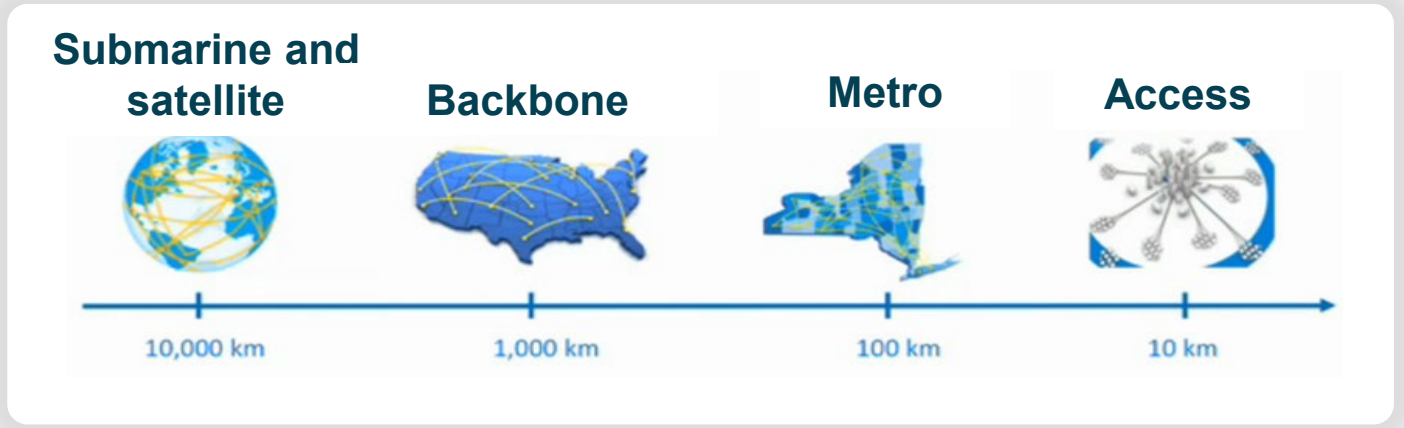
Next steps in QKD from a network operator perspective

