Telefónica

QKD for network operators

EPIC online Quantum Technology Meeting on Implementing Secure Strategies for Past, Present and Future Communications

Antonio Pastor
Transport & Core. CTIO
Telefónica
09.04.2021

OPEN QKD

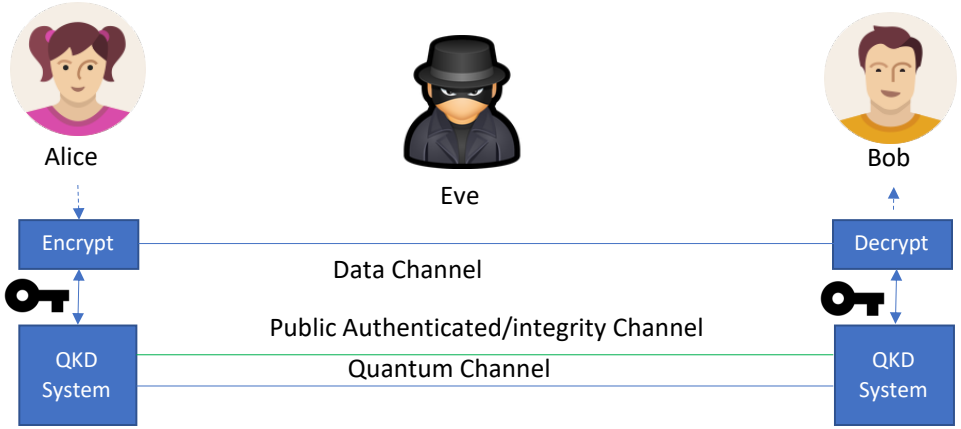
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156.

Quantum Key Distribution system

In a nutshell

Telco vision:

- *"Synchronized source of random numbers…"*
- …that requires *dedicate & delicate* optical transmission resources
- …that open new services opportunities



OPEN QKD

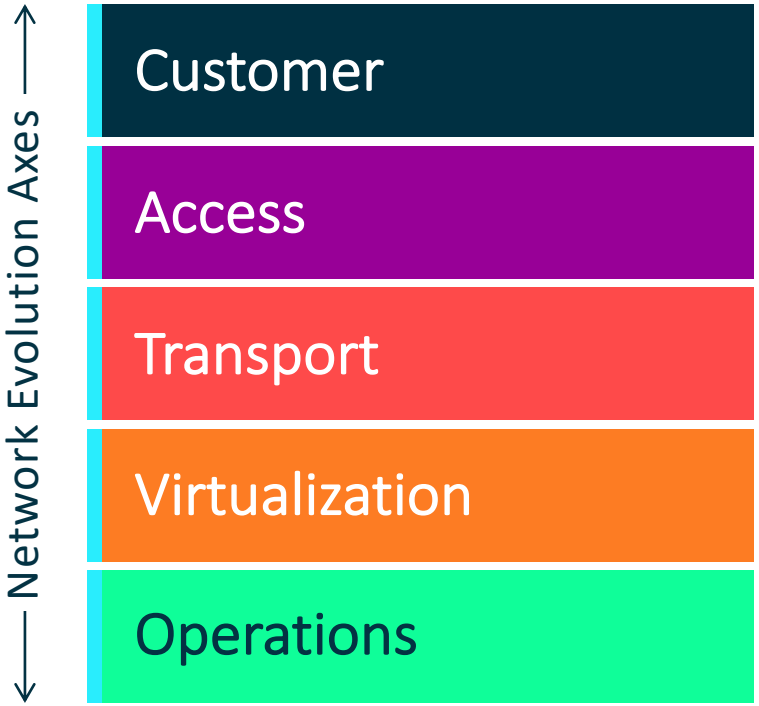
Prepare the deployment of Europe-wide QKD-based infrastructure in future. Pan-European trials for securing traditional industries and vertical application sectors.

