CERN QTI Workshop 2021

Quantum Communications and Networks

QUANTUM
TECHNOLOGY
INITIATIVE

Alberto Di Meglio

CERN

The CERN QTI Roadmap – Quantum Communication and Networks

Objective	Contributes to top level objective(s)
N1: Identify and support use cases for specific uses, in collaboration with appropriate research and industry partners in area such as security, privacy protection, medical applications	T1, T2
N2: Identify, extend, co-develop CERN technologies relevant to quantum infrastructures, such as time synchronization and clocks, photon sources, laser technology	T2
N3: Formalise CERN's participation in the pan-European quantum infrastructure, providing operational and technical support	T4

Areas of investigation

Confidential computing

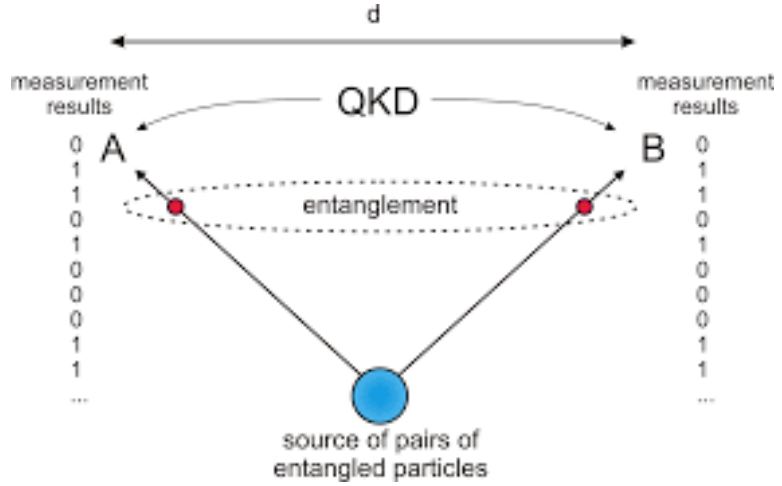
- QKD protocols and applications
- Secure distributed infrastructures

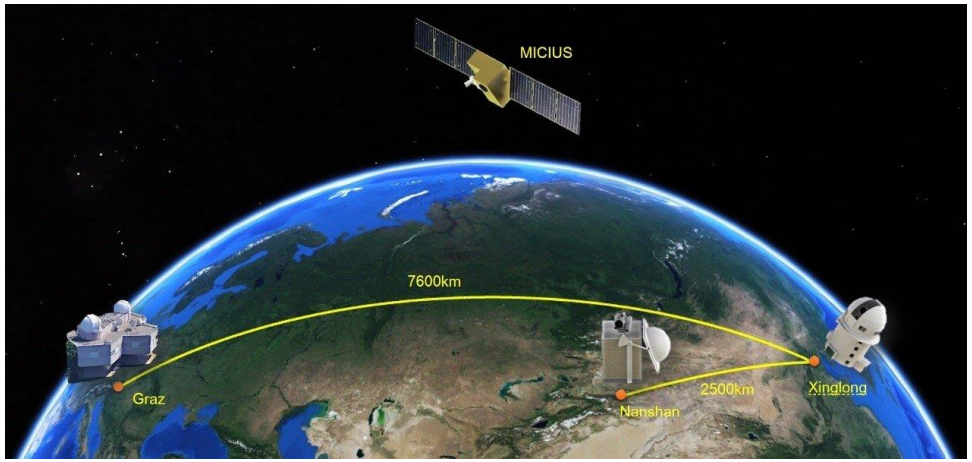
Communications technologies

- Opto-electronics
- Time synchronisation, frequency distribution, clocks

Quantum Communications

- John Bell was a theoretical physicist at CERN when he published his work on Bell's inequalities and the Bell's Theorem in 1964
  - A test of the "spooky action at a distance"
- Work on extending the distance of range of quantum communication channels already had CERN involved 2009-2011 As part of the SwissQuantum project
- Current research at CERN focuses on:
  - Assessment of quantum infrastructure technologies (mainly QKD)
  - Experimental and theoretical work on (quantum) optics and opto-electronics (supercrystals)
  - Generation and distribution of quantum random numbers for simulation, security, etc.
  - Time synch (White Rabbit)
  - Laser technologies



