BE-QCI project:

Information session

05-06-2024

Belnet

Connecting communities

.be

Belnet

Connecting communities

Agenda

1. 11:00 Introduction (Emmanuel de Vinck)
2. 11:05 Presentation of the BeQCI project (Jo Segaert – Belnet)
3. 11:20 Use case (Cédric Bruynsteen – U-Gent-imec)
4. 11:30 Use case (Lotfi Guedria – Cetic)
5. 11:40 Q&A

Belnet

Connecting communities

Introduction

- What is BE-QCI consortium and Belnet
- BE-QCI : https://beqci.eu/

Jo Segaert - Belnet

1. BE-QCI projet: QKD & QCI

QKD & QCI

A view into the future of the internet

JO SEGAERT

Overview

1 | ## The promise of quantum computers

They promise to help us solve many scientific question.

2 | ## Shor's algorithm and Q-day

And break most of our commonly used cryptography.

3 | ## Quantum-resistant cryptography

Possible solutions.

4 | ## QKD - Quantum Key Distribution

The solution we will test.

5 | ## EuroQCI & BeQCI

