

SCIENTIFIC THINKING, INDUSTRIAL MINDSET

the AIT KMS for QKD networks

Stephan Laschet, 2025.05.28



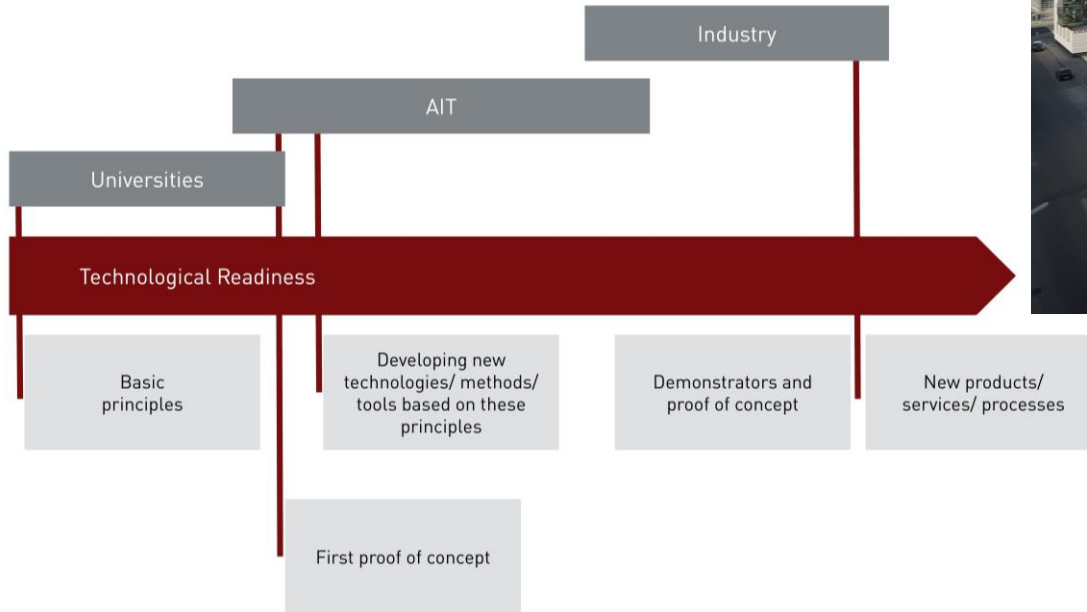
KEY MANAGEMENT FOR QKD NETWORKS

Scientific thinking



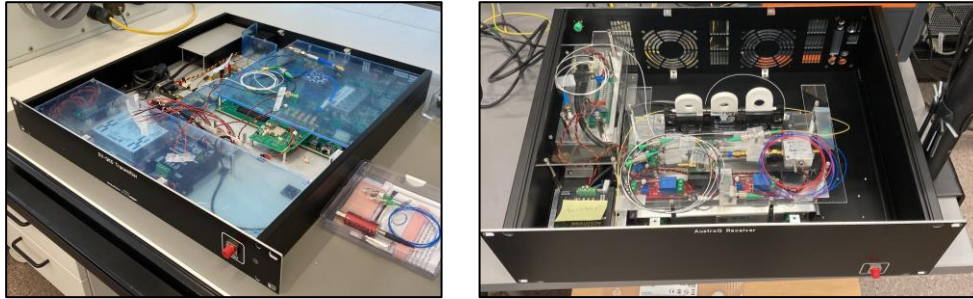
AUSTRIAN INSTITUTE OF TECHNOLOGY

- Austria's largest research and technology organization.
- State owned, publicly and privately funded

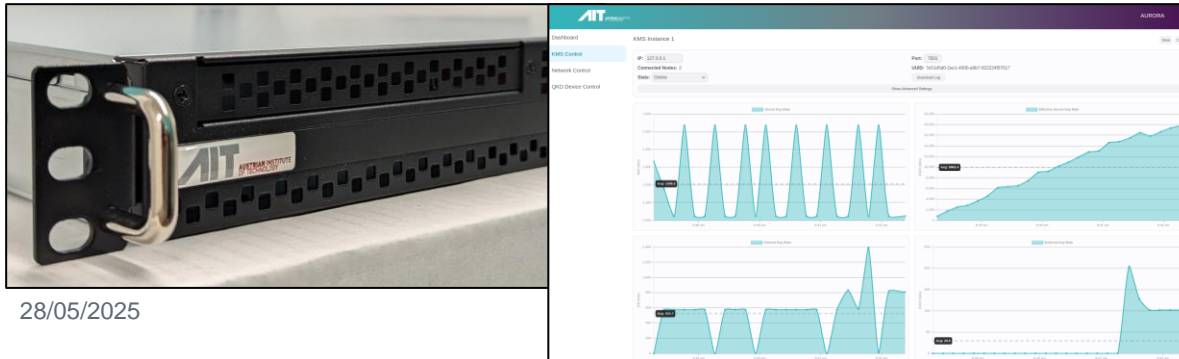


AIT QKD PORTFOLIO

QKD Hardware (experimental setup)

