OPEN QKD

Use-cases in the Open European Quantum Key Distribution Testbed

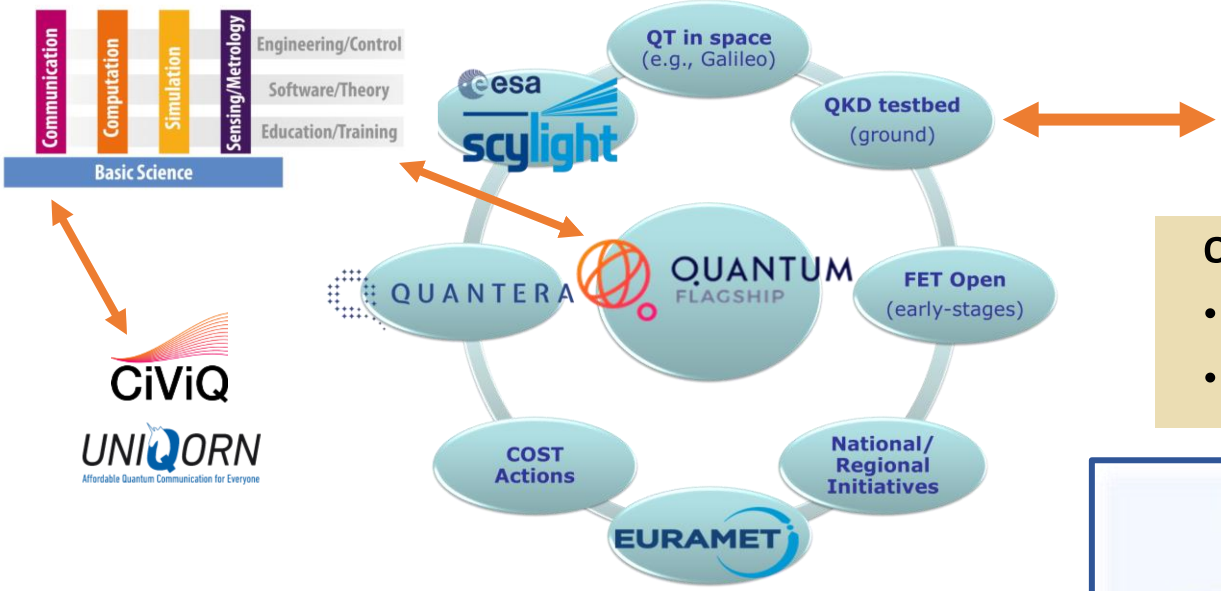
Andreas POPPE
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Vienna, Austria

andreas.poppe@ait.ac.at

This project has received funding from the European Union‘s Horizon 2020 research and innovation programme under grant agreement No 857156.

Coordinated by: AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Framework Programme H2020 + EU Project OpenQKD



Communication

Computation

Simulation

Sensing/Metrology

Engineering/Control

Software/Theory

Education/Training

Basic Science

CiViQ

UNIQORN

Affordable Quantum Communication for Everyone

esa

scylight

QT in space (e.g., Galileo)

QKD testbed (ground)

QUANTERA

QUANTUM FLAGSHIP

FET Open (early-stages)

COST Actions

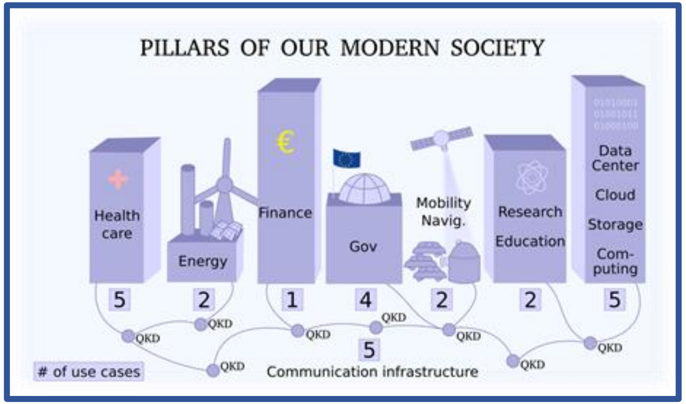
EURAMET

National/ Regional Initiatives

OPEN QKD

QKD Testbed Infrastructure:

- Sep. 2019 – Feb. 2023
- Project size: 18 M€

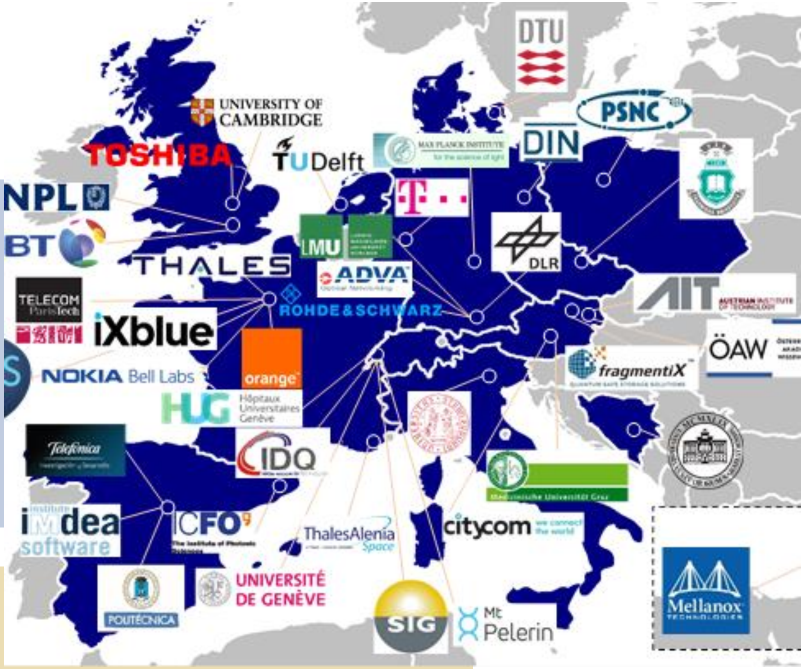


- More than 35 QKD systems in field deployments
- Free-space und simulation of satellite QKD
- Open calls to attract external partners