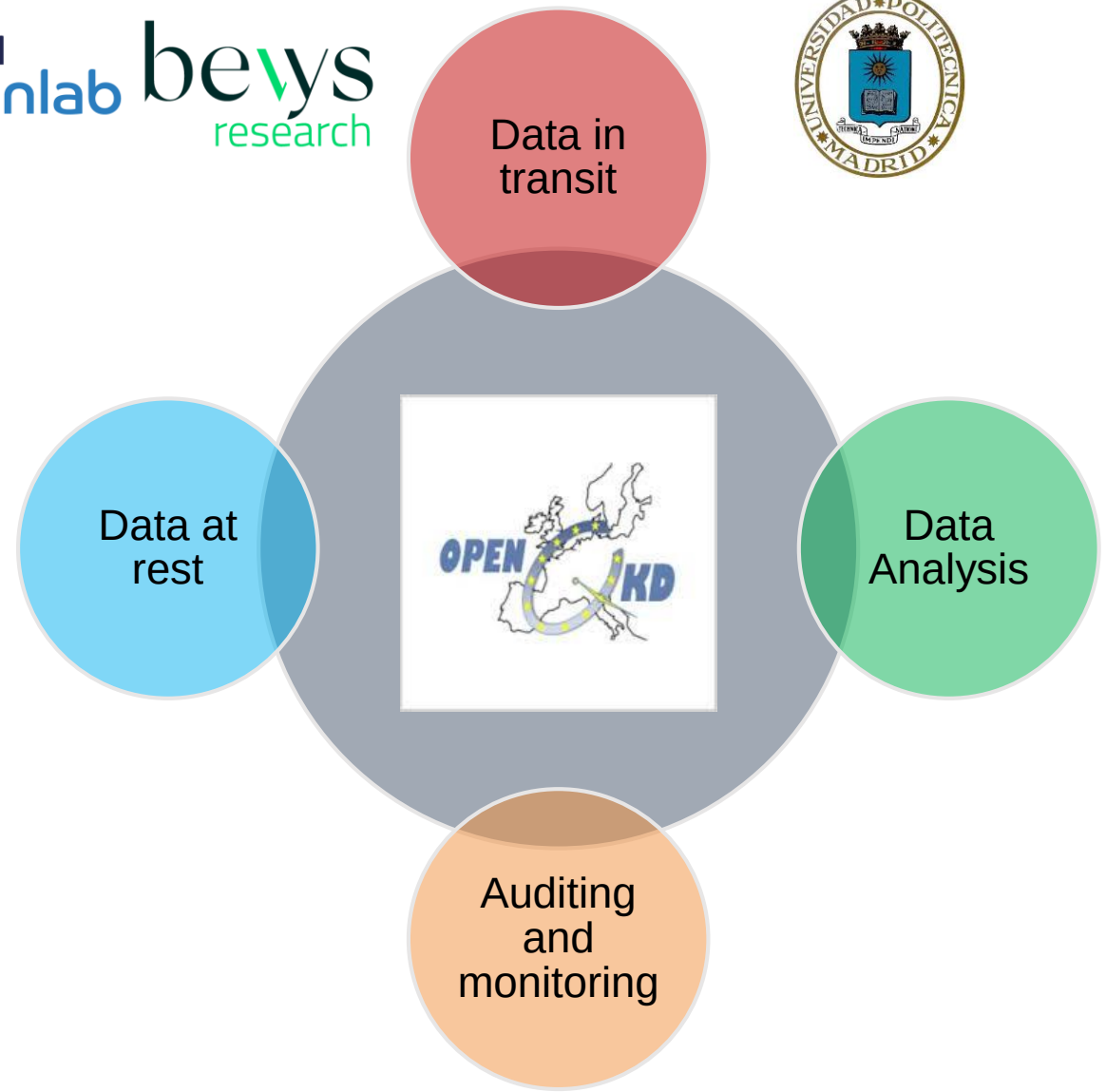


QUANTUMACY

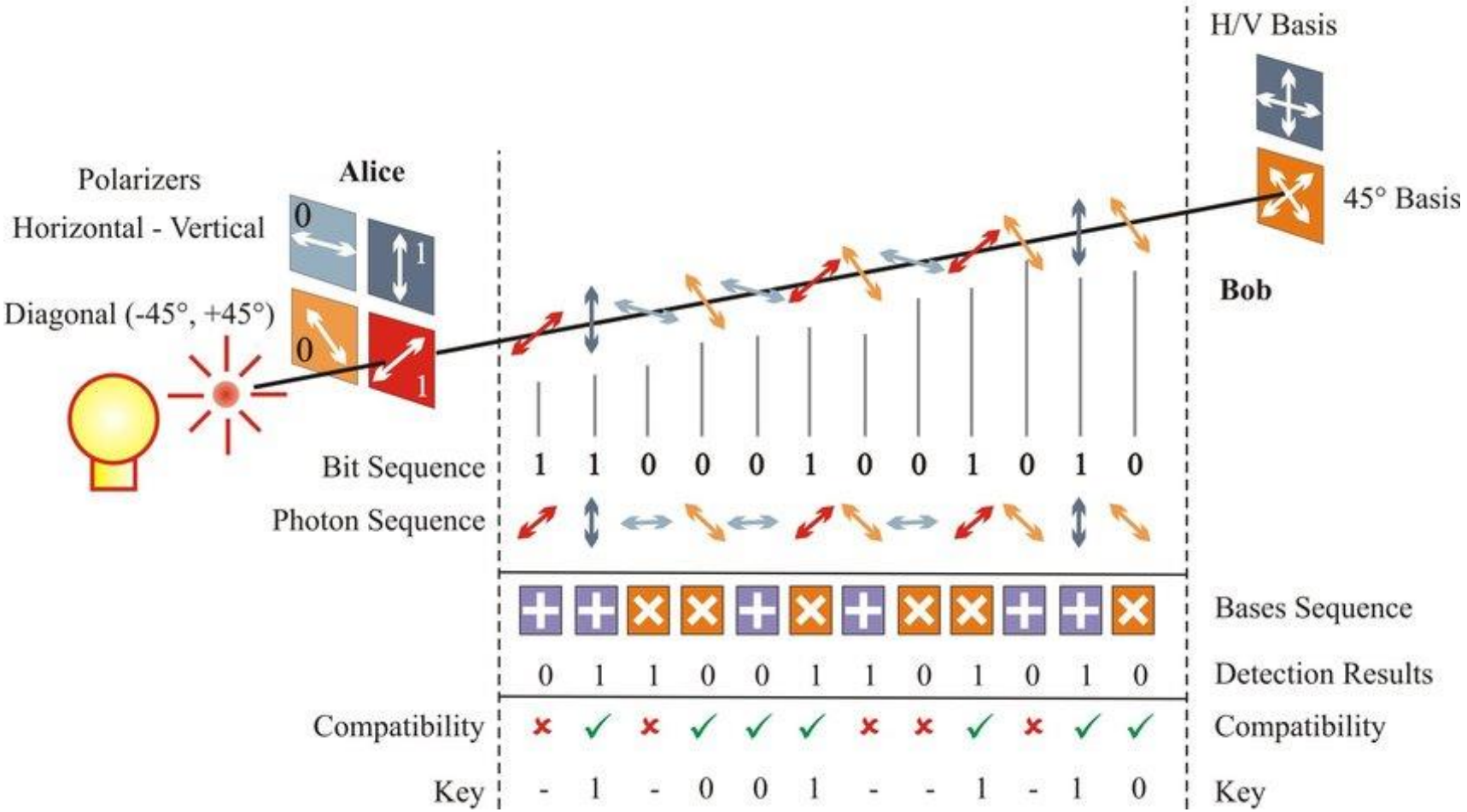
CERN openlab

beyys research

- **QUANTUM-based privacy and self-determination**
- Funded as an openQKD open call project
- End-to-end use of **QKD** to secure distributed data analysis over cloud infrastructures
- Data analysis: **quantum homomorphic encryption, SMPC, Federated Learning**
- Auditing: **quantum block chains**
- **Medical use cases**: image classification and segmentation for neurological diseases research