Telefonica Activities

- Test QKD vendor devices
- Evaluate applications and use cases
- Interconnect Telefonica QKD network with Redimadrid
- Define management architectures
- Standardization in ITU,ETSI,IETF

Quantum Key Distribution can help operator…

- **Offer secure communication** (ITS)
  - Mathematically proven to be unbreakable and based on the **laws of physics**.
  - **Additional** (physical) layer to **protect network infrastructures**.
- The **only** known **symmetric key distribution** method is **demonstrably secure**
  - You can assume that the attacker can access the channels.
  - Safe even for an attacker with infinite power or computing resources.
- **Immune to any classical or quantum computer attack** (cryptanalysis)
  - Unlike post-quantum cryptography.
  - It will allow to replace (or combine with) current cryptographic key exchange techniques, which are based on public key cryptography.



Madrid Quantum Comms. Infrastructure

Telefonica Spain & RediMadrid in OpenQKD

redimadrid links

Telefonica links

Field-trial on a production network

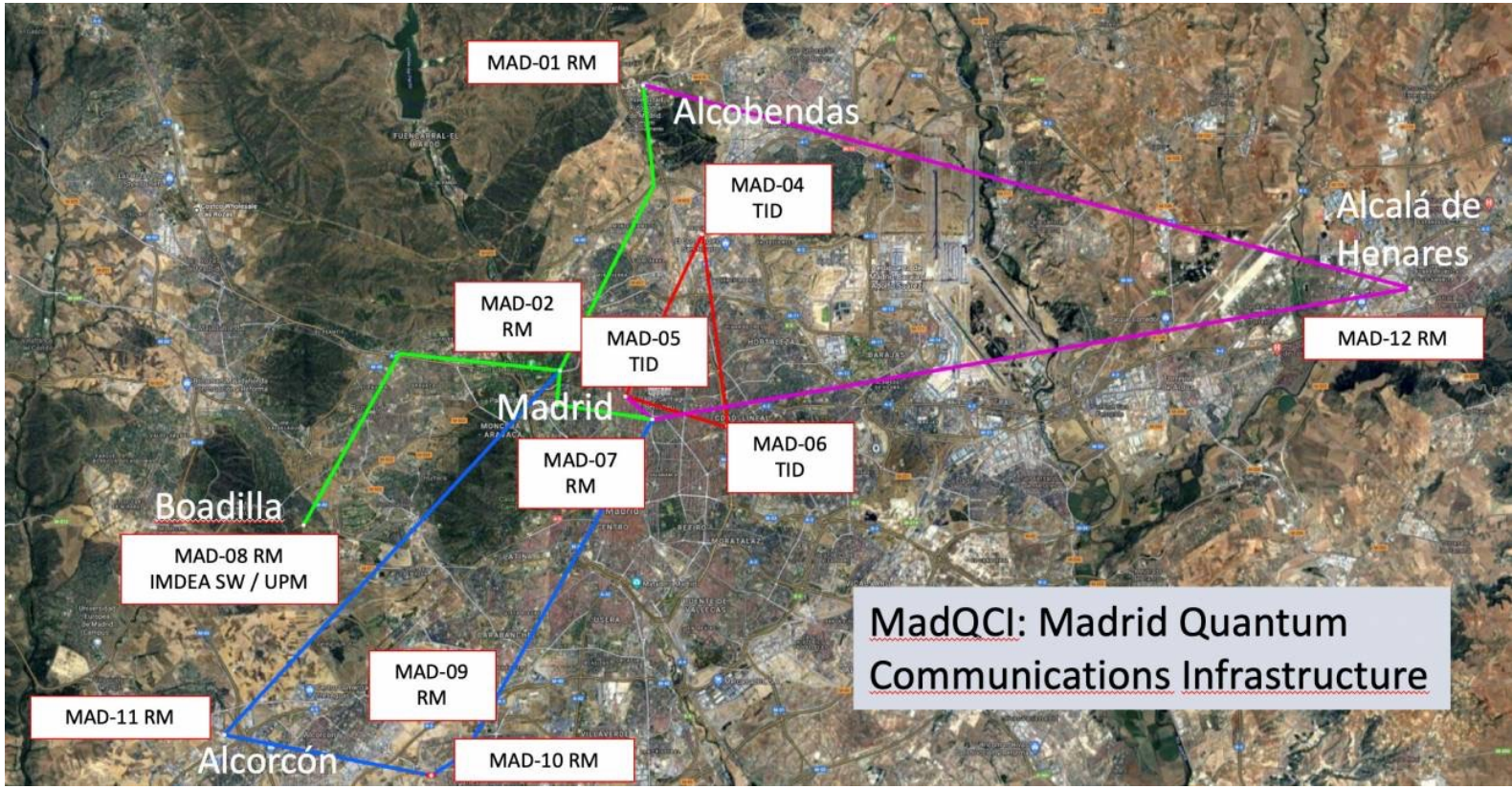
Multivendor (idQ, Toshiba,etc..)