Objectives of OpenQKD

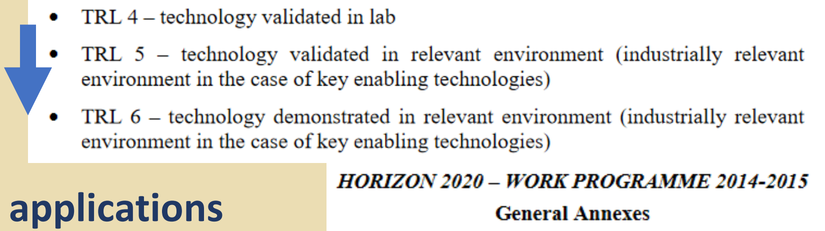
Wide spectrum of 38 partners with different background:

- Telco operators
- QKD developers
- Suppliers of classical network equipment (encryption)
- End-users
- Academic groups



Motivation and benefits:

- Experimental testing platform to **increase TRL** of components, devices and systems
- Kick-start European QKD industry
- Demonstrate high maturity of technology
- OpenQKD support standardisation and certification
- Cooperation with **end-users to demonstrate real world applications**
- Pilot for pan-European quantum communication infrastructure



- TRL 4 – technology validated in lab
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)

HORIZON 2020 – WORK PROGRAMME 2014-2015

General Annexes

Use-cases

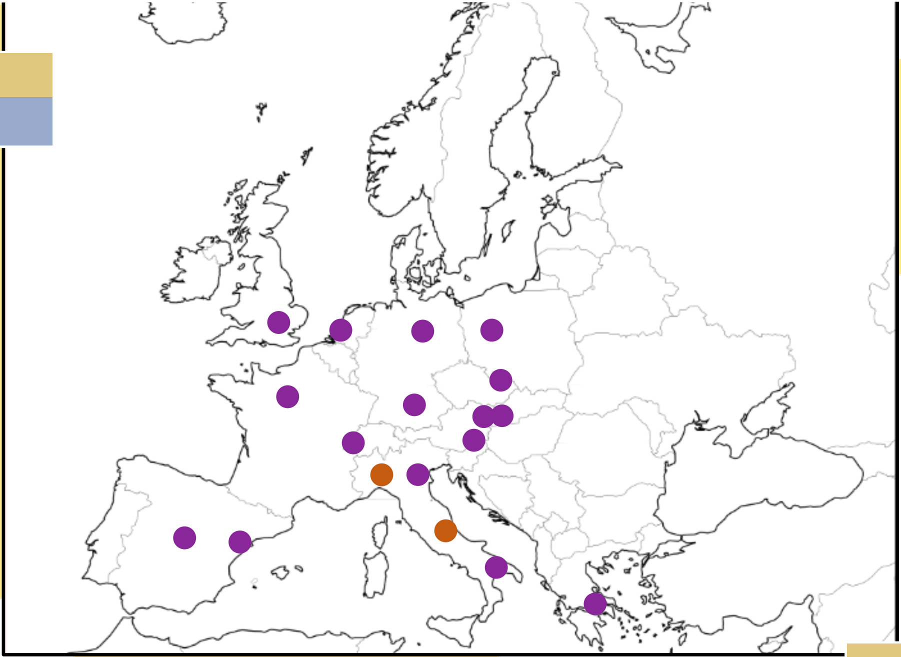
Within OpenQKD we will demonstrate different kinds of use-cases:

- **32** different official use-cases defined in the original proposal of OpenQKD
  - List at our project homepage https://openqkd.eu/openqkd-in-action/
  - Will be operated at 16 different sites
  - Use-cases with the numbers **UC01 – UC32**
- **7** additional use-cases born in the project
  - Partners at 3 different locations agreed to extend their demonstrations
  - Use-cases with the numbers **UC33 – UC39**
- **9** additional funded use-cases from the first wave of open calls **UC40 - UC48**
- **X** use-cases from the second round of open calls (X>7)

18 OpenQKD testbed sites

OPEN QKD

Large geographic reach-out



Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

Cambridge UK
Data Centers

Paris FR
Academic network

Oberpfaffenhofen DE
Satellite QKD

Geneva CH
Smart Grid

Barcelona ES
Video Com

Torino IT
Telecom 5G

L'Aquila IT
Telecom multi-core

Athens GR
Data Com

Ostrava CZ
High Perf. Comp.