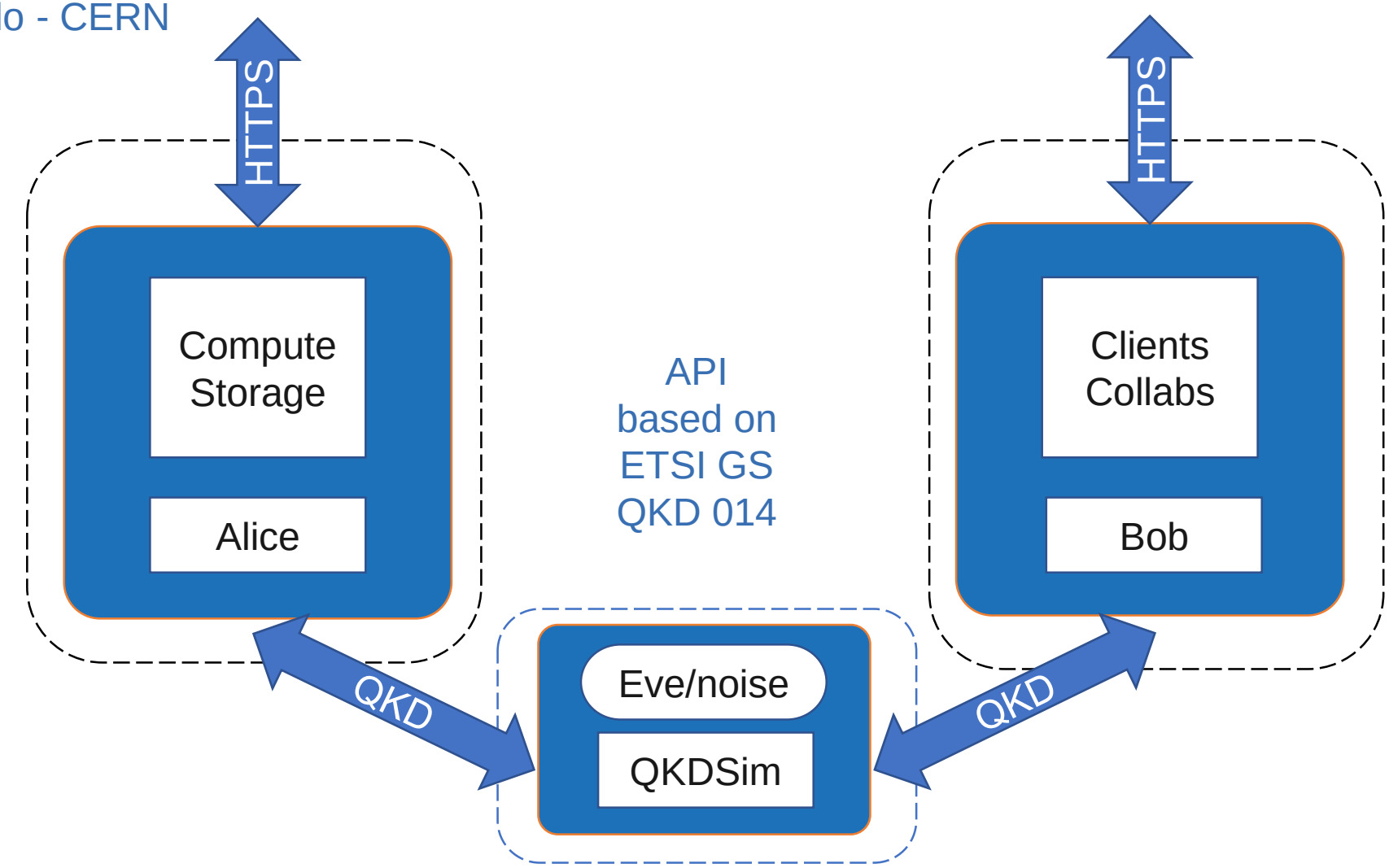


BB84 schema


H/V Basis
45° Basis
Bob
Alice
Polarizers
Horizontal - Vertical
Diagonal (-45°, +45°)
0
1
0
1
Bit Sequence
1 1 0 0 0 1 0 0 1 0 1 0
Photon Sequence
Bases Sequence
0 1 1 0 0 1 1 0 1 0 1 0
Detection Results
Compatibility
✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓
Compatibility
Key
- 1 - 0 0 1 - - 1 - 1 0
Key