Quantum technologies in Spain. The future is now

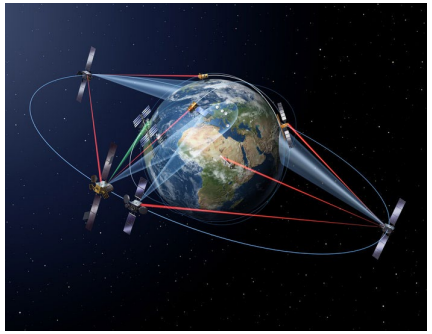
Victor Lopez - gCTIO

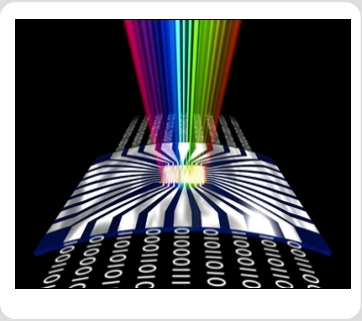
08.05.2019

Telcos have different network scenarios…



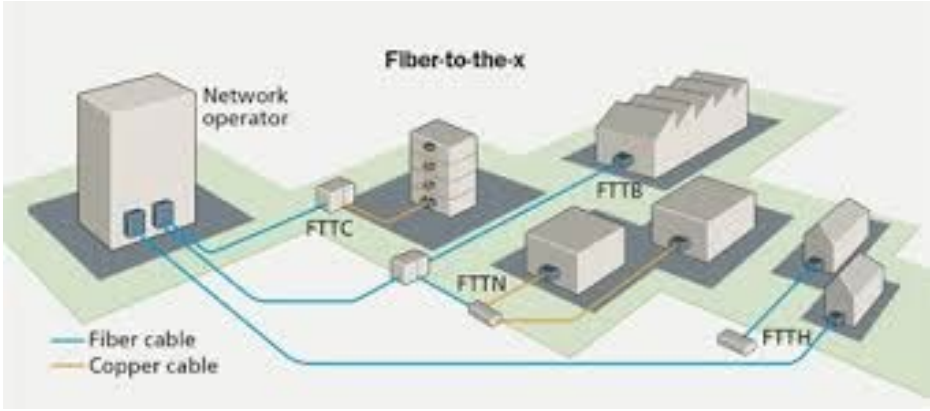
…, technologies…





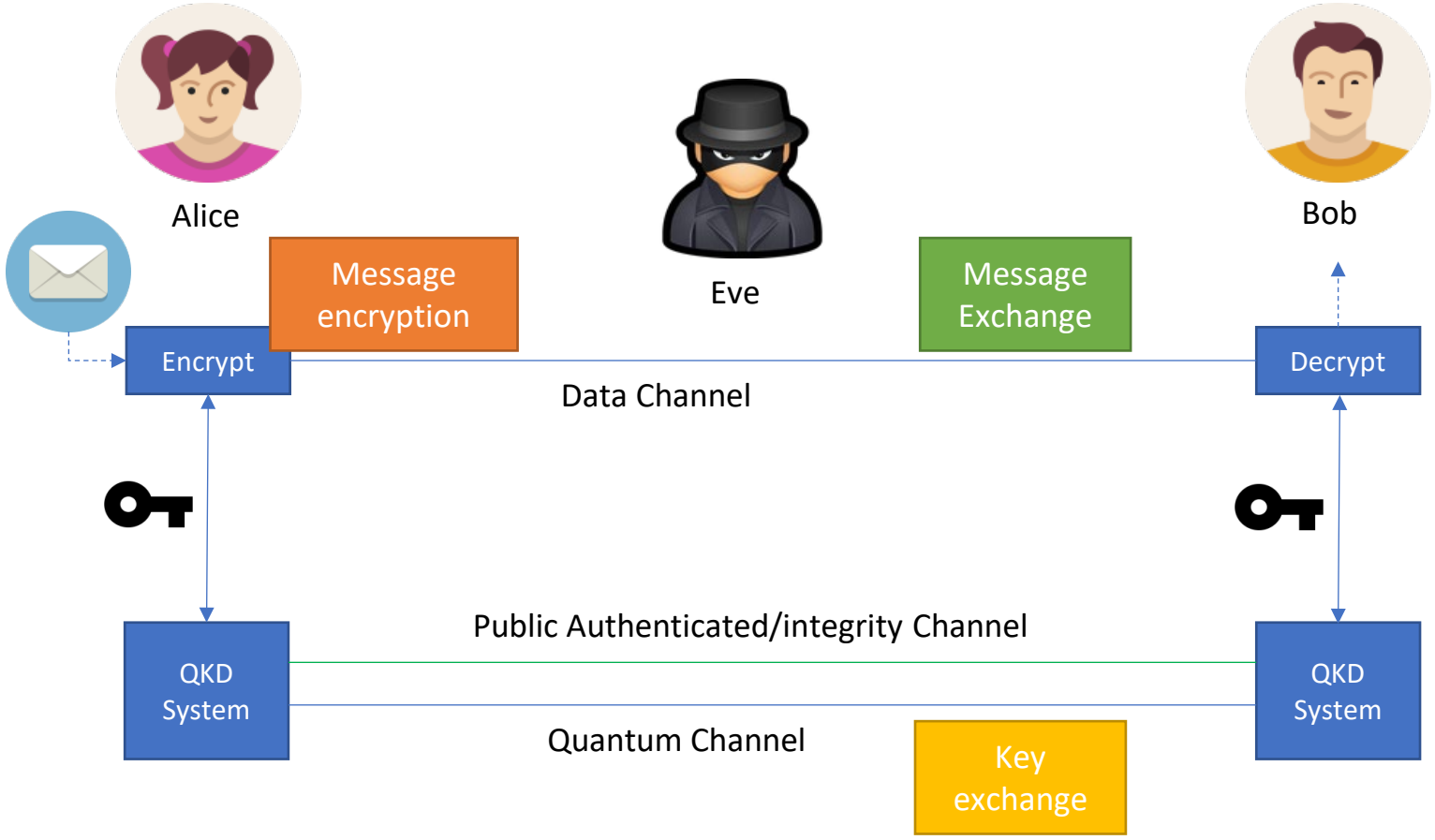
… and planes

- Management Plane
- Control Plane
- Data Plane



#RECONECTA

Quantum Key Distribution system



Ingredients:

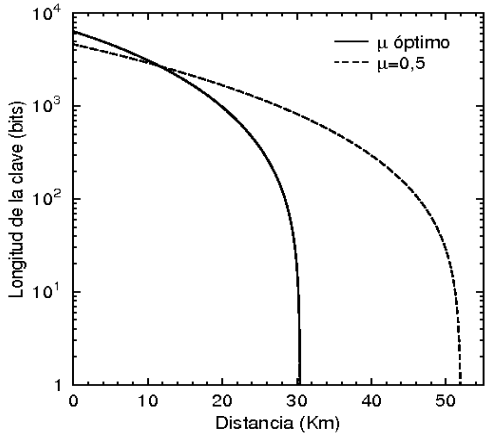
- Qubit **transmitter**: Alice
- Single qubit **receiver**: Bob
- **Quantum channel** (capable of transmitting qubits from Alice to Bob)
- **Public authenticated channel**

Main steps:

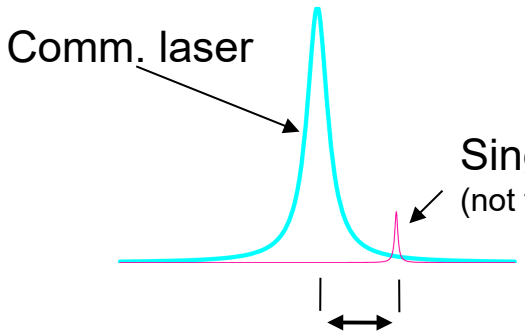
- **Raw key exchange** (using the quantum channel)
  - Qubit transmission
  - Sifting (basis reconciliation)
- **Key post-processing** (using the public authenticated channel)
  - Information reconciliation
  - Error verification
  - Privacy amplification

Quantum communications and networks, why is it difficult?

Limited reach, point to point.



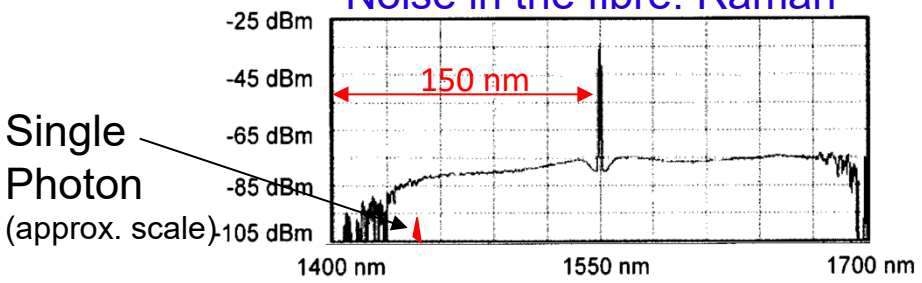
extremely weak signals.



Δλ = 0.2~0.8 nm (DWDM)
Δλ = 3~20 nm (CWDM)

- Difficult to detect.
- Absorpions
- Masked by the noise

Noise in the fibre: Raman



Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

It is a delicate technology.

R. Doisneau

Quantum Cryptography with Continuous Variables: CV-QKD

- Continuous Variables based on the **quadratures of the electric field of an electromagnetic wave**
  - Also subject to the **Heisenberg indeterminacy principle**.

Advantages

- Homodyne/heterodyne detection
  - **Forget** about bulky/expensive/cold **single photon detectors**.
  - **Better co-propagation** with classical signals (works as noise filter)
- Piggybacking on standard telco technology.
  - Better **industrialization** possibilities
  - Better **miniaturization** possibilities
  - **Cheaper**/better potential **to take over the market**