Multi technology (CV-QKD,DV-QKD)

Quantum channel co-propagation

Software-defined Networking (SDN) to manage the QKD resources

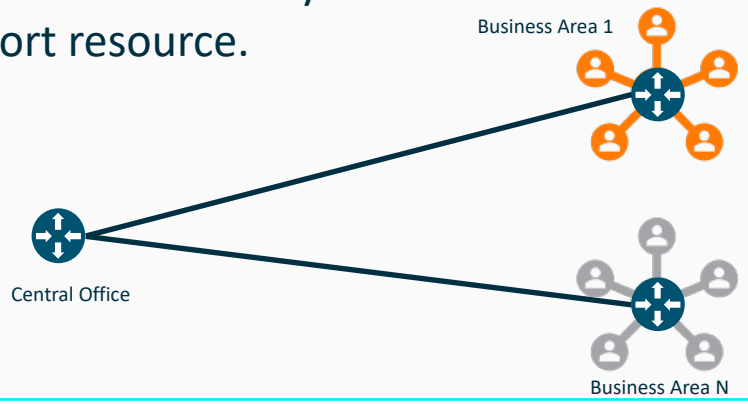
Open calls infrastructure



Customer & access secured with QKD

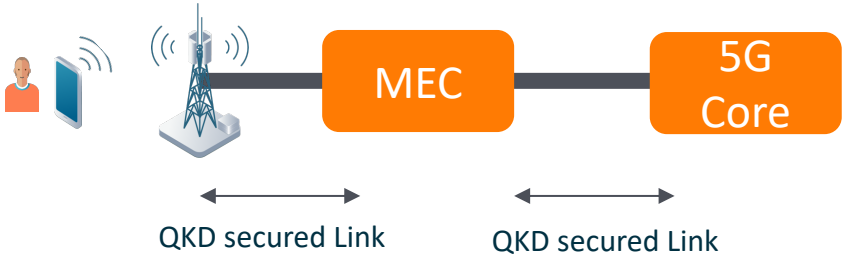
Point to Point connections for local business access

- **Point to point connections** encompass many business offers.
- Business customers with a dedicated fiber resource not shared with another customer are generally very demanding for a connection with a high security level.
- QKD can thus be a way to offer them a more secured transport resource.



Quantum Cryptography for 5G networks

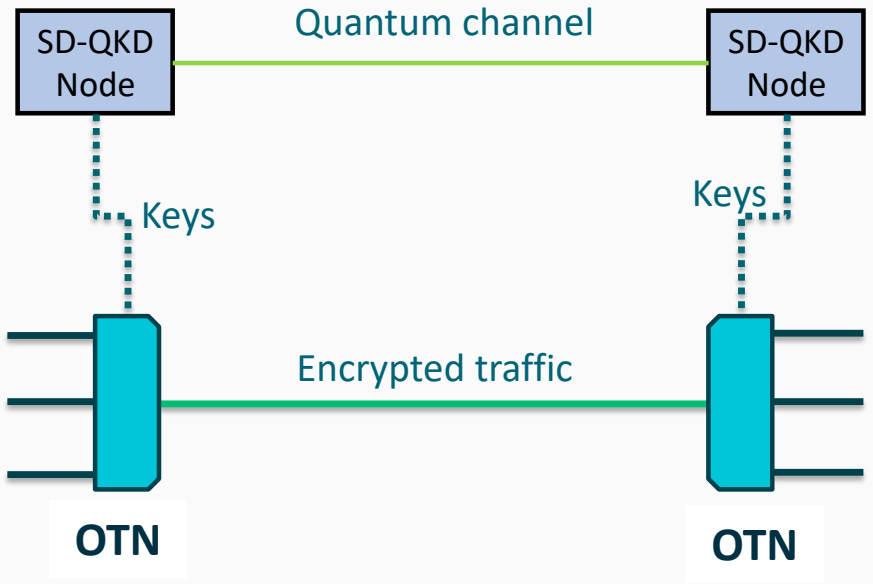
- QKD play an important role securing transport services.
- This will allow encrypting connectivity from **base stations** to **MEC,** and/or **core** (e.g. for 5G), to incorporate quantum-safe security for end users' communications.