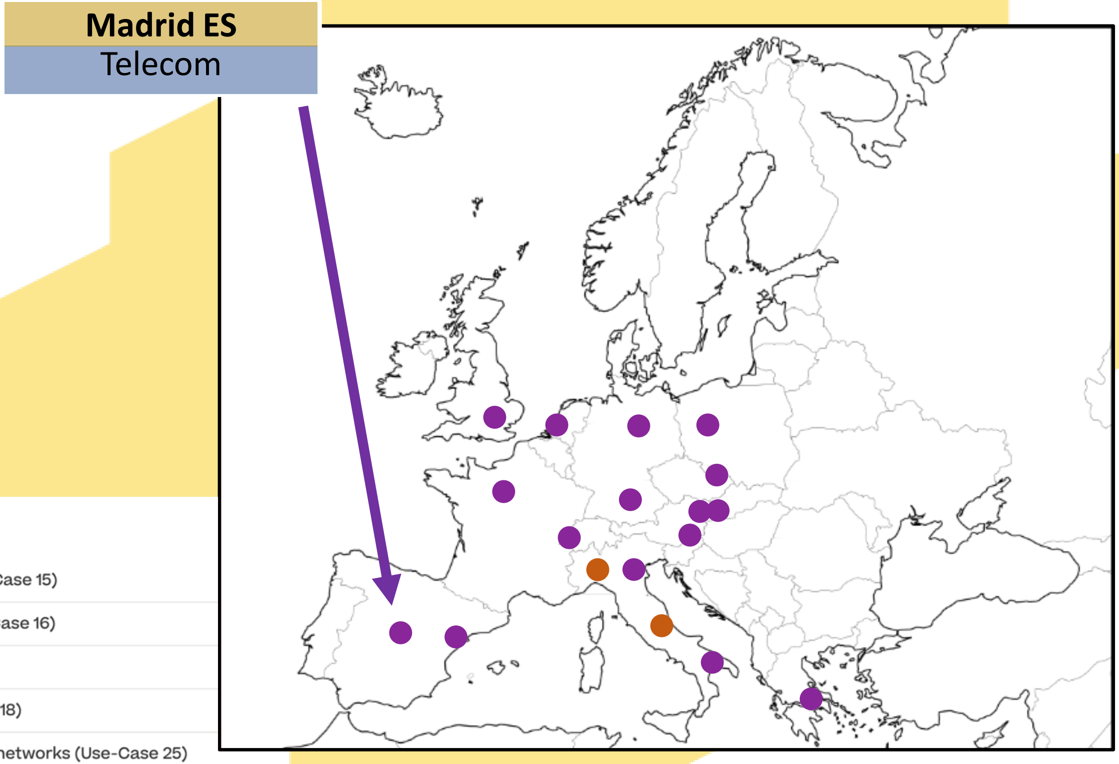
Bratislava CZ
Government

Graz AT
Healthcare

Padua IT
Free-space QKD

Matera IT
Satellite QKD

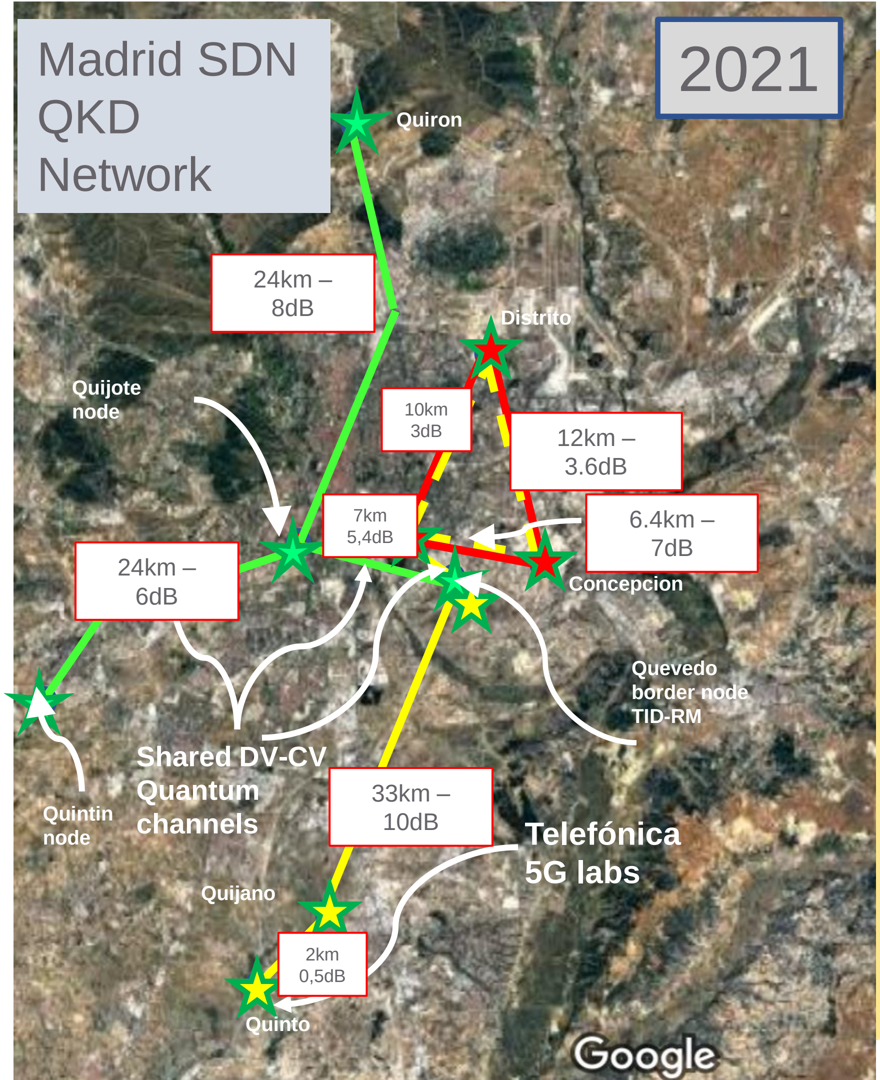
Operation of SDN with QKD



Madrid, ES

- + Network security and attestation (Use-Case 15)
- + Critical infrastructure protection (Use-Case 16)
- + QKD as a cloud service (Use-Case 17)
- + Security in e-health services (Use-Case 18)
- + Quantum cryptography for B2B and 5G networks (Use-Case 25)
- + Self-healed network management (Use-Case 26)

Madrid SDN QKD Network



★ Deployed, full installation.

★ Moving, (prev. Lab. installation)

★ Expected, (summer)

BoM:

- 8 QKD pairs (DV: 2xC & 1xO band, 5 CV, O Band)
- 5 QKD pairs pending (Before summer)
- Optical transport equipment.
- Level 1 & Level 2 encryptors

Important: **A real world network**.