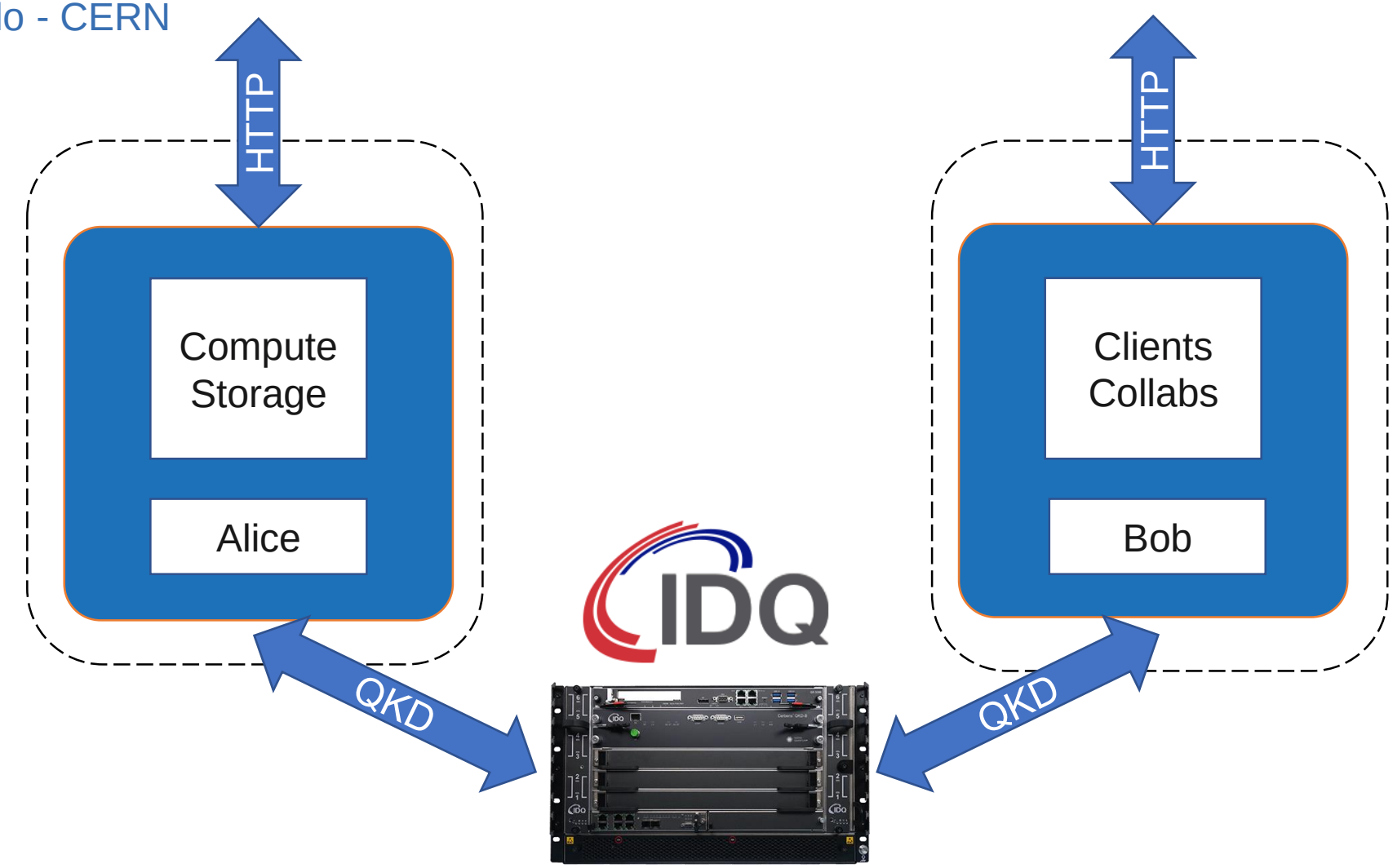
QKD: Simulations and hardware links

Gabriele Morello - CERN



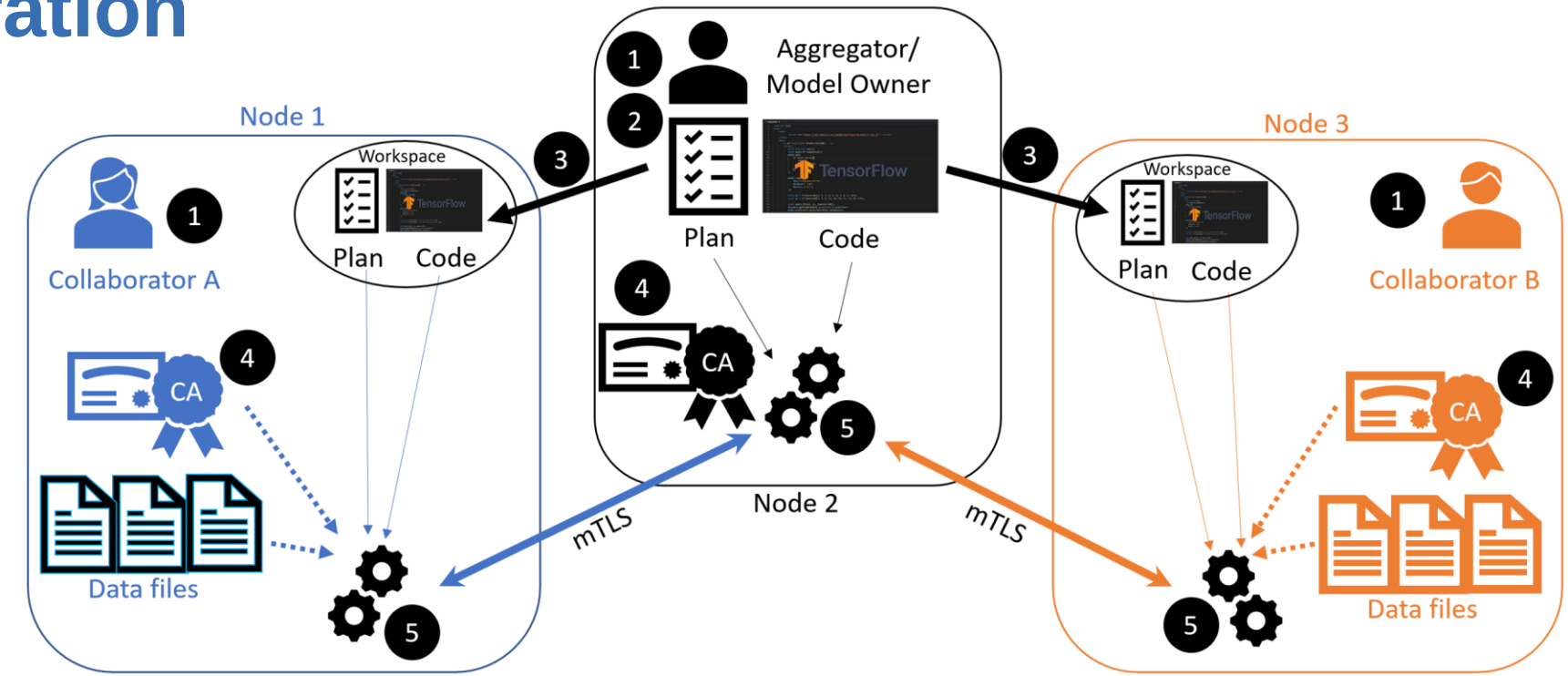
QKD: Simulations and hardware links

Gabriele Morello - CERN



OpenFL integration

Gabriele Morello - CERN



- Currently working on
  - Pairing each client with a unique ID and handling all these pairs on server side
  - Encrypting all the gRPC calls used by OpenFL
  - Understanding integration with higher level OpenFL
- Replace/extend mTLS connection with QKD-AES
- Replace certificates with a request to a QKD node

Next priorities

- **Set up dedicated activities at the network infrastructure level (time/frequency distribution)**
  - Several national and international projects are laying the foundations for the future quantum infrastructures
- **Extend the collaboration on QKD to other interested labs/projects**
- **Find a person to take responsibility of the Quantum Communications and Network activities in the CERN QTI Coordination Team**


CERN
QUANTUM
TECHNOLOGY
INITIATIVE