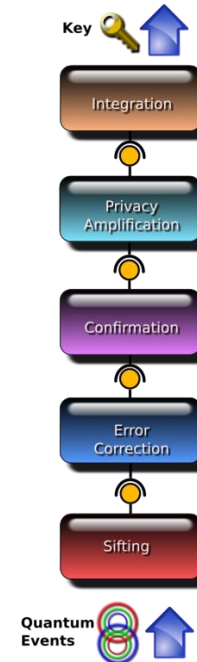


QKD Key Management System (KMS)



28/05/2025


Quantum Postprocessing System (QPS)



CURRENT PROJECTS – KMS CONTRIBUTION

- Military Use-Cases:

- Discretion – SDN focus 

- Anquor – free-space QKD and military application integration 

- Industrial research:

- Quarter – Direct integration with QPS 

- eCausis – Highly integrated QKD Node & Certifiability 

- Civil, Government & EuroQCI:

- QCI-CAT – Austrian EuroQCI and gov. use-cases 

- Q-CRIT – Securing critical infrastructure with QKD

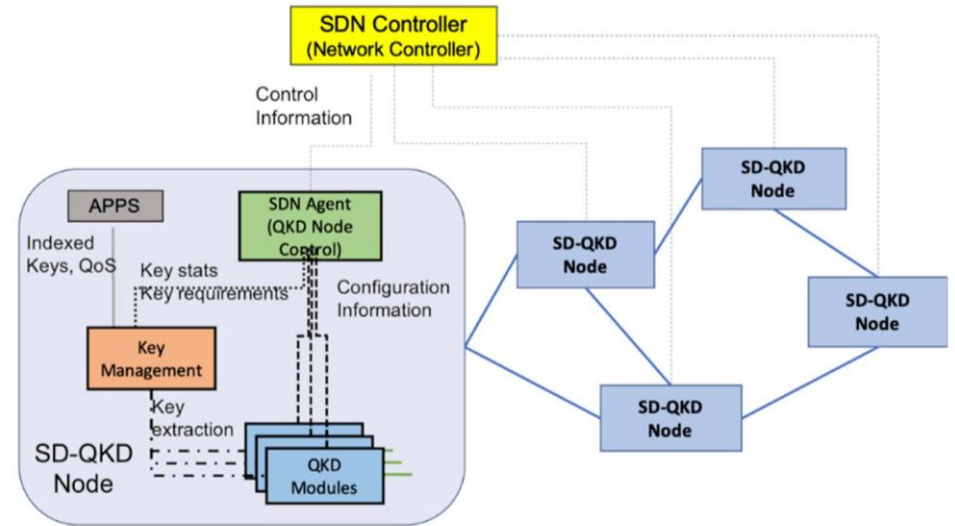


- QKD and KMS related research:



QKD KMS SYSTEM DESIGN WITH SDN

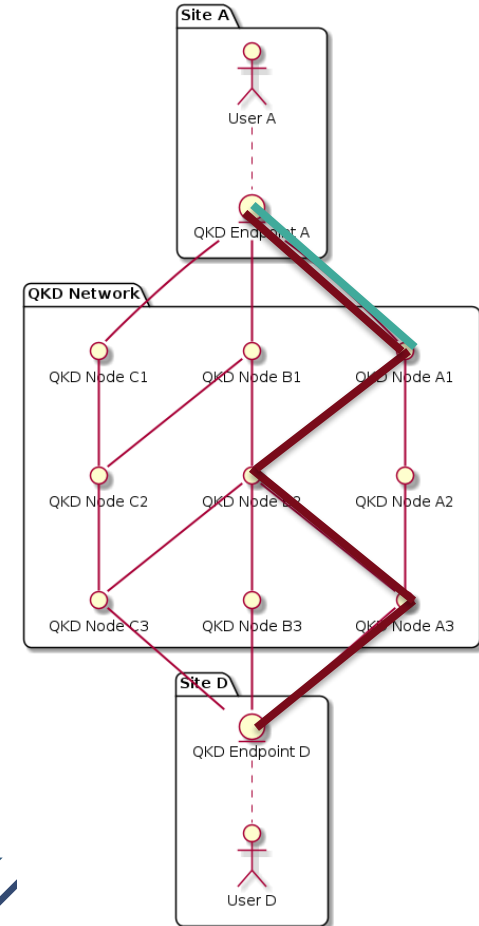
- SDN by design
- On one Node:
 - QKD Modules
 - Key Management System
 - Applications
 - SDN Agent
- Outside the node:
 - SDN Controller
 - Other Nodes



