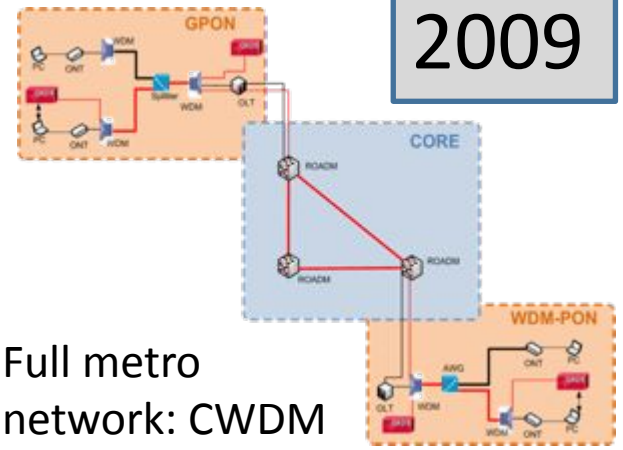
Orchestrating Security: QKD SDN and KM in production networks

Juan Pedro Brito Méndez
juanpedro.brito@qoolnet.eu

Universidad Politécnica de Madrid
QoolNet.

Vicente Martín (vicente@qoolnet.eu)
Laura Ortiz (laura.ortiz@qoolnet.eu)

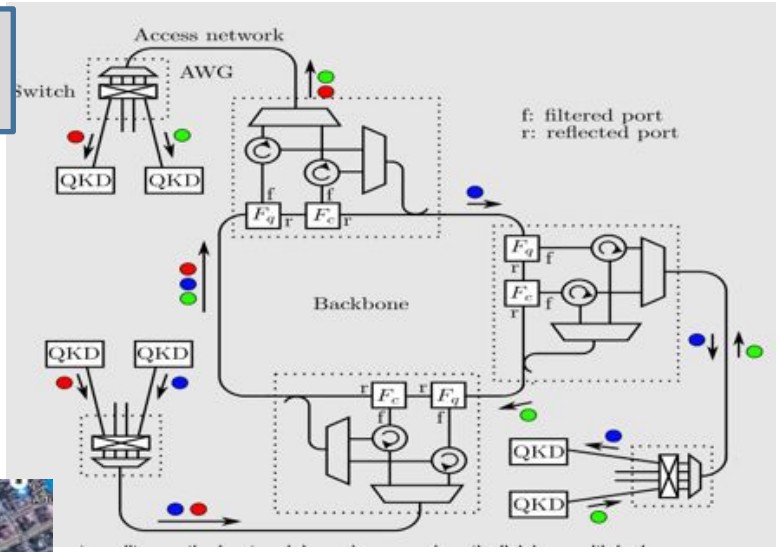
Evolution of Madrid Quantum Communication Infrastructure



2009

Full metro network: CWDM core + GPON access

2014



2018

"The Engineering of a SDN Quantum Key Distribution Network" IEEE Comms. Mag. July 2019, Special number "The Future of Internet" doi: 10.1109/MCOM.2019.1800763 ; http://arxiv.org/abs/1907.00174

- Industrial participation.
- Real world network installed in production facilities.
- Full network stack developed by UPM

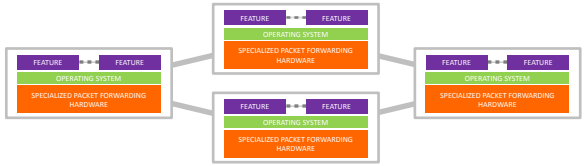
1. Introduction: Why SDN to integrate quantum communications?

Network equipment as Black boxes

SDN

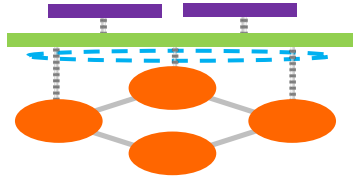
Open interfaces and models for instructing the boxes what to do

Programmability: A SDN controller can manage the Network.