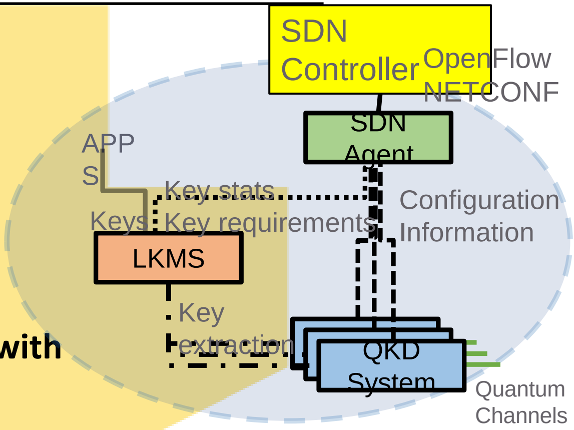
Shared quantum and Classical infrastructure, including optical fibre. **CV+DV systems on the same Fibre**. Two **connected operators**. **Several manufacturers** (quantum and Classical, QKD & encrypt.) **Production facilities.**

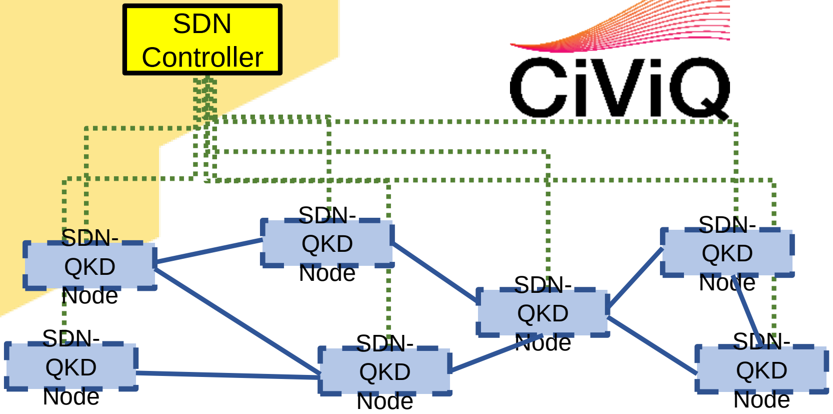
The 2018 versión:
“The Engineering of a SDN Quantum Key Distribution Network”
IEEE Comms. Mag. July 2019, doi: 10.1109/MCOM.2019.1800763;
http://arxiv.org/abs/1907.00174

Key Basic Technologies Deployed

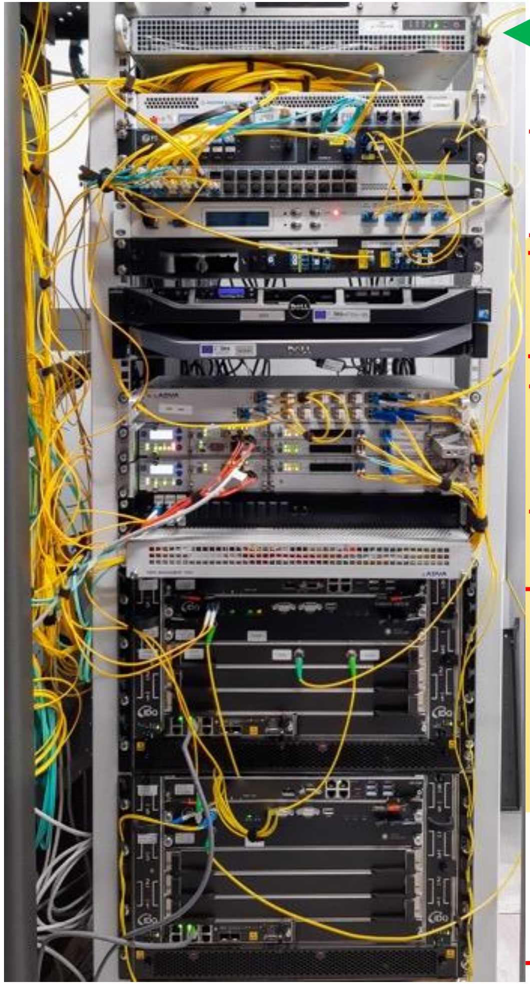
SDN-based software stack

- **Transparent routing** of keys, **end-to-end**, over the whole network.
  - Among different vendors
  - Among different networks (border nodes)
- **Network-wide Key Manager**
  - The objective is actually the integration in existing industria grade KM
- Integration of **QKD keys in the main L2&L3 protocols** (including **hybridization with classical keys** and derived services)
  - TLS → Https, pop, imap, smtp etc.
  - IPSec →Any E2E protocolo/application IP service (Eg. VPN, SCADA)
    - Also used for 5G channel securization
  - Can mix QKD keys with D-H either RSA or PQC
- High level (external and internal) **services integration**
  - Network Function Virtualization protection based on QKD
  - Secure Ordered Proof of Transit (Quantum service chain verification on the fly)
  - Self-healed infrastructure protection
  - ZeroQonf: Auto QKD link-up





OPEN QKD



R&S L2 encryptor

OADM+programm. Switch (add/drop Quantum Channels)