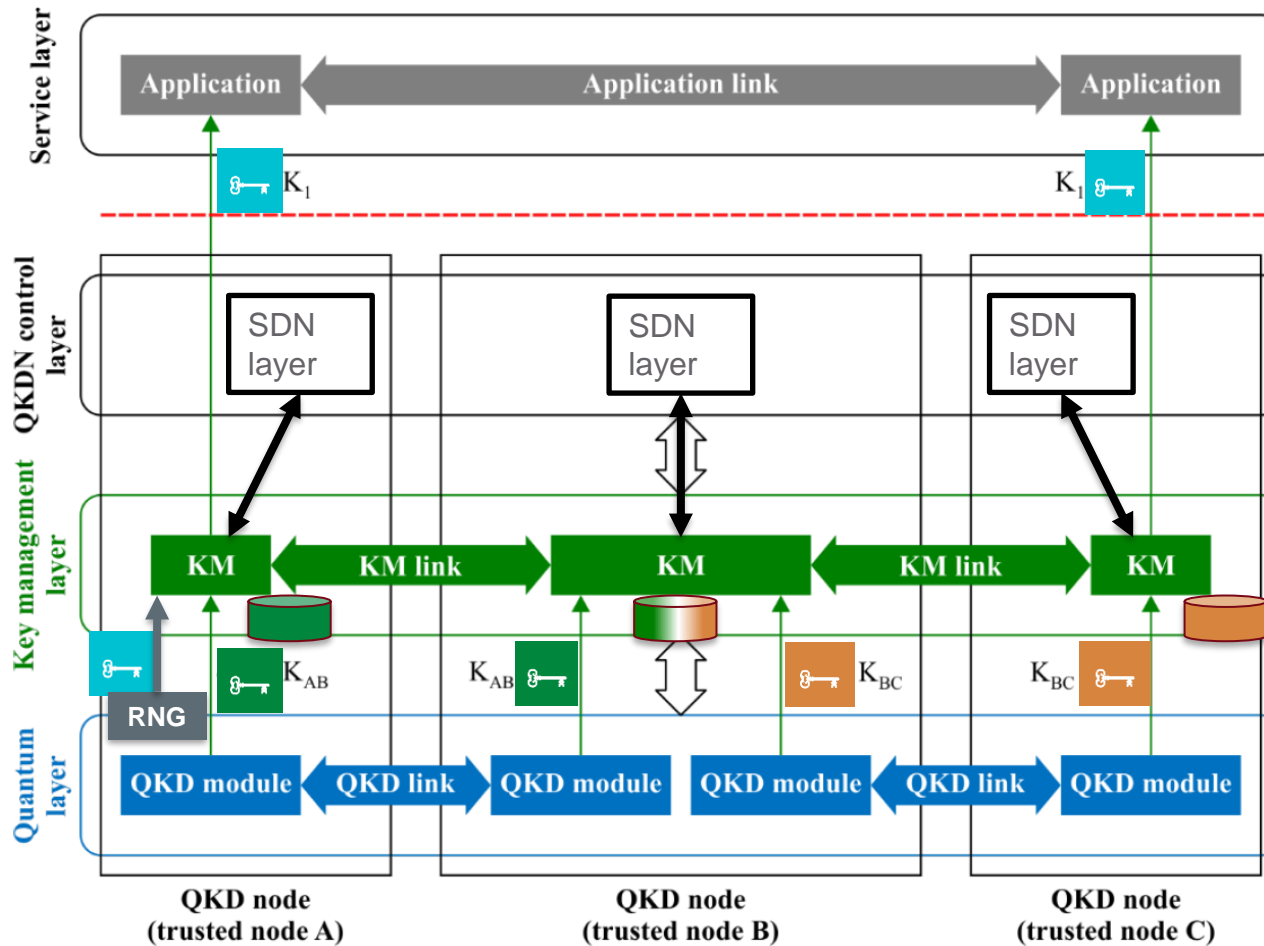
QKD + SDN Network. Source ETSI QKD GS 015 v1.1.1

