SPONSORED BY THE

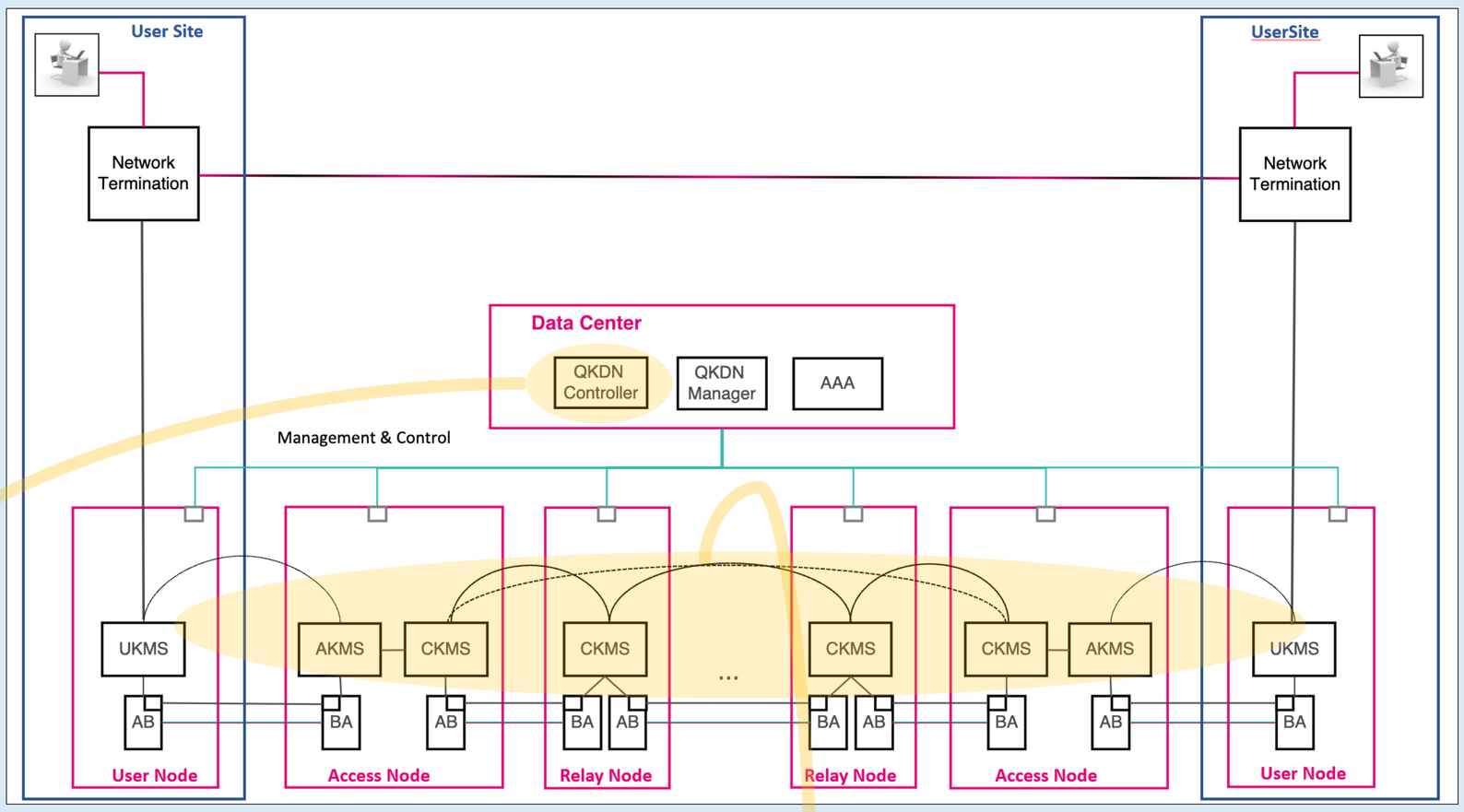
Federal Ministry of Education and Research