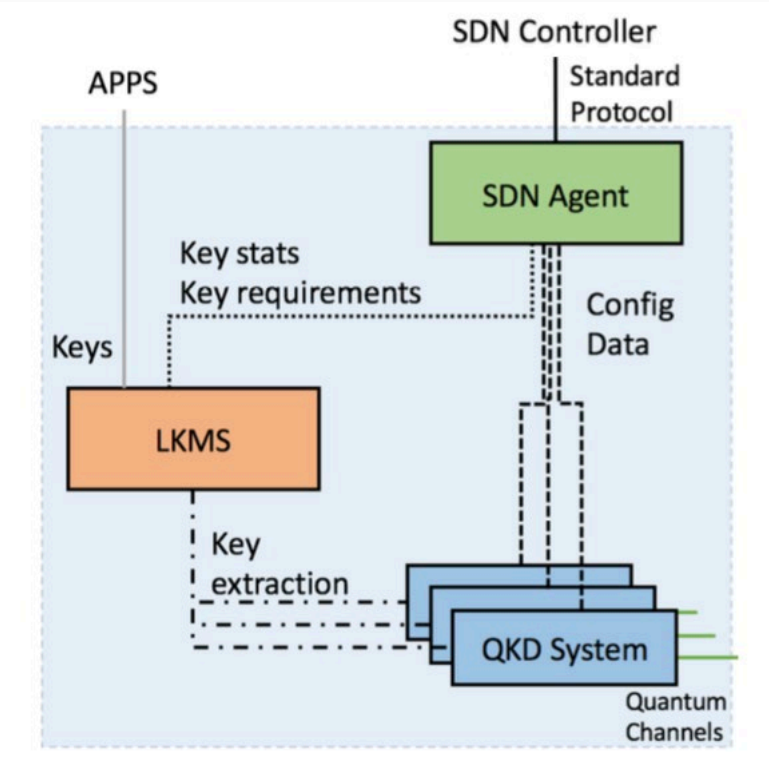
Disadvantages

- **Lower key rate** than DV-QKD
  - Can be higher at low distance/losses
- **Tolerate less losses**
  - Less reach/tolerant to bad channels
- Computationally **heavy postprocessing**

Quantum Key Distribution can help operator…

Software Defined QKD Networks

Software Defined QKD Node



Control plane protocols and interfaces within a transport network

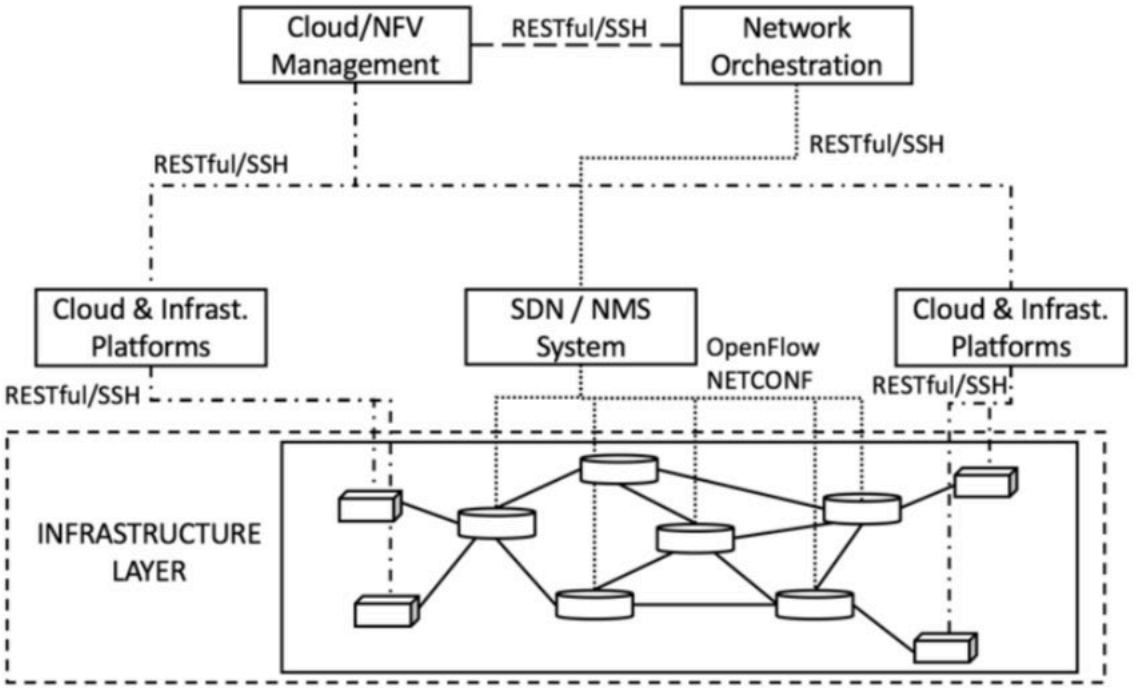
- **Software Defined Networks** (SDN) enables the **automation** of service provisioning within network operator infrastructures.
- With the **dynamic network requirements**, operators can not anymore deploy their services based on manual intervention or using proprietary vendor solutions.
- **Standard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

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.

