of further critical infrastructure and commercialization

QKD @ DT: QUANTUM COMMUNICATION INVOLVEMENT



CiViQ

- CV-QKD
- Deutsche Telekom Technik
- Until March 2022



OpenQKD

- Laboratory demonstration
- T-Labs + DT Technik
- Until autumn 2022



QSAFE

- Detailed Design for EuroQCI
- Commercial project for European Commission
- DT Technik is project prime



- AIT, Telefonica, Thales SIX, ThalesAleniaSpace France
- until July '22



Bundesministerium
für Bildung
und Forschung

DemoQuanDT

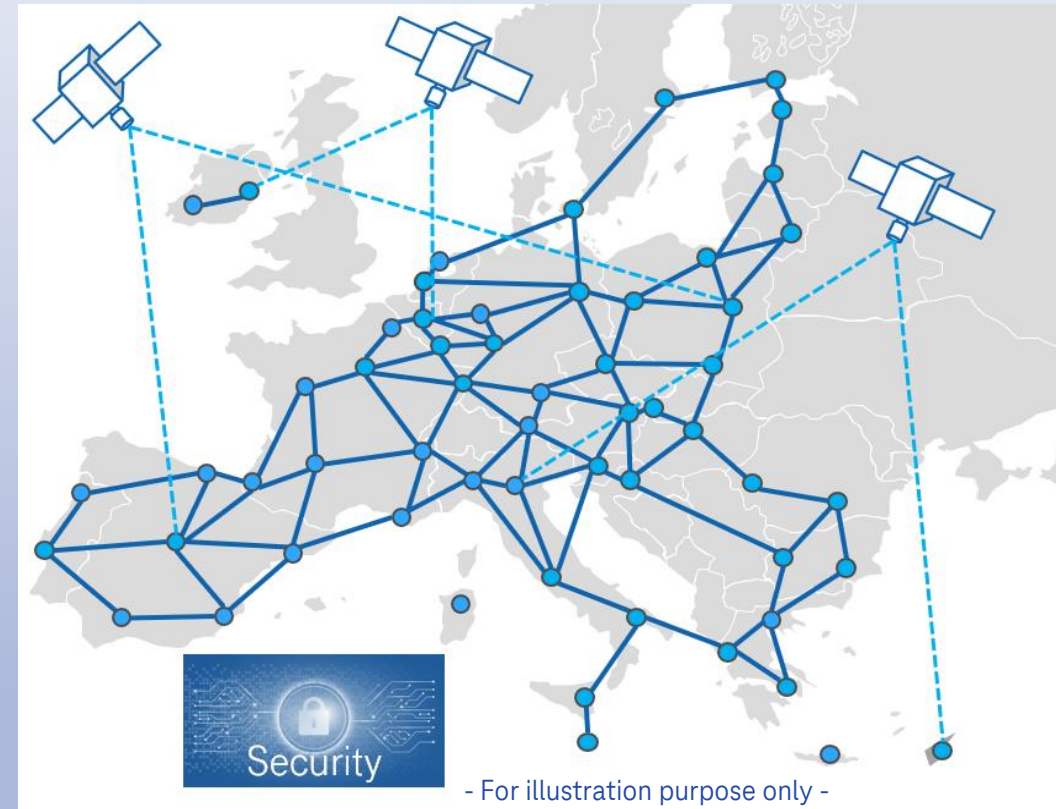


Detailed System Study for a Quantum Communication Infrastructure

- We described the overall architecture of the EuroQCI as EU's cybersecurity shield for the coming years.
- We generated the blueprint for a European QKD platform
 - ... which covers the security-by-design principle,
 - ... which follows network providers' best practice design guidelines,
 - ... and which allows a future-proof deployment of a EuroQCI.