Crypto-agile Design and Testbed for QKD-Networks

DemoQuanDT

Motivation

- Quantum computers may break classical public key algorithms like RSA or ECDH – nearly all Internet connections affected
- Quantum effects can be used to exchange secret keys and detect eavesdropping (Martin et al., 2021)
- QKD Network (QKDN) implements hop-by-hop forwarding via trusted nodes in a meshed network topology to establish shared secrets over arbitrary distances (Evans et al., 2021)



Goals

- **Short term:**
  Complete QKD route in telecom network enabling test operation close to live network
- **Medium to long term:**
  Protect critical infrastructures in Germany

Subjects

Design:
- Protocols & Interfaces
- Cryptography
- Security

Software:
- Key-Management-Systems (KMS)
- QKDN-Controller

Implementation:
- Reference Lab
- Demonstrator

Time Period

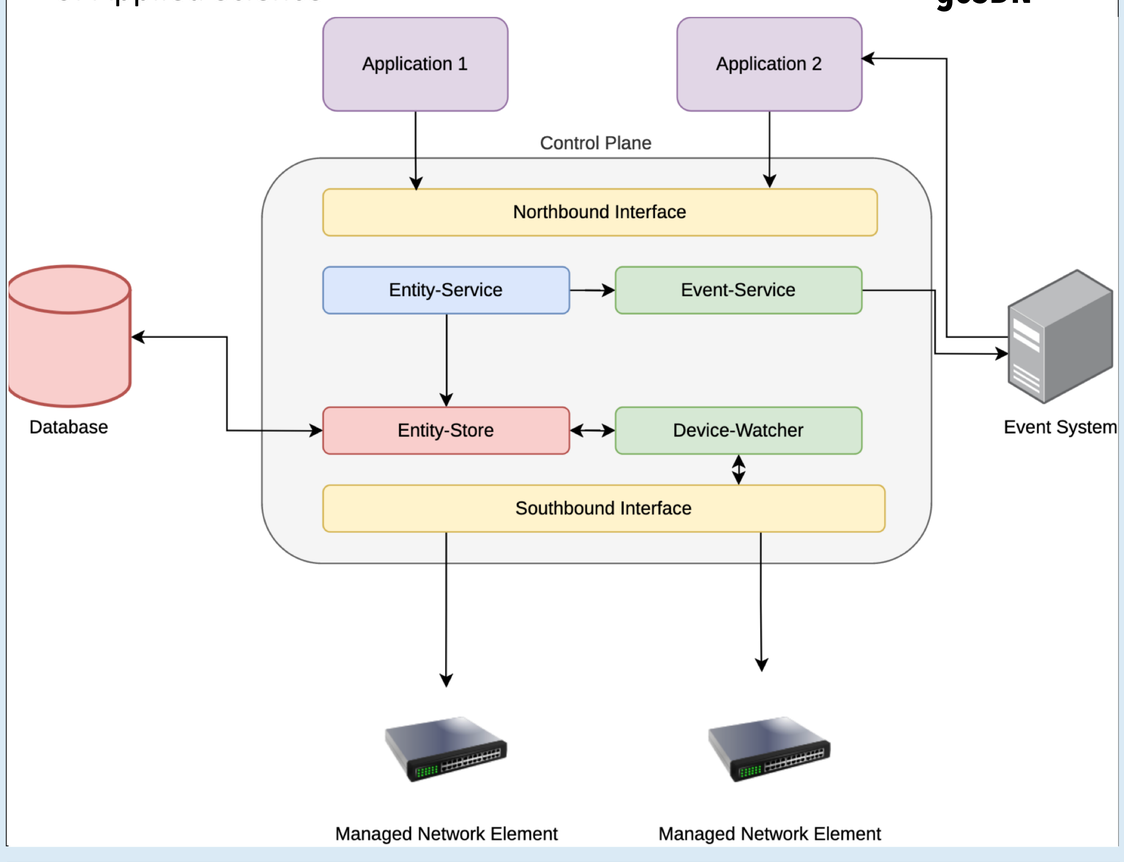
2022 – 2024

QKDN-Controller

Centralized control of trusted nodes and demand-driven routing for key distribution in QKD Networks (QKDN)