KMS MAIN FUNCTIONALITY IN A QKDN

- Range and connecting participants require QKD Network
- Each node connected with QKD link
- KMS distributed system in the Network
- Collect point-to-point keys, assign them to usage
- QKD Devices establish Keys on direct link
 - ITS due to QKD protocols
- KMS establishes end-to-end Key from direct link Keys
 - Must retain ITS for used primitives:
 - Encryption OTP XOR
 - Authentication & integrity: MAC based on UHF



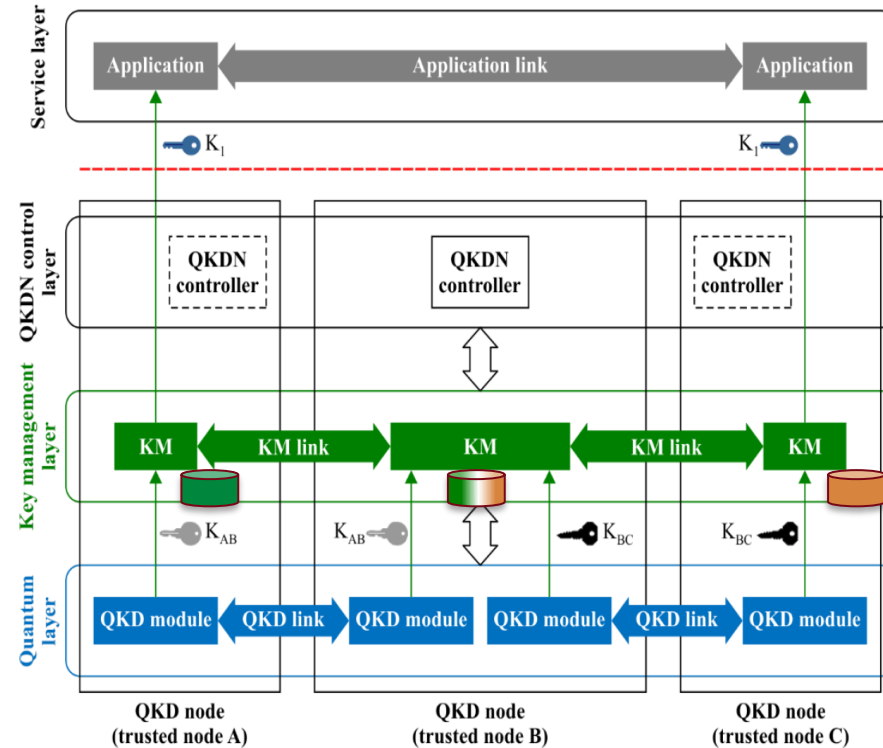
KMS MAIN FEATURE: KEY FORWARDING



Key Forwarding. Figure based on ITU Y3800

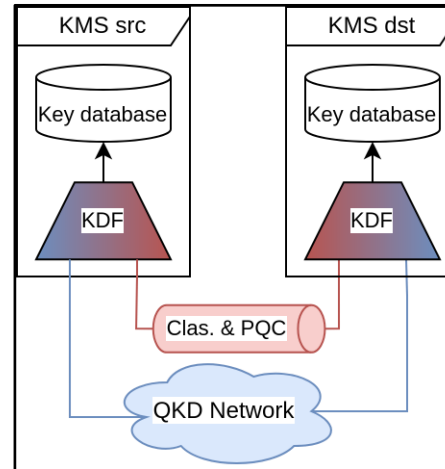
OTHER FEATURES

- Keeping databases in sync
- Keeping a buffer of keys (reserve)
- Key maintenance
- Reformat keys
- ITS encryption and authentication