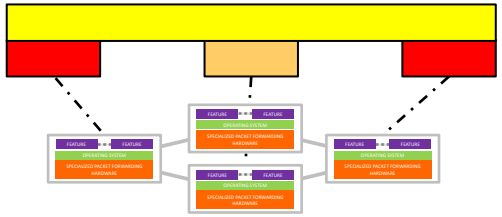


Boxes with autonomous behaviour

SDN

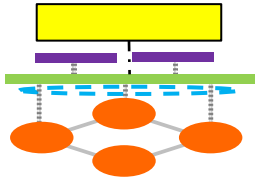


Decisions are taken out of the box



Adapting OSS to manage black boxes

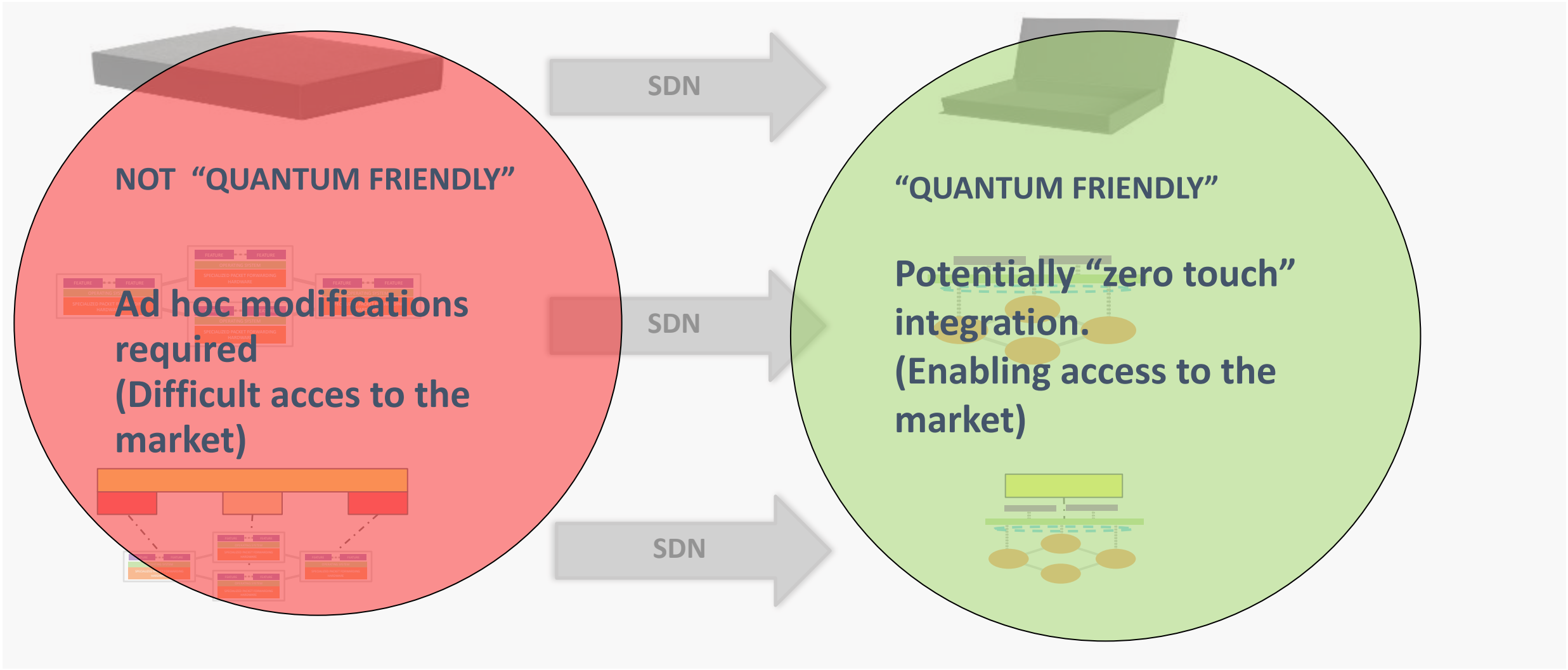
SDN



Simpler OSS to manage the SDN controller

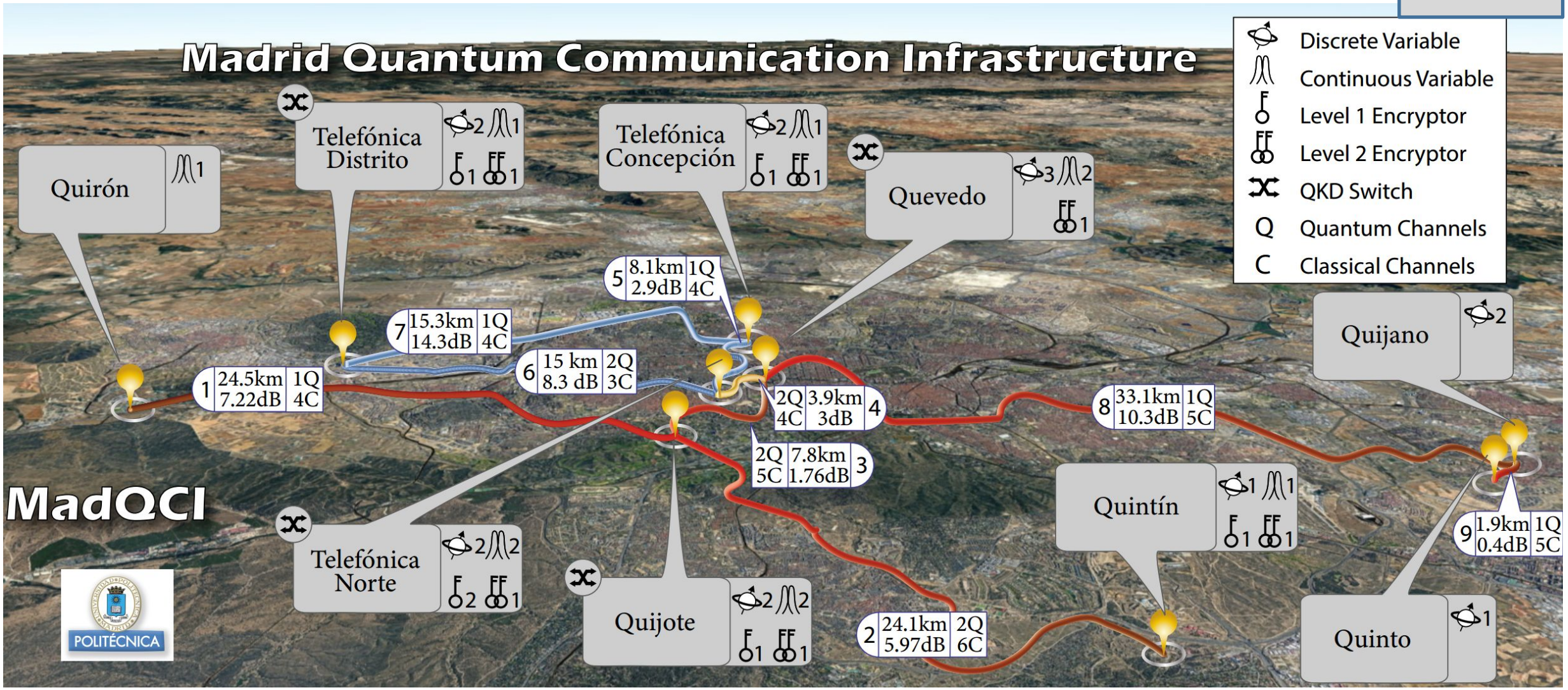
SDN can adapt, allowing for a fast innovation Cycle.