- Based on goSDN Controller of Darmstadt University of Applied Science

goSDN



Security

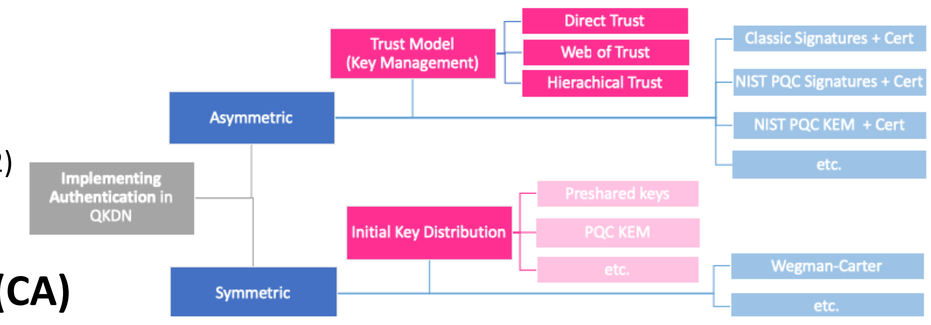
Secure Key Exchange via Trusted Nodes

Trusted nodes are a weak point of QKDN and information-theoretic security of QKD is abandoned (Evans et al., 2021). Considered countermeasures:

- Physical Security
- Multipath Routing
- Hybridization of shared secrets (Classical & Post Quantum Cryptography (PQC))

Authenticity

- (Paul et al., 2022)
- (Bibak et al., 2022)



Crypto-Agility (CA)

- Trade-off CA and complexity

Key-Management-Systems

- Key material quantity in KMS (potential for damage vs. flexibility)
- Key age (How often change keys?)
- Standardization of KMS interfaces (ETSI GS QKD 004, 014, 015, 020)

Current Contribution

- SDN controller for optical transport networks across multiple operator domains
- Investigation of actual state of PQC Migration (Alnahawi et al., 2021) and CA (Alnahawi et al., 2022)
- Crypto-Agility Maturity Model (CAMM) (Hohm et al., 2022)

CAMM on!

Next Steps

- Investigate Impact of hybridizing shared secrets (QKD keys)
- Evaluation of security & performance of authentication options depending on different types (requirements) of QKDN interfaces
- Evaluation of CA in implemented QKDN using CAMM
- Implement & improve standards for KMS interfaces

Literature

- Nouri Alnahawi et al.: "On the State of Crypto Agility." 18. Deutscher IT-Sicherheitskongress, 103–126. SecuMedia Verlags-GmbH (2022).
- Philip Evans et al.: "Trusted Node QKD at an Electrical Utility." *In: IEEE Access*. (2021).
- Khodakhast Bibak et al.: "Authentication of variable length messages in quantum key distribution." *EPJ Quantum Technol.* 9, 8 (2022).
- Julian Hohm et al.: "Towards a maturity model for crypto-agility assessment." (2022). *15th International Symposium on Foundations & Practice of Security (FPS)*. (2022)
- Sebastian Paul et al.: "Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3." *Asia Conference on Computer and Communications Security*. (2022).
- Vicente Martin et al.: "Quantum technologies in the telecommunications industry." *EPJ Quantum Technology* 8.1 (2021): 19.
- Nouri Alnahawi et al.: "On the State of Post-Quantum Cryptography Migration." *INFORMATIK 2021. Gesellschaft für Informatik, Bonn.* (S. 907-941) (2021).

Authors: Johanna Henrich (johanna.henrich@h-da.de), Andreas Heinemann, Martin Stiemerling, Fabian Seidl

Adva Network Security · h_da hochschule darmstadt · KEEQUANT · Rohde&Schwarz Make ideas real · Technische Universität Darmstadt · UCS User-Centered Security