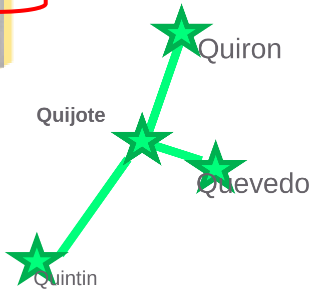
SDN server

ADVA OTN + Link encryptor

2 idQ DV QKD (C and O-band, 1550 nm + 1310nm) OpenQKD systems

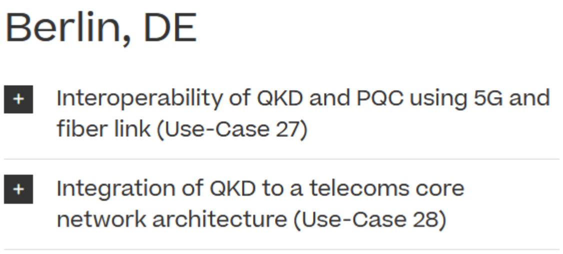
2 HWDU CV QKD + 2 servers From CiViQ

Quijote
a “central” Node



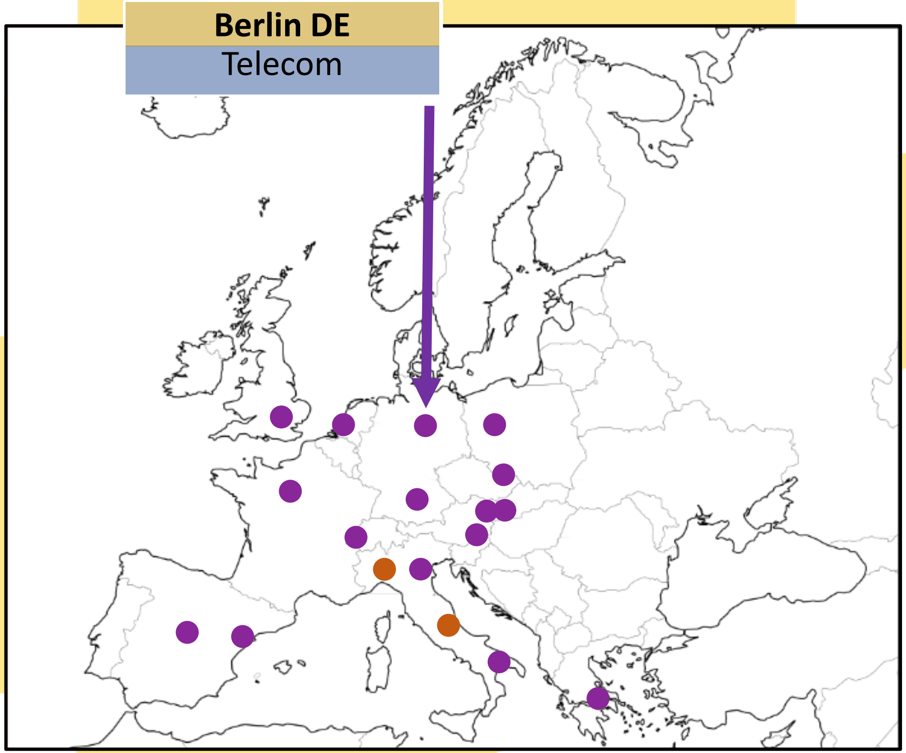
- 2 Quantum & service channels DV and CV from/to previous/next node. Compatibility in C & O bands in same fiber.
- Classical communications in bidi fiber, cyphered L1, L2 & L3 traffic.

QKD integration in 5G and PQC



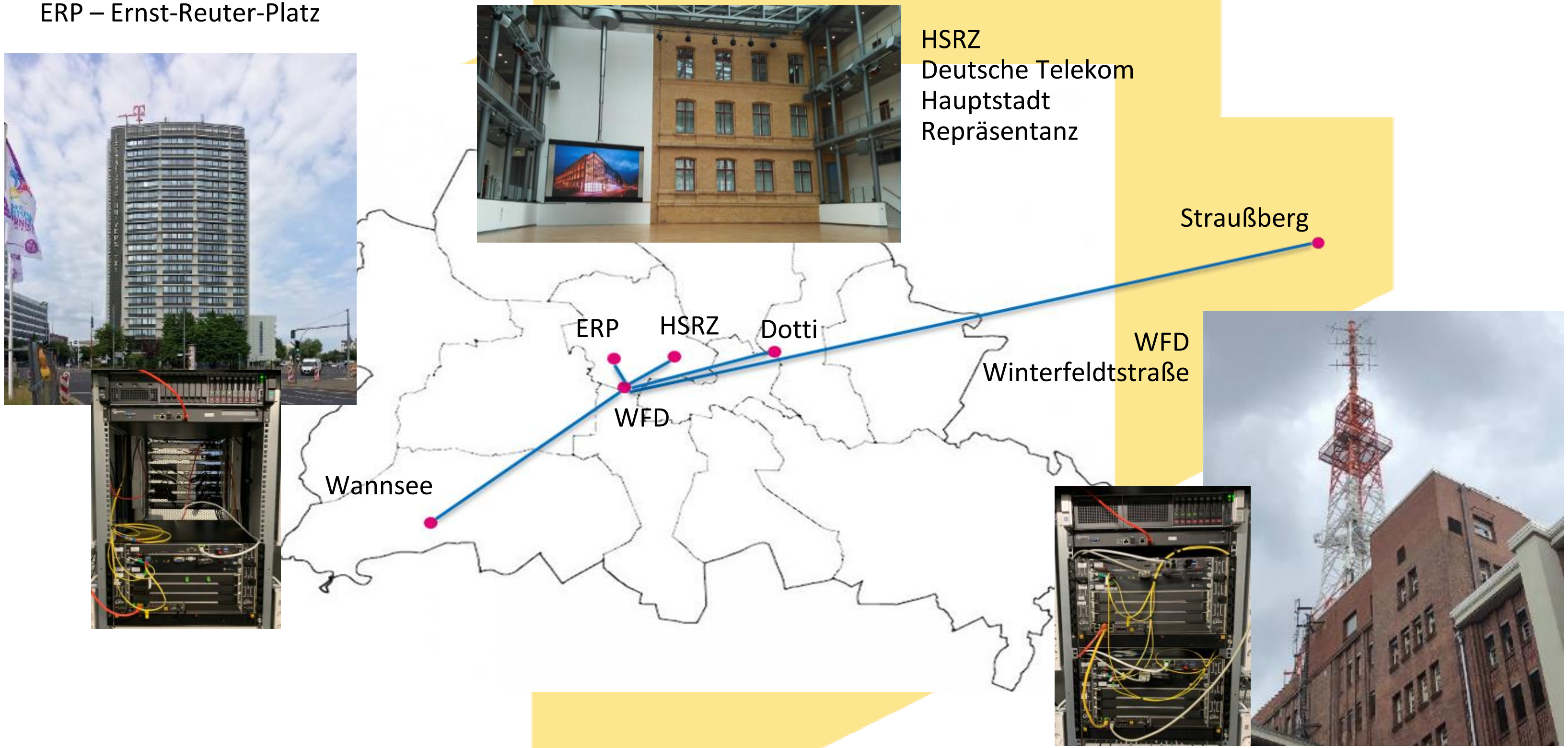
Berlin, DE

- + Interoperability of QKD and PQC using 5G and fiber link (Use-Case 27)
- + Integration of QKD to a telecoms core network architecture (Use-Case 28)