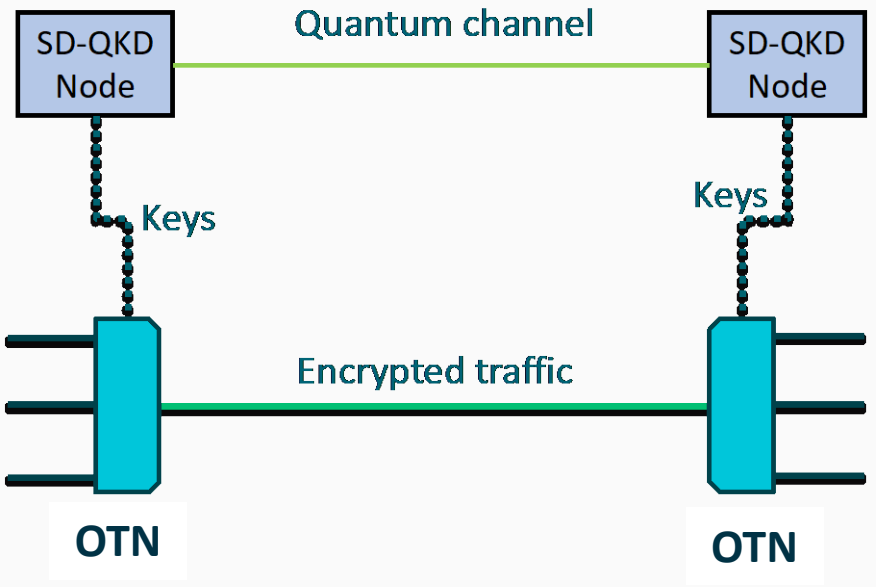
Control plane protocols and interfaces within a transport network



End-to-end quantum-encrypted connections

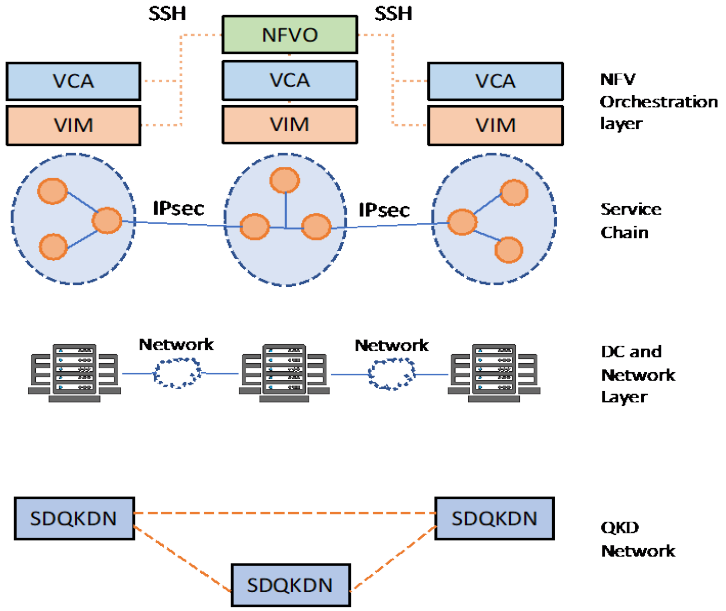
Quantum security embedded in network elements

- 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.