1. Introduction: Why SDN to integrate quantum communications?



Last Madrid Quantum Communication Infrastructure

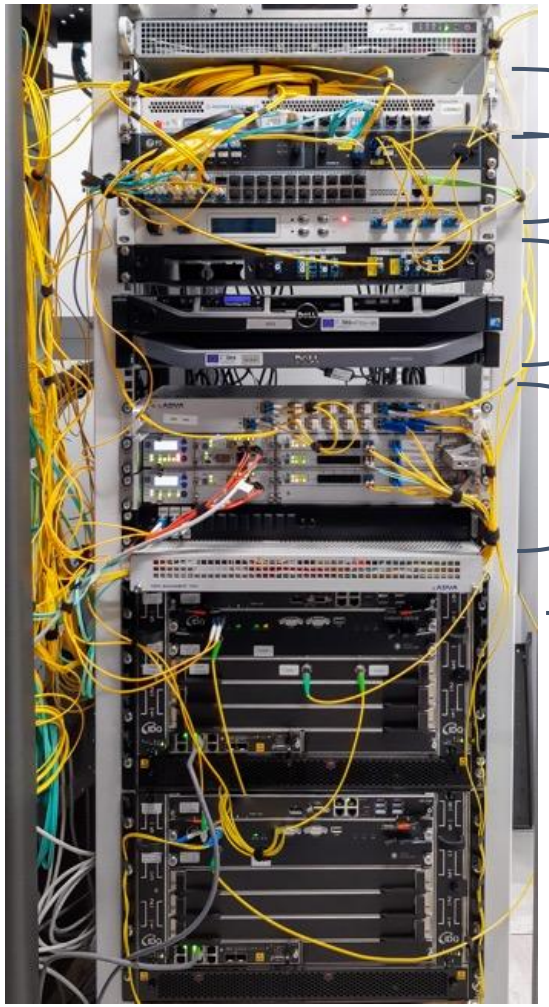
2022



OPEN QKD

CiViQ

Last Madrid Quantum Communication Infrastructure: Trusted Node