Berlin Testbed Overview

ERP – Ernst-Reuter-Platz



HSRZ
Deutsche Telekom
Hauptstadt
Repräsentanz

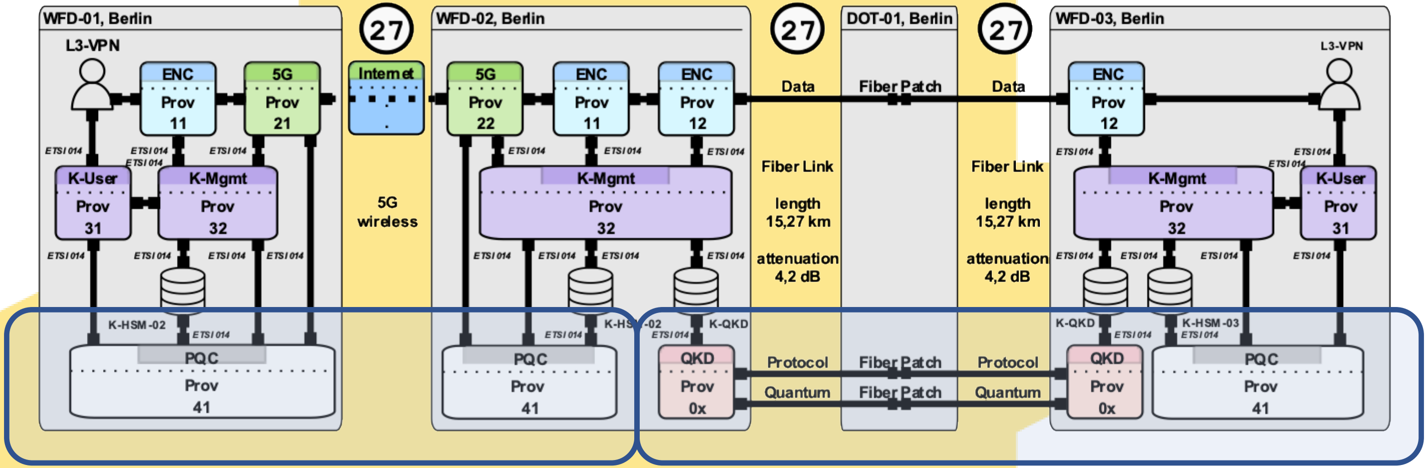
WFD
Winterfeldtstraße

OpenQKD – TestNet Berlin – UC#28 /#27

Architecture

- Layered network
- Network domains
- Network functionalities
- Network performance
- Applications
- Key performance

QKD Prov 01:	idQuantique
QKD Prov 02:	Toshiba
ENC Prov 11:	tbd
ENC Prov 12:	ADVA
5G Prov 21:	DTAG
5G Prov 22:	DTAG
K-User Prov 31:	DTAG
K-Mgmt Prov 32:	DTAG
PQC Prov 41:	DTAG
K-HSM-xy:	DTAG
N-Mgmt Prov 51:	DTAG



- QKD Prov 01 – idQuantique
  - QKD-01 Cerberis System
    Quantum channel at 1310 nm
    1 x 10GBASE Protocol channel
  - QKD-02 Cerberis System
    Quantum channel at 1552,72 nm
    1 x 10GBASE Protocol channel

- QKD Prov 02 – Toshiba
  - QKD-03 Toshiba-01 (TREL#3)
    Quantum channel at 1310 nm
    3 x 10GBASE Protocol channels
    as λs, or as DWDM data channels?
  - QKD-04 Toshiba-02 (TREL#4)
    Quantum channel at 1550,12 nm
    3 x 10GBASE Protocol channels
    as λs, or as DWDM data channels?

- Encryptor Prov 12 – ADVA
  - ENC-01-0x ADVA-01
    FSP3000 DWDM System
    10x10-100G Muxponder
    C-Band tunable