Detailed System
Study for
European QCI



DEMOQUANDT: APPLICATION-ORIENTED DEMONSTRATION OF QUANTUM COMMUNICATION IN DEUTSCHLAND

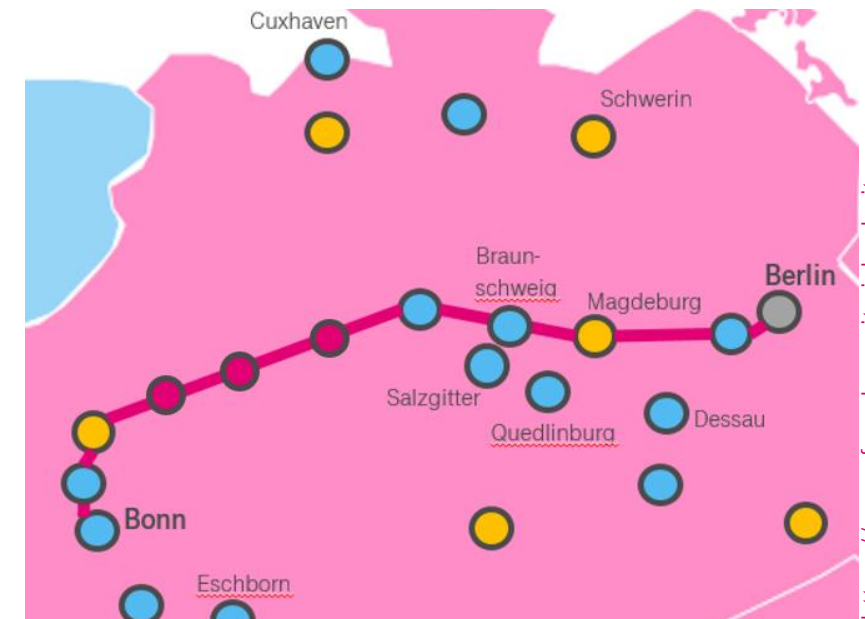
Goal

- Large-scale QKD network demonstration closest to real-life application
- Deployment of a chain of 18 trusted nodes btw. Berlin & Bonn
- Gaining experience in how to handle QKD equipment
- Interworking and Interoperation
- Close to a real network operation
 - Derivation of security requirements & software development
 - Integrability into DT's OSS ecosystem & establishment of relevant DT processes
- Security check of crypto primitives, protocols & interfaces
- Verification of a “highly-secure transport service”

Framework

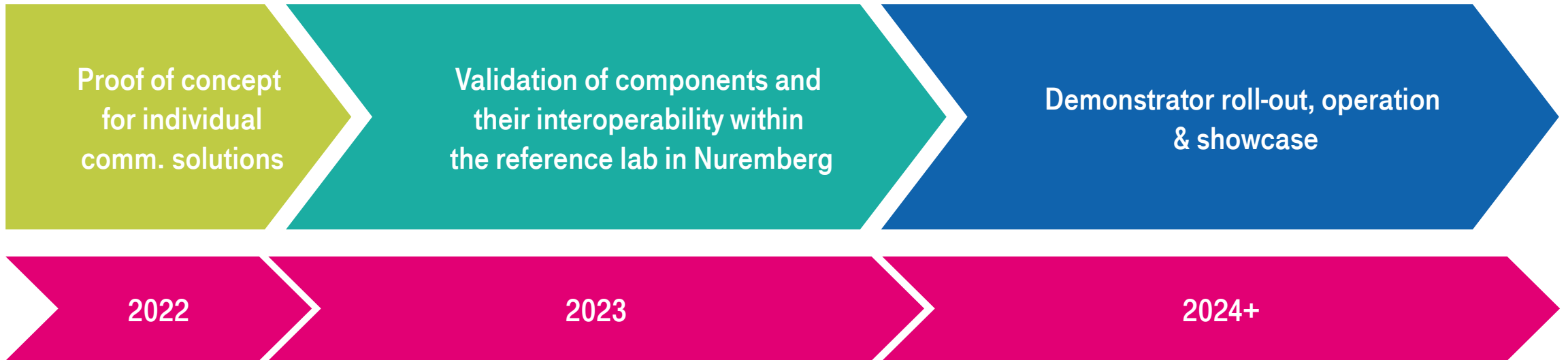


- Organisation: VDI on behalf of BMBF
- Runtime: 1.1.2022 to 31.12.2024
- Total budget: 15,2 Mio. €
 - Telekom budget: 9,6 Mio. € (50% funding; 4,8 Mio. €)



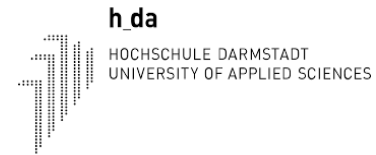
<https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/demoquandt>

METHODOLOGY AND TIMELINE



DEMOQUANT: APPLICATION-ORIENTED DEMONSTRATION OF QUANTUM COMMUNICATION IN DEUTSCHLAND

Partners



- Prime

Use case definition, integration of components & systems, QKD network operation, standardisation.