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

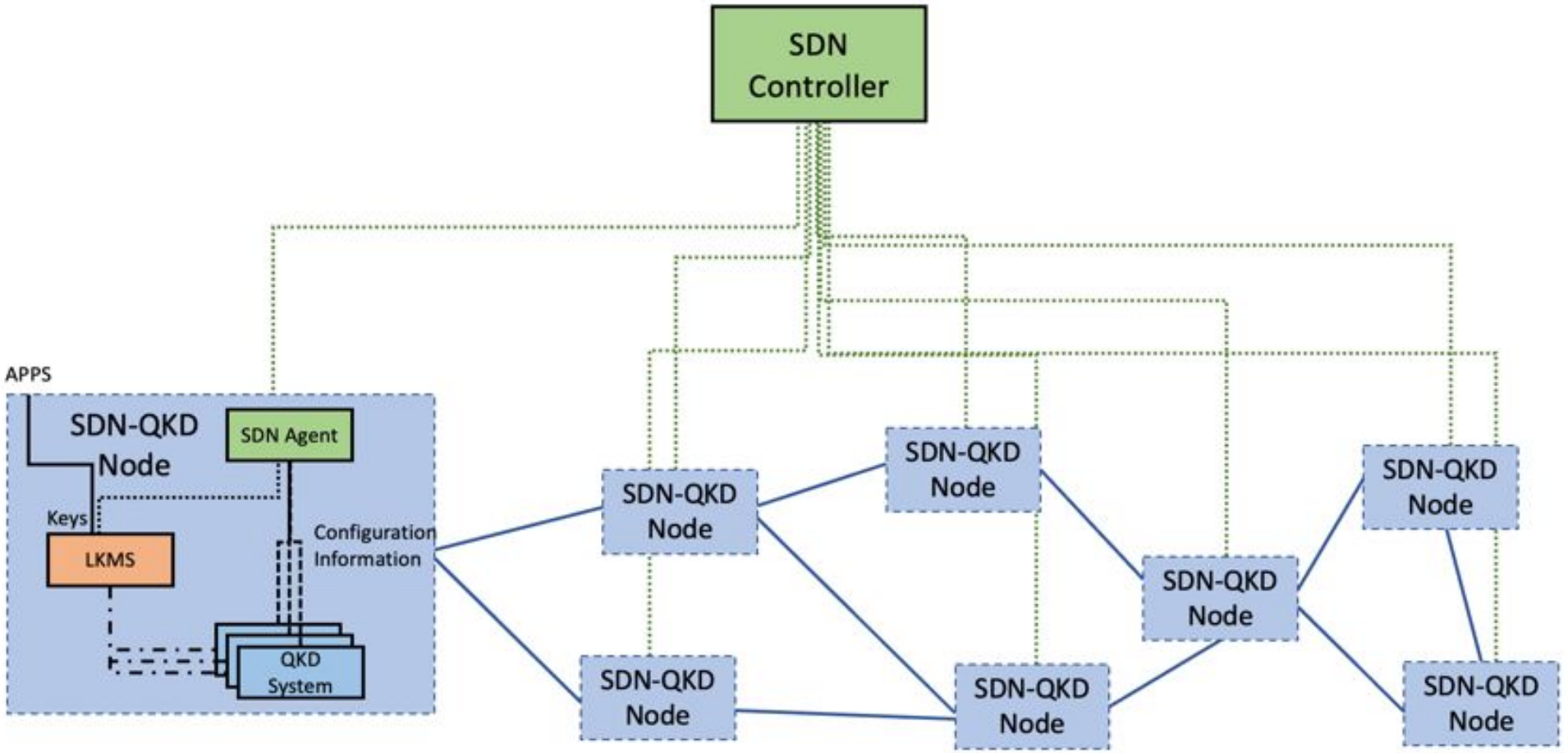
OPEN QKD

CiViQ

QoolNet

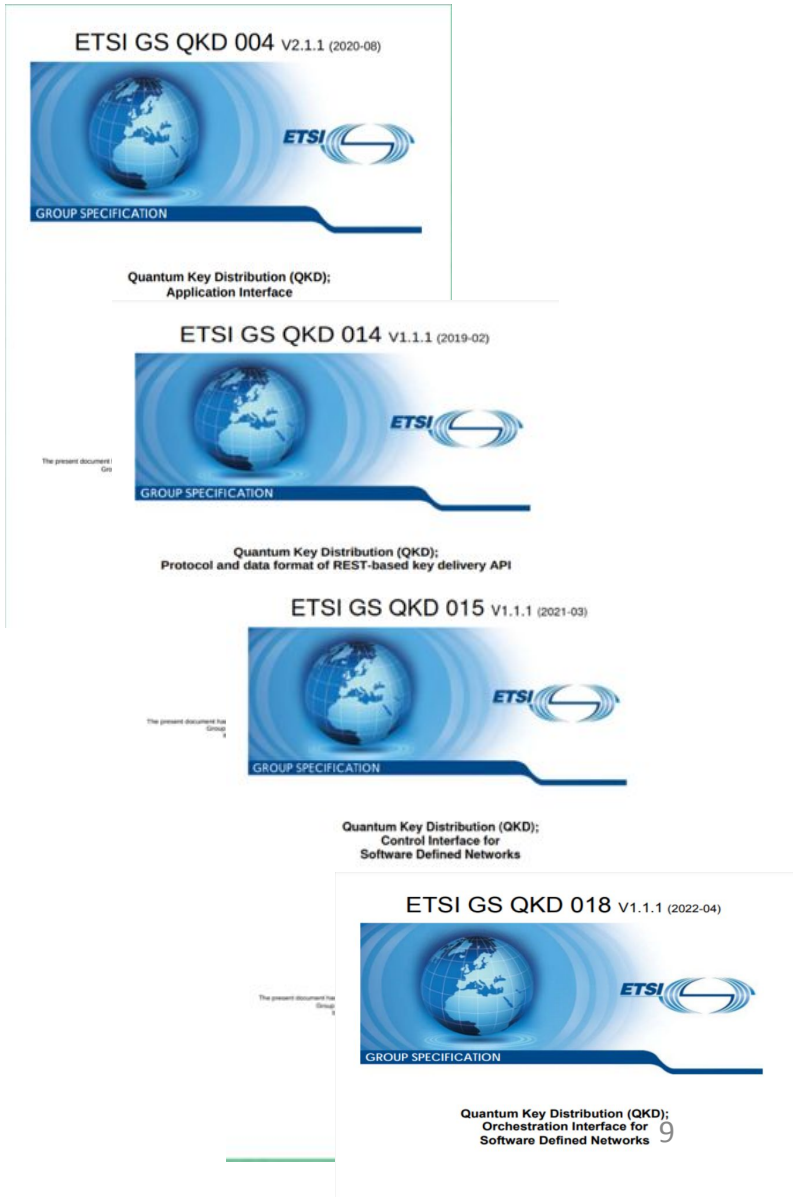
Solution to build and operate **production-ready quantum safe networks**.