End-to-end quantum-encrypted connections

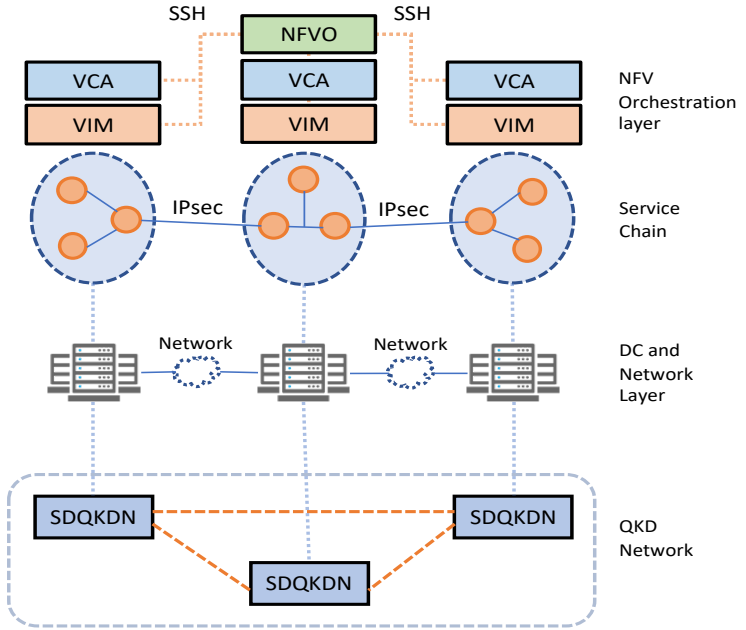
Quantum security embedded in network elements

- Aggregate up to cyphered OTN channels plus the quantum channel



Quantum cryptography for IPSec via SDN

- SDN controller integrates the management and generation of keys (based on a QKD infrastructure) used by IPsec.