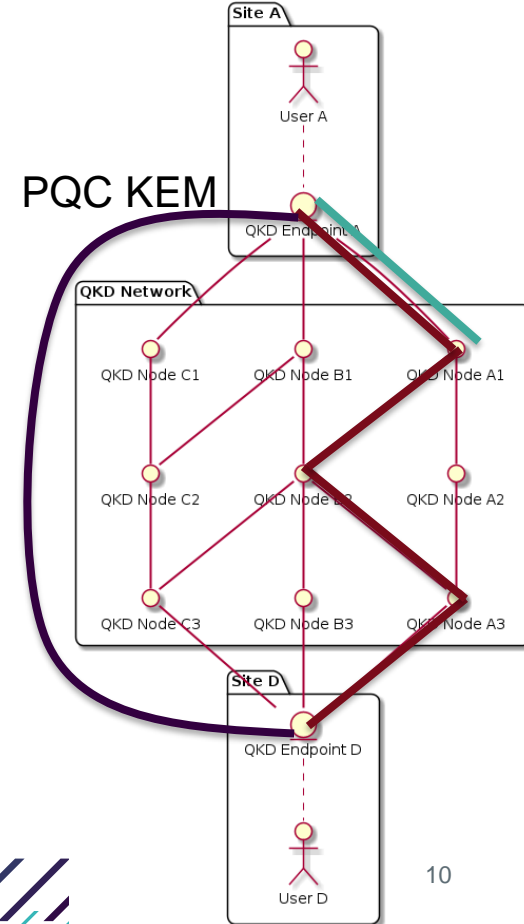


OTHER FEATURES

- Keeping databases in sync
- Keeping a buffer of keys (reserve)
- Key maintenance
- Reformat keys
- ITS encryption and authentication
- Classical + PQC +QKD hybrid

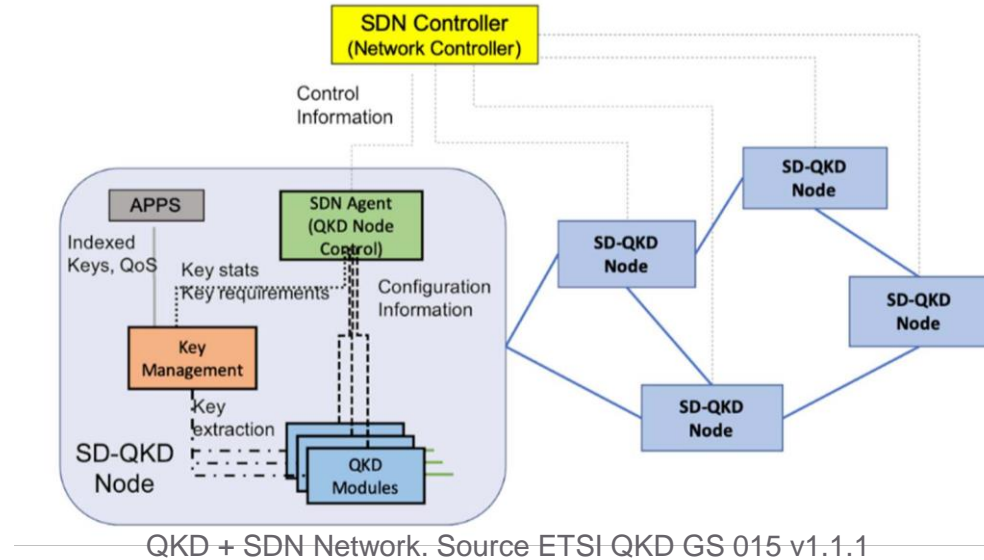


PQC KEM



OTHER FEATURES

- Keeping databases in sync
- Keeping a buffer of keys (reserve)
- Key maintenance
- Reformat keys
- ITS encryption and authentication
- Classical + PQC +QKD hybrid
- Central „hub“ for multiple needs
- ...
- Scope:
 - Key Management System manages Keys
 - No network management → SDN



KEY MANAGEMENT FOR QKD NETWORKS

Industrial Mindset



KMS DEVELOPMENT METHODOLOGY

- Industry grade development methods
 - TDD ~89% unit test coverage
 - Static / Dynamic Code Analysis
 - CI/CD with regular releases, currently at v0.10.0
 - Full system simulation test with each release
 - Deployable on COTS server HW
- Used technologies:
 - C++20 for KMS
 - Database sqlite
 - Cryptography library Botan
 - Hardware TPM as RNG
 - SDN in Python and React for frontend
 - http(s) and CoAP for network communication