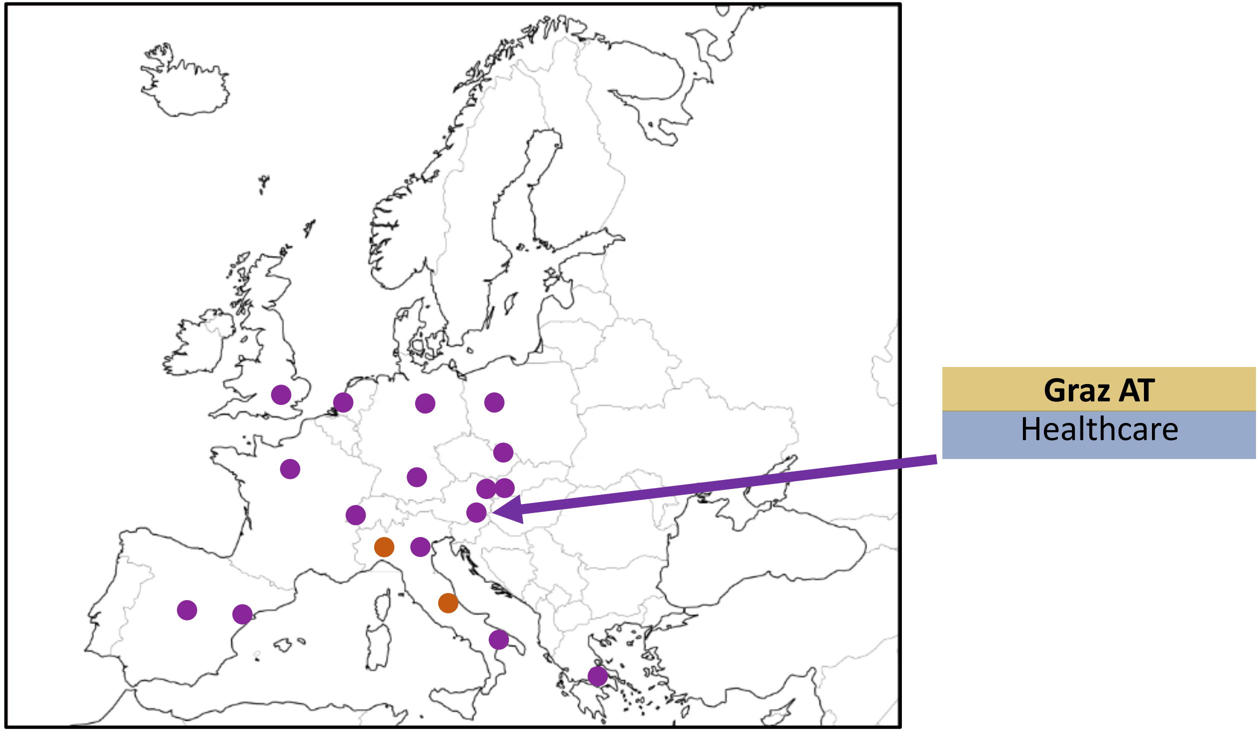
- User application L3-VPN – Thales
  - User devices, L3-VPN getting Keys

QKD: Quantum Key Distribution PQC: Post Quantum Cryptography

Medical use-case in Graz

Graz, AT

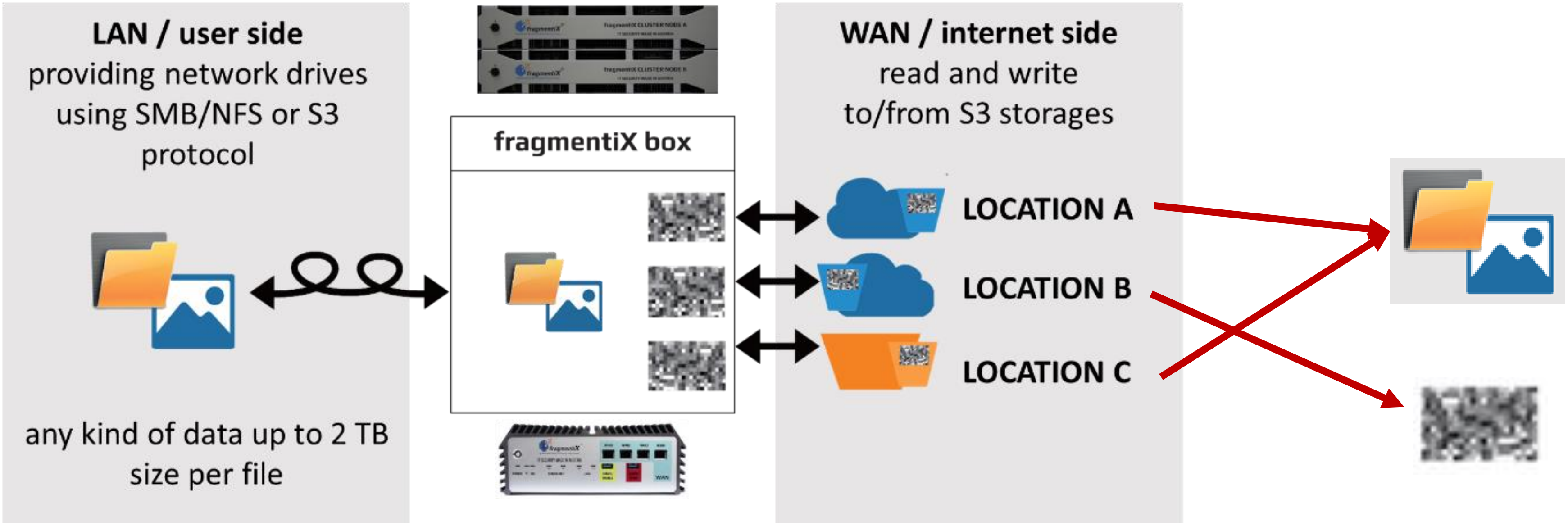
+ ITS securing sensitive medical data at rest and in transit (Use-Case 21)