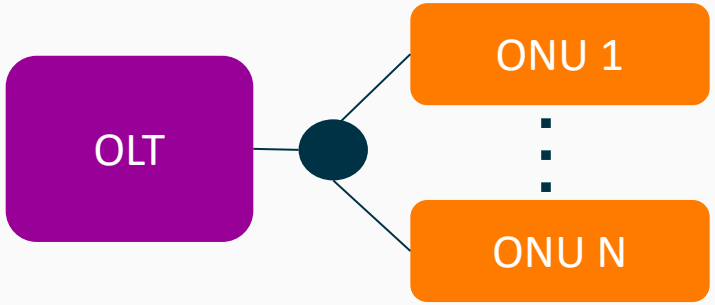


Enhance last mile services

Customer
Access

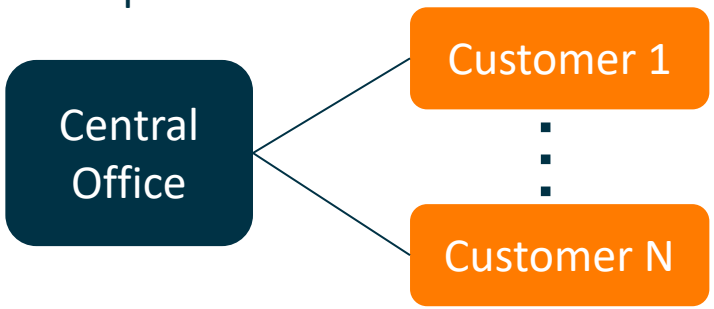
Improve security in Business Offers

- FTTH (Fiber To The Home) deployments are ongoing based on Passive Optical Network (PON) equipment and the number of homes connected is increasing.
- In GPON systems, an encryption mechanism is integrated and it is based on AES-128 encryption.

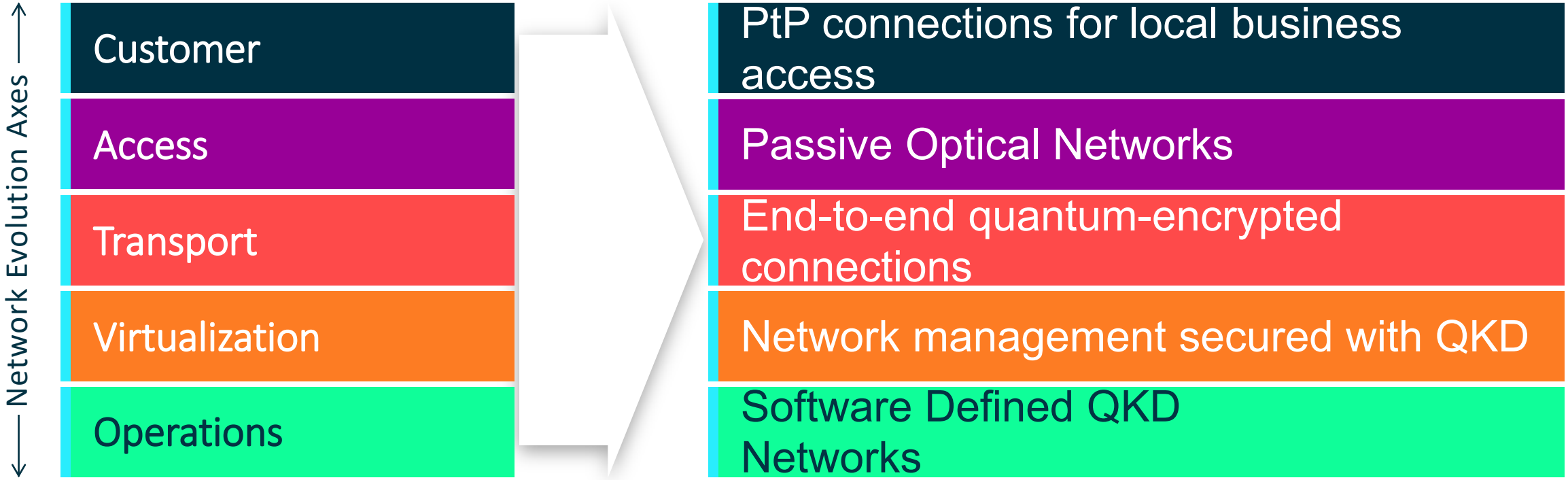


Point to Point connections for local business access

- Point to point connections encompass many business offers.
- This architecture allows business customers to benefit from a dedicated fiber resource that will not be shared with another customer.
- These customers 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 Key Distribution Scenarios



Cartoon from NIST

THANK YOU !!!

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 820466
This text reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.