- Transport technology

L1 encryptors, hybrid PQC/QKD, QKD emulation, standardisation.

- Cyber security

L2/L3 encryptors, key management, security concepts, standardisation.

- QKD supplier

Key management systems, standardisation.

- Computer and telecommunication networking

Crypto agility, hybrid PQC/QKD, authentication for e2e security, software-defined networking, protocols.

- Cryptoplexity

Symmetric crypto, authentication, security proofs.

DESIGN PRINCIPLES FOR CARRIER-GRADE QKD NETWORKS

Clear separation of QKD platform and key consuming devices/applications



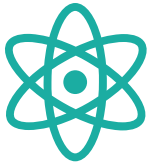
- Protected application traffic never directly forwarded inside the key generation platform
- No interrelation between QKD platform and state-of-the-art networking mechanisms
- Exchangeable QKD devices shall use standard network infrastructure where/when beneficial

Minimally invasive intervention to existing network assets



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

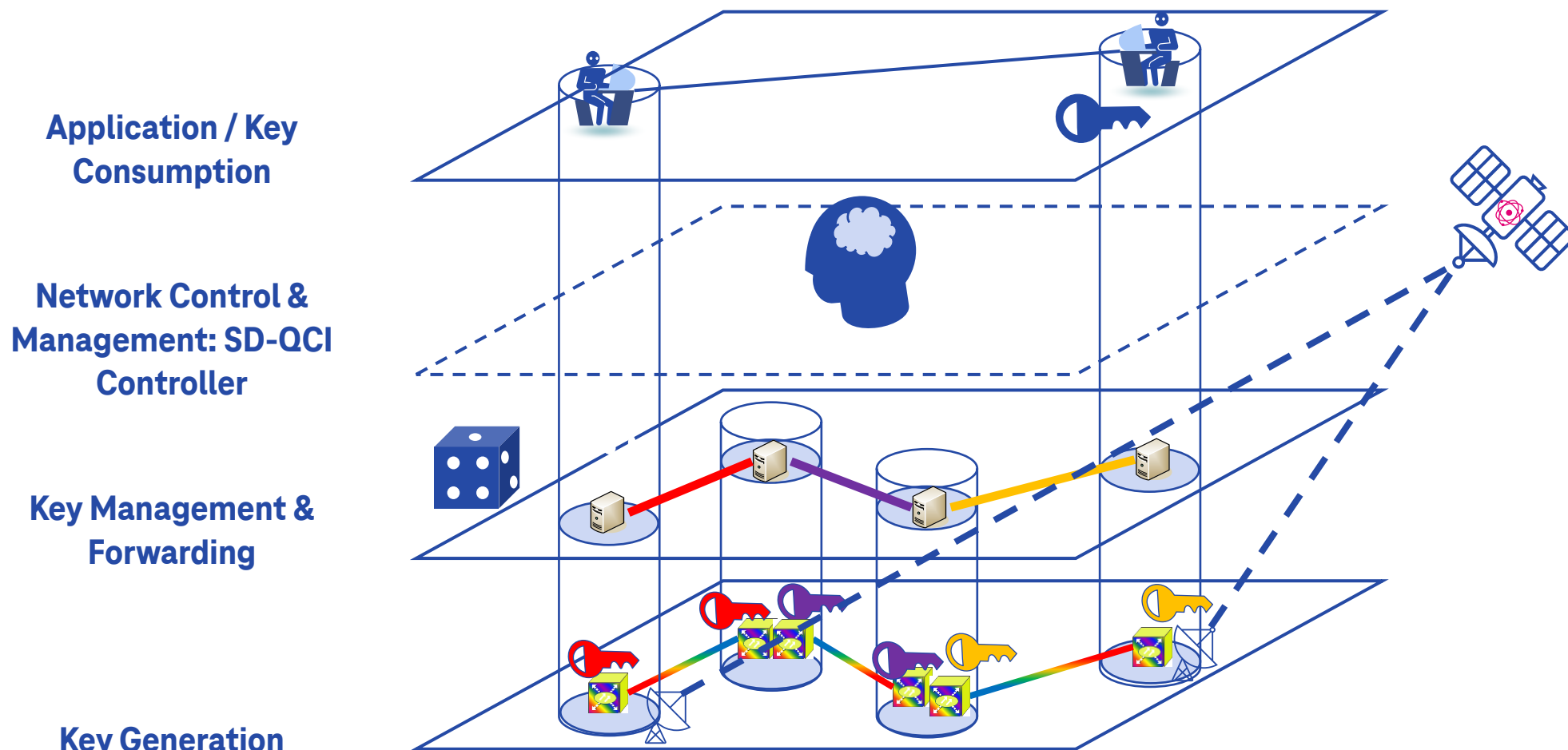
Smooth QKD integration



- Coexistence with today's crypto mechanisms and future PQC
- No further needless assumptions 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)