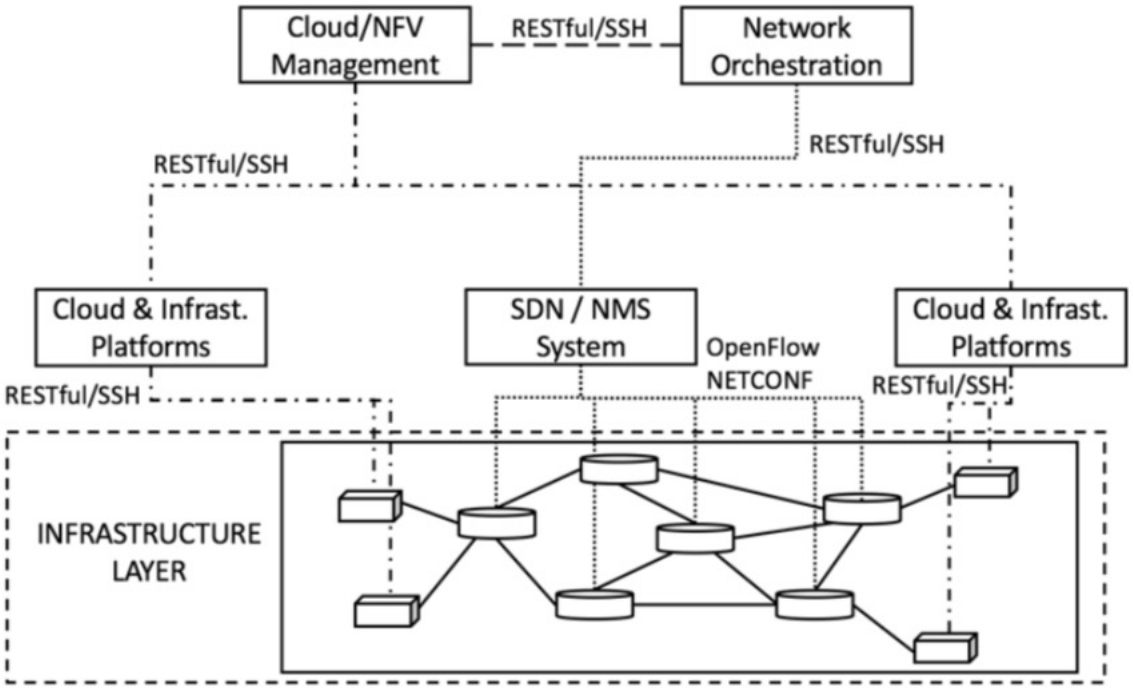


Network management secured with QKD

Planes in operator's network

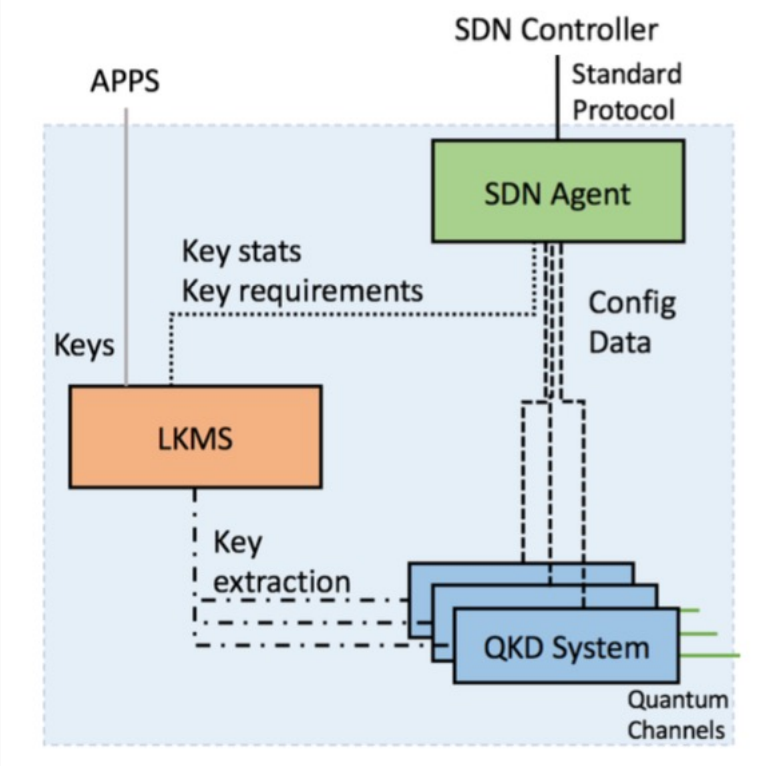
- **Management and control plane** become critical in virtualization environments.
- **Security mechanisms** are meant to be implemented in the network management plane, to securely handle any centralized operation, including the communications channels between **NFV platforms**, the communication between an **SDN controller** and a network device, etc.

Control plane protocols and interfaces within a transport network



Software Defined QKD Networks

Software Defined QKD Node



Control plane protocols and interfaces within a transport network

- **Software Defined Networks** (SDN) enables the **automation** of service provisioning within network operator infrastructures.
- With the **dynamic network requirements**, operators can not anymore deploy their services based on manual intervention or using proprietary vendor solutions.
- **Standard programmability** is key in the next-generation network infrastructure and any new technology must be integrated with this paradigm.

Telefónica