SDN-QKD network –> U (SD-QKD Nodes)

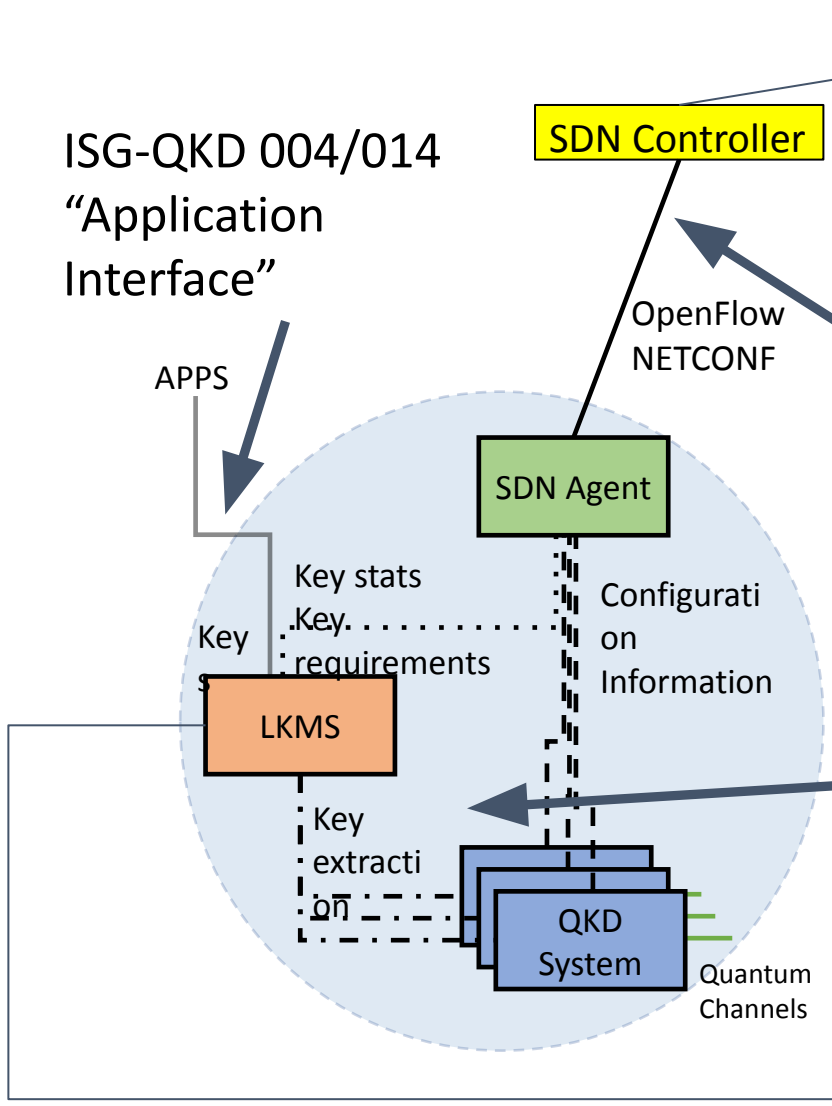


Interoperability through standards

- **European Standardization (ETSI)**
  - **ETSI GS 004**: Application Interface
  - **ETSI GS 014**: Protocol and data format of REST-based key delivery API
  - On going:
    - **ETSI ISG 020**: Protocol and data format of REST-based Interoperable Key Management System API
    - **ETSI ISG 017**: QKD Network Architectures
  - Other necessary standards
    - **ETSI GS 015**: Control Interface for Software Defined Networks
    - **ETSI GS 018**: Orchestration Interface for Software Defined Networks
- **Integration**
  - QKD Vendors
    - QKD devices
    - QKD encryptors adapted
  - Telcos



SDN-QKD-node based network and SDN-helped Key Management Layer



ISG-QKD 004/014 "Application Interface"

ISG-QKD 018 "Orchestration Interface for Software Defined Networks"

ISG-QKD 015 "Quantum Key Distribution Control Interface for Software Defined Networks"

ETSI: Industry Specification Group on QKD.