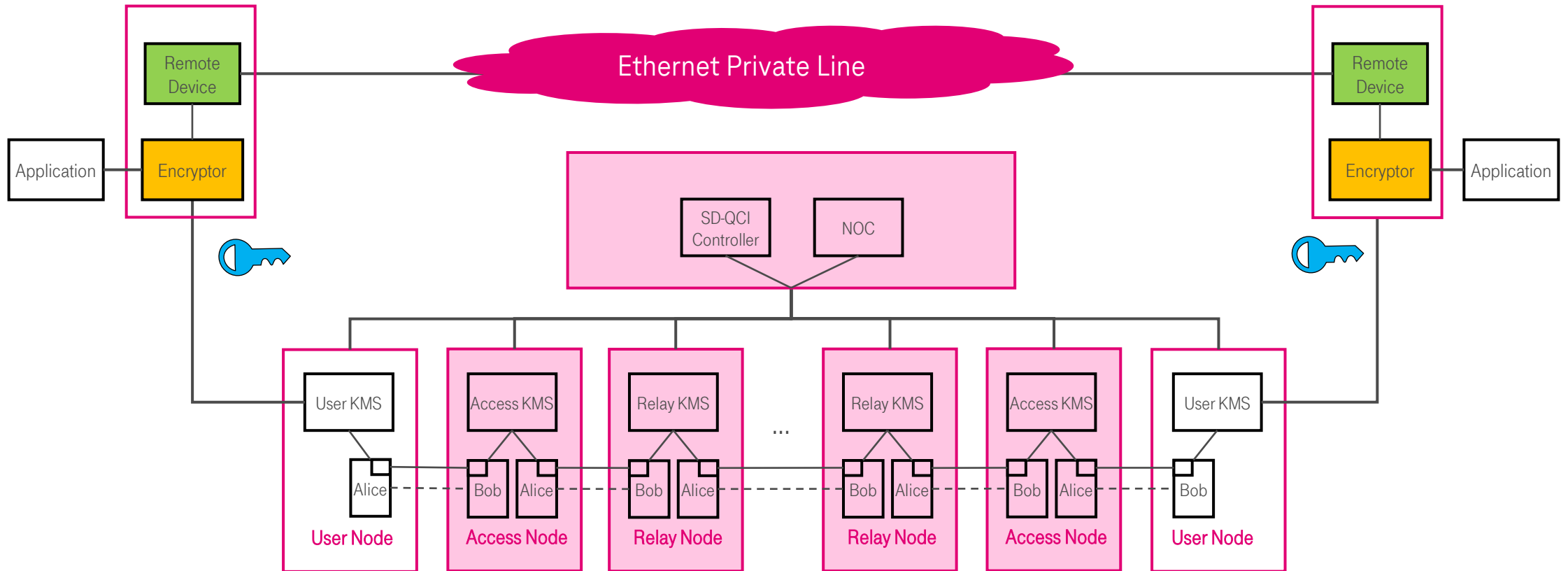
EUROQCI / DEMOQUANDT

SIMPLIFIED FUNCTIONAL ARCHITECTURE OVERVIEW



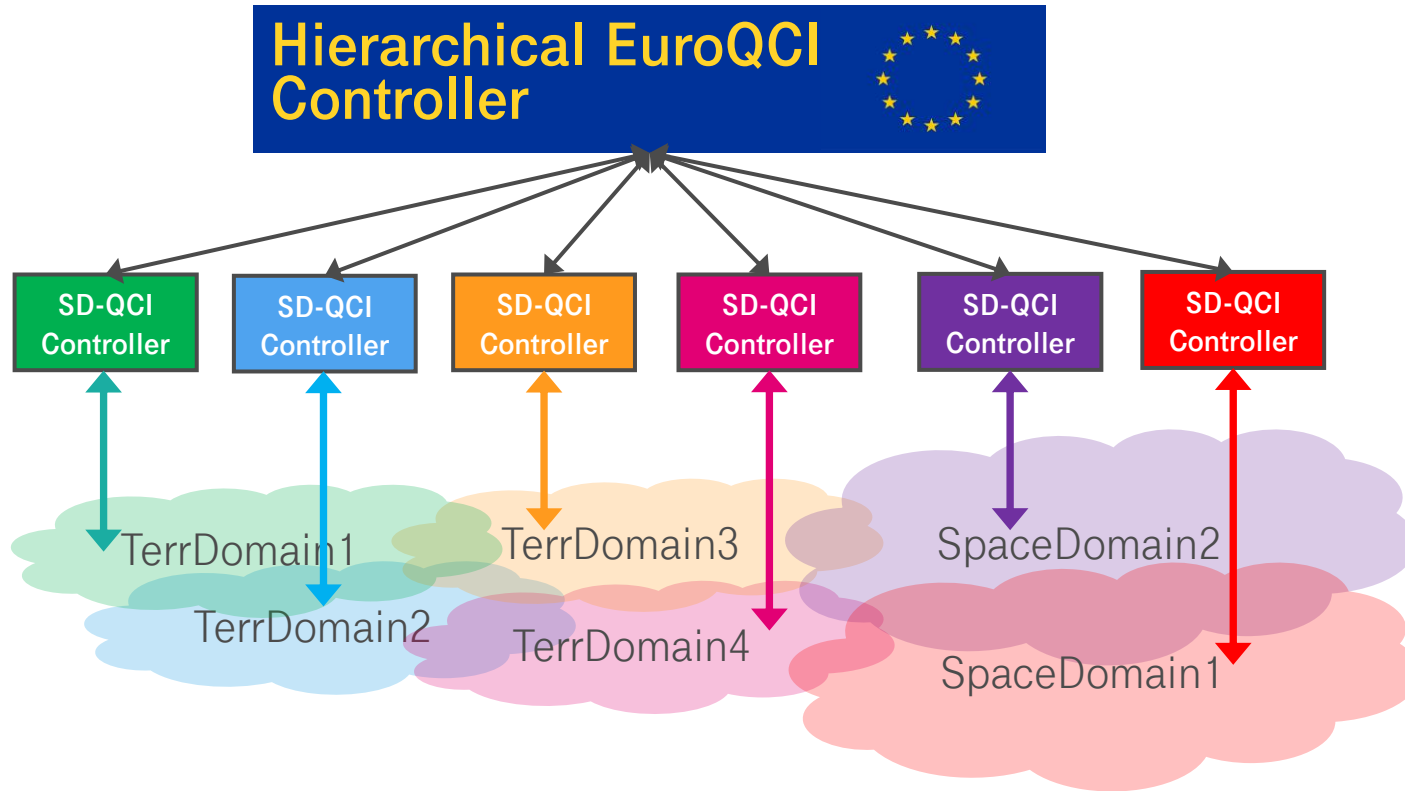
DEMOQUANDT

TARGET VIEW OF THE QKD DEMONSTRATOR LINK



CENTRALIZED QCI CONTROL ARCHITECTURE

CONTROLLER HIERARCHY



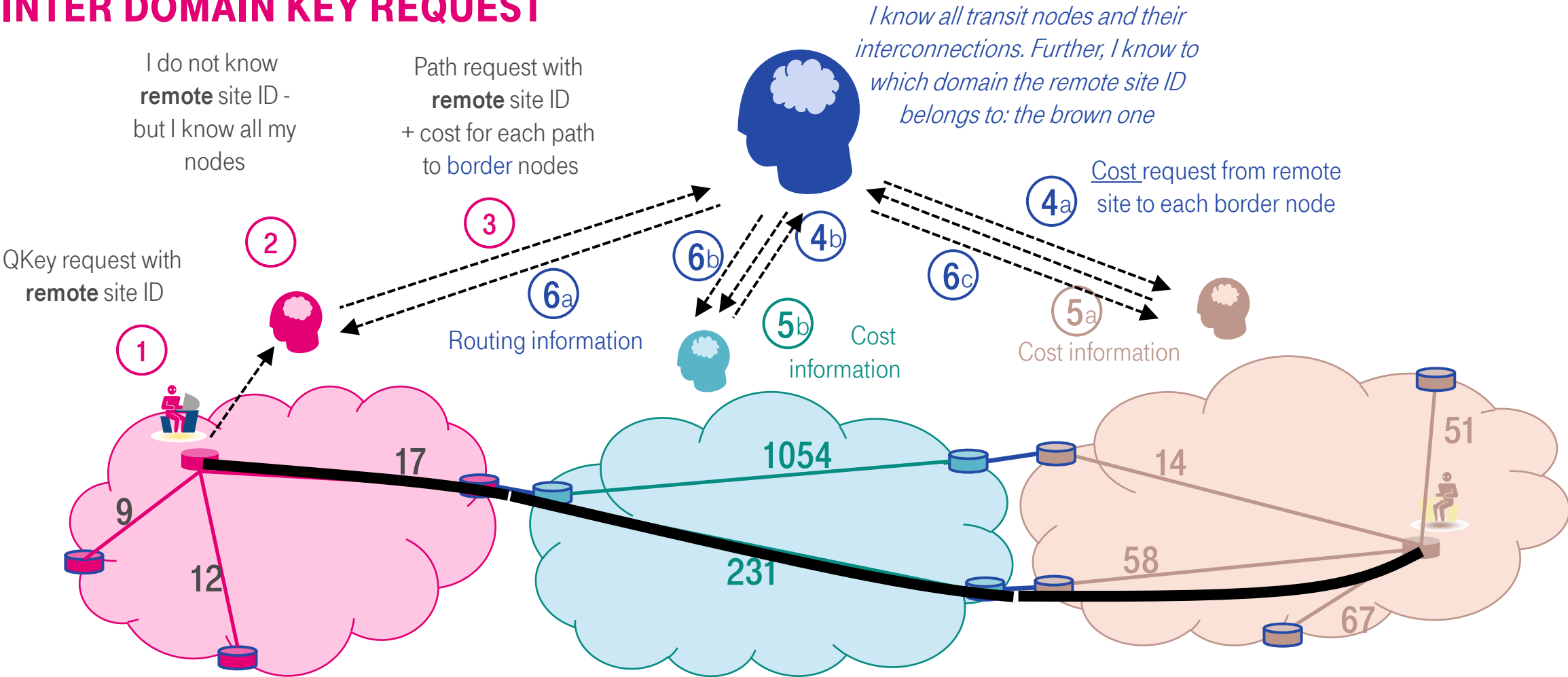
Why centralized control?

- **SD-QCI controllers**
 - domain abstraction
 - Interoperability
 - integration of new technology
- **Hierarchical controller**
 - knows transit nodes, but no domain internals
 - stitches domain-overarching key paths together

Confederated QCI domains: the only feasible way forward for a successful EuroQCI!

CENTRALIZED QCI CONTROL ARCHITECTURE

INTER DOMAIN KEY REQUEST



DEMOQUANDT

SUMMARY

- **We are building the quantum-secure network of the future**
- Multiple critical infrastructures to be served with quantum keys
- DT's previous involvements in Quantum Communication projects
 - Horizon 2020
 - QSAFE
- **DemoQuanDT**
 - Goals
 - Partners
 - Scope & Methodology
- Domain approach and centralized SDN control
- QCI design principles





OUR MISSION

WE BUILD UP THE QUANTUM SECURITY OF THE FUTURE