M.Sc. Stephan Laschet
Research Engineer



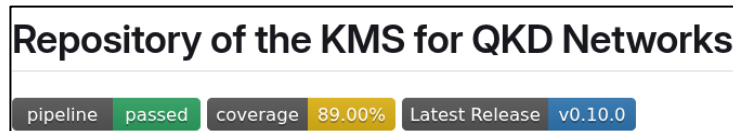
Dr. Sebastian Ramacher
Scientist



M.Sc. Luca Torresetti
Research Engineer

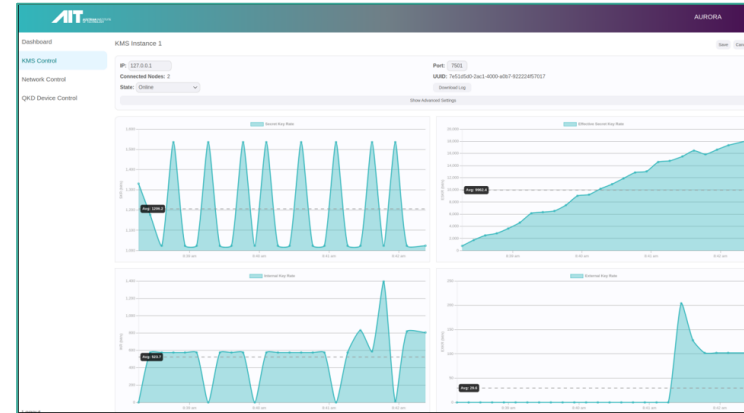


Dr. Paul James
Research Engineer



KMS FEATURE SET

- **Interface to applications:**
 - ETSI GS QKD 014
 - ETSI GS QKD 004 in CoAP and https
- **Interface to QKD:**
 - ETSI GS QKD 014
 - ETSI GS QKD 004 (push mode)
- **Secure Key management**
 - ITS authenticated + key ITS encrypted during forwarding
 - Classical + PQC + QKD Hybrid
 - Key resizing, lifecycle
 - User, device and key reserve management
 - Group key feature
- **SDN interface:**
 - Custom, developed with experts (no standards available)
 - Static Configuration also possible
- **Integrated with most major EU-QKD devices**
 - LuxQuanta, ThinkQuantum, QTI, KEEQuant, QOJ





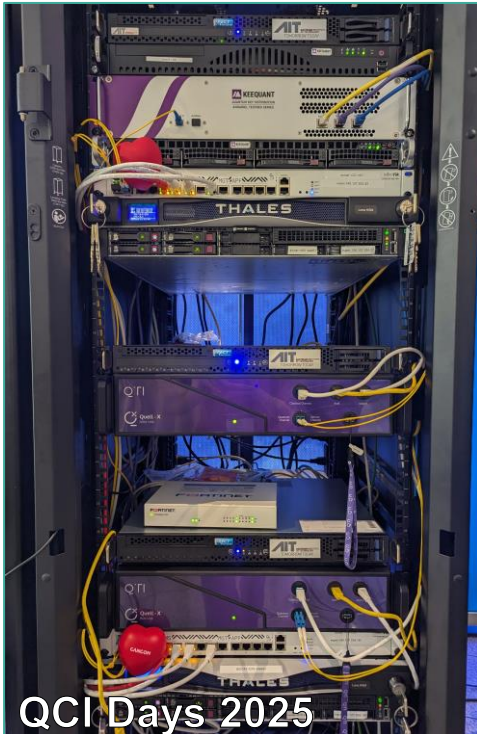
QCI Days 2025



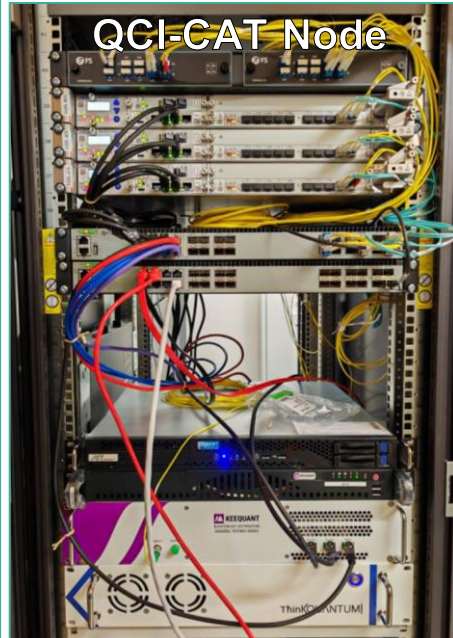
FEINDEF



REPMUS (NATO event)



QCI Days 2025



QCI-CAT Node



EC & PT embassy

THANK YOU!

Stephan Laschet

qkd-kms.ait.ac.at