ISG-QKD 004/014 "Application Interface"

KMS is one of the modules!

SDN-QKD-node based network and SDN-helped Key Management Layer

Regular KMS responsibilities

- Key Management deals with the **generation, exchange, storage, use, destruction and replacement of keys.**
- KMS systems are typically focused on **public key cryptography.**
  - Eg. NIST 800 – 53 (parts 1 to 3) / -56A/B/C / FIPS 140-3 etc.
- KMS use a **variety of crypto algorithms, serving many users** (might be heavy on CPU requirements).
- KMS are **complex systems** used on critical infrastructures
  - NATO
  - Governmental agencies
  - Military infrastructures
- As a keystone of cybersecurity, they require a **high certification level.**
- It is a very complex module!

SDN-QKD-node based network and SDN-helped Key Management Layer

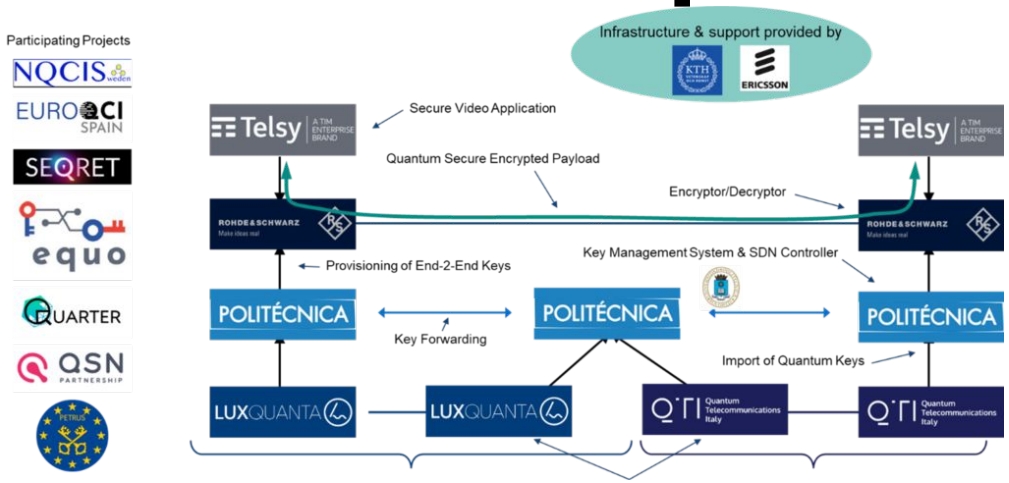
QKD KMS What's different?

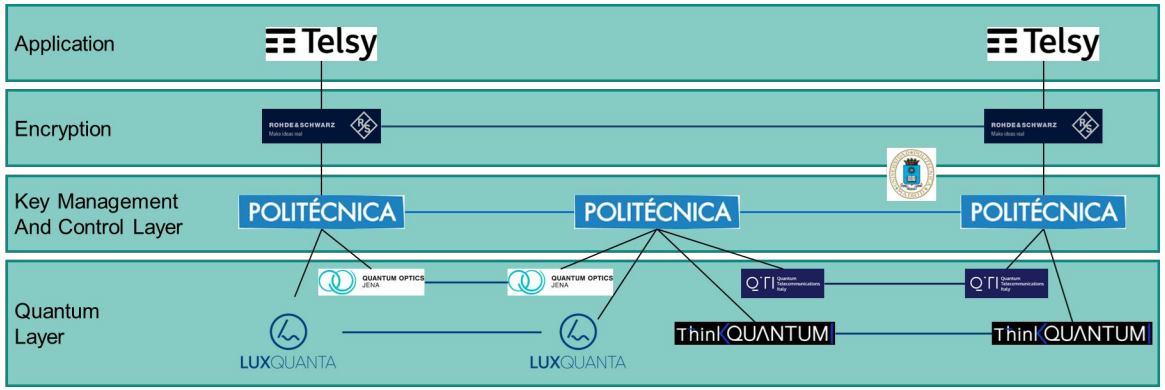
- Deals with **symmetric crypto**. It is the connection point of the apps.
- Adapted to a **continuous flow of symmetric keys among many devices.**
- Use ITS primitives.
  - **QKD KMS consumes QKD keys.**
- Support of **new functionality** (e.g. mix keys from different protocols /paths / manufacturers to increase the security)
  - Hybridization of key material.
- **In practice:**
  - Currently **low TRL** (sp. Network level) but increasing maturity day by day!
  - Need to **deal with a variety of QKD systems** (not necessarily very much standardized. Some experimental -> **Interfaces** to network and apps.)
  - Strange mix of tasks: Used also for **Key transport**/routing (on behalf of the network). **Not a Key management task!**

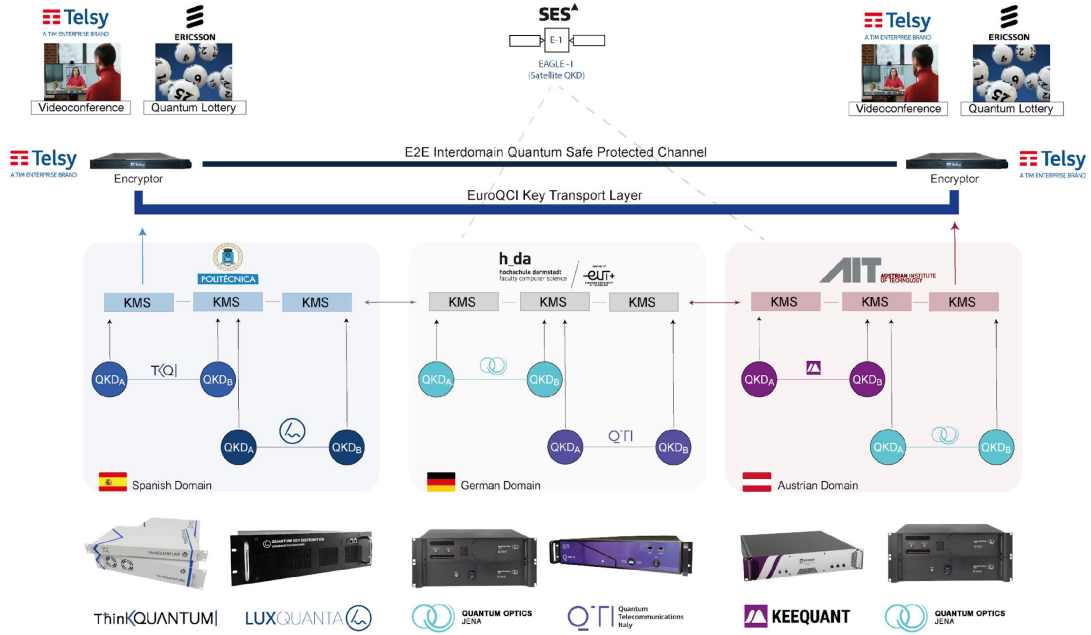
SDN-QKD-node based network and SDN Key Management Layer

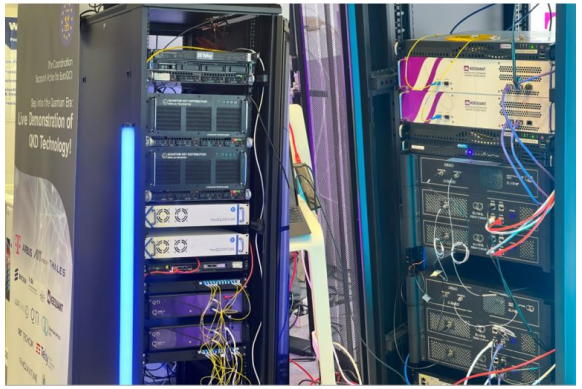
- Based on open standards → QoS ready by nature (ETSI GS QKD 004)
- Continuous stream of key, even concurrently to multiple applications running on parallel on different links
- Highly softwarizable and extensible -> It makes the KMS easy to update and maintain
  - It simplifies the QKD side focusing the work on the key generation process and not their maintenance
- Minimal integration efforts on QKD side → Interfaces!
- No need to fully trust your QKD vendors → Combine/Hybridize keys of different vendors, PQC etc
- Highly extensible and configurable, from telcos, software developers, new companies exclusively focused on this topic etc.
- Global KMS Forwarding Plane dealing with multivendor: SDN controller manages all key transport task in a transparent way. → A global KMS layer. It can connect any node in the network, manage several QKD devices per node, without regard of manufacturer and provide keys to any encryptor or application

Proof of Concepts

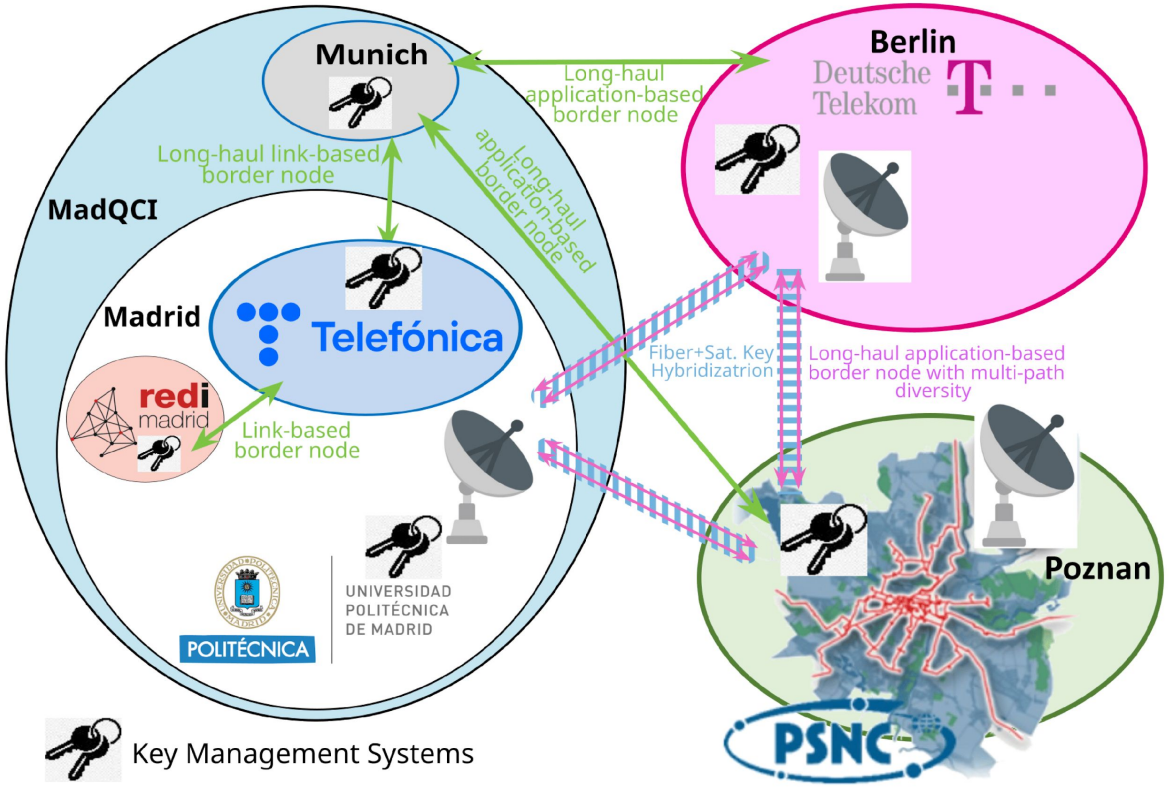








Proof of Concepts

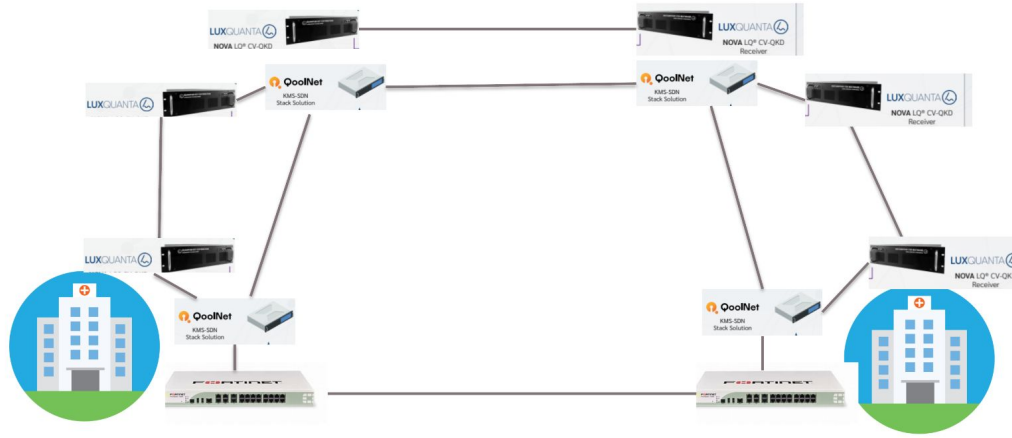


Paper: Linking QKD testbeds across Europe

Anexo arquitectura

Central Madrid Concepción

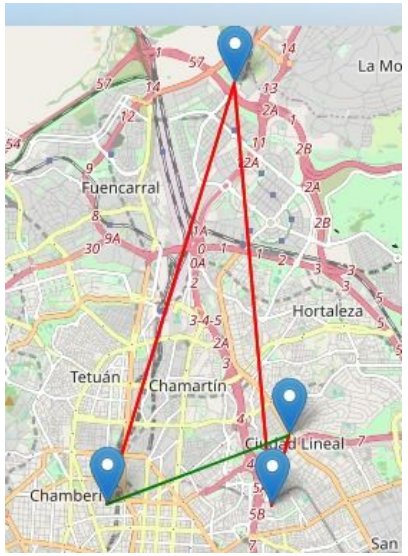
Central Norte



Vithas Arturo Soria

Vithas Milagrosa

eHealth QKD demonstration



Real time demo at MWC

Orchestrating Security: QKD SDN and KM in production networks

Juan Pedro Brito Méndez
juanpedro.brito@qoolnet.eu

Universidad Politécnica de Madrid
QoolNet.

Vicente Martín (vicente@qoolnet.eu)
Laura Ortiz (laura.ortiz@qoolnet.eu)