Graz AT

Healthcare

SHAMIR'S SECRET SHARING



LAN / user side

providing network drives using SMB/NFS or S3 protocol

any kind of data up to 2 TB size per file

fragmentiX box

WAN / internet side

read and write to/from S3 storages

Need at least 2 shares to retrieve full data

A single share yields no information

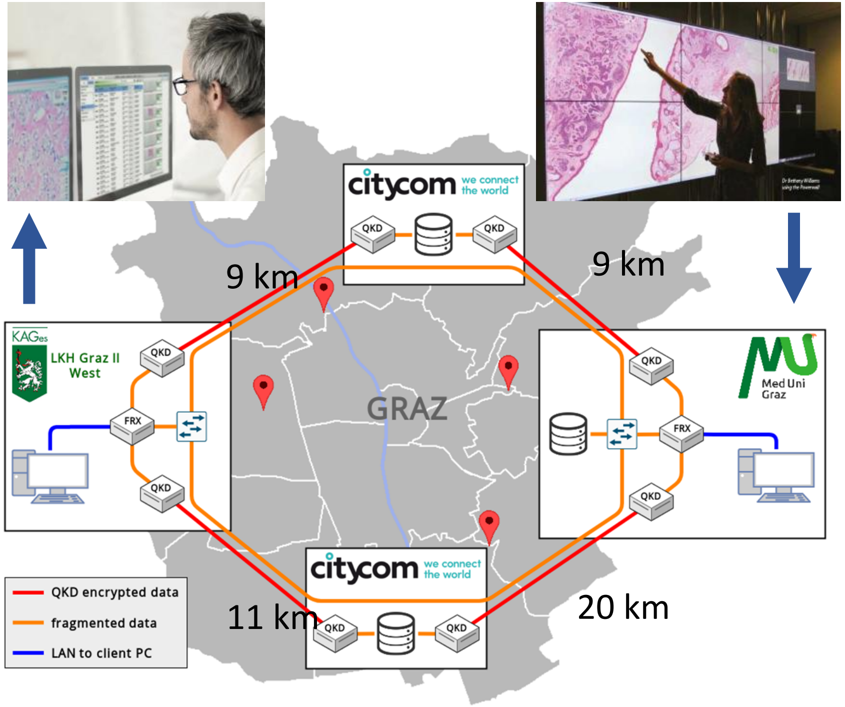
Medical use-case in Graz

OPEN QKD

Deployment finalized in Graz:

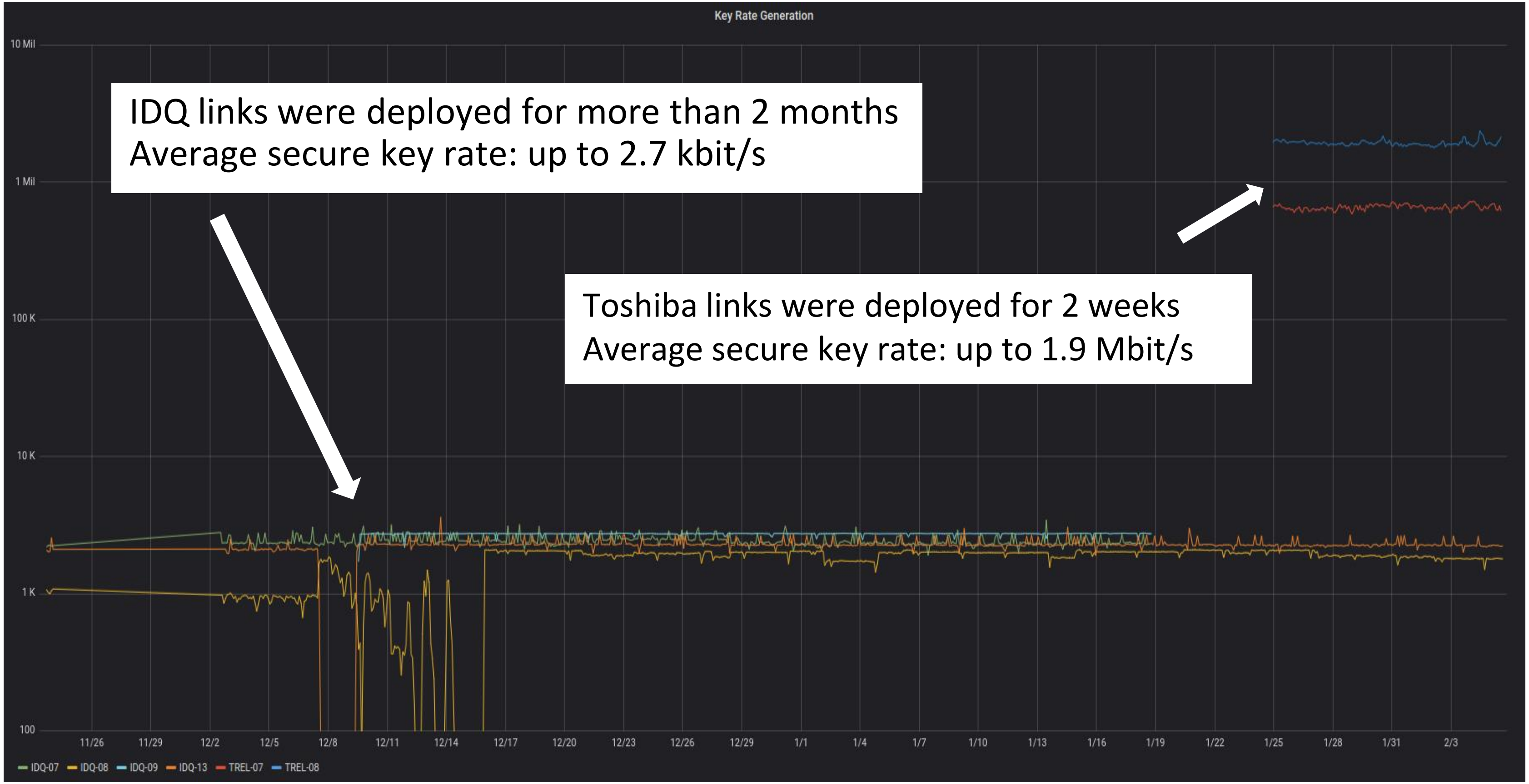
- □ Test of QKD links (4 from IDQ, 2 from Toshiba) and completed under realistic conditions
- □ Fiber infrastructure characterized
- □ Interface to encryptors (ADVA) implemented
- □ Storage solution by FragmentiX

Dry-run of optical network



Geographic layout of network nodes

Secure Key Rates from the Field Test



IDQ links were deployed for more than 2 months
Average secure key rate: up to 2.7 kbit/s

Toshiba links were deployed for 2 weeks
Average secure key rate: up to 1.9 Mbit/s

OPENQKD Get involved

Quantum Industry Board

- Industry discussion forum
- Up to date project info via newsletter
- Face-to-face meetings for QIB members

Register via:

bob@openqkd.eu

Open Calls

- 1.000.000 € to expand project’s innovation power
- 2nd round open now
- Up to 80.000€ per mini-projects
- Applications, use-cases, technological development (HW & SW)
- 2 stage process, brief project idea at stage 1
- Deadline stage 1: **04.06.2021**

More information on: www.openqkd.eu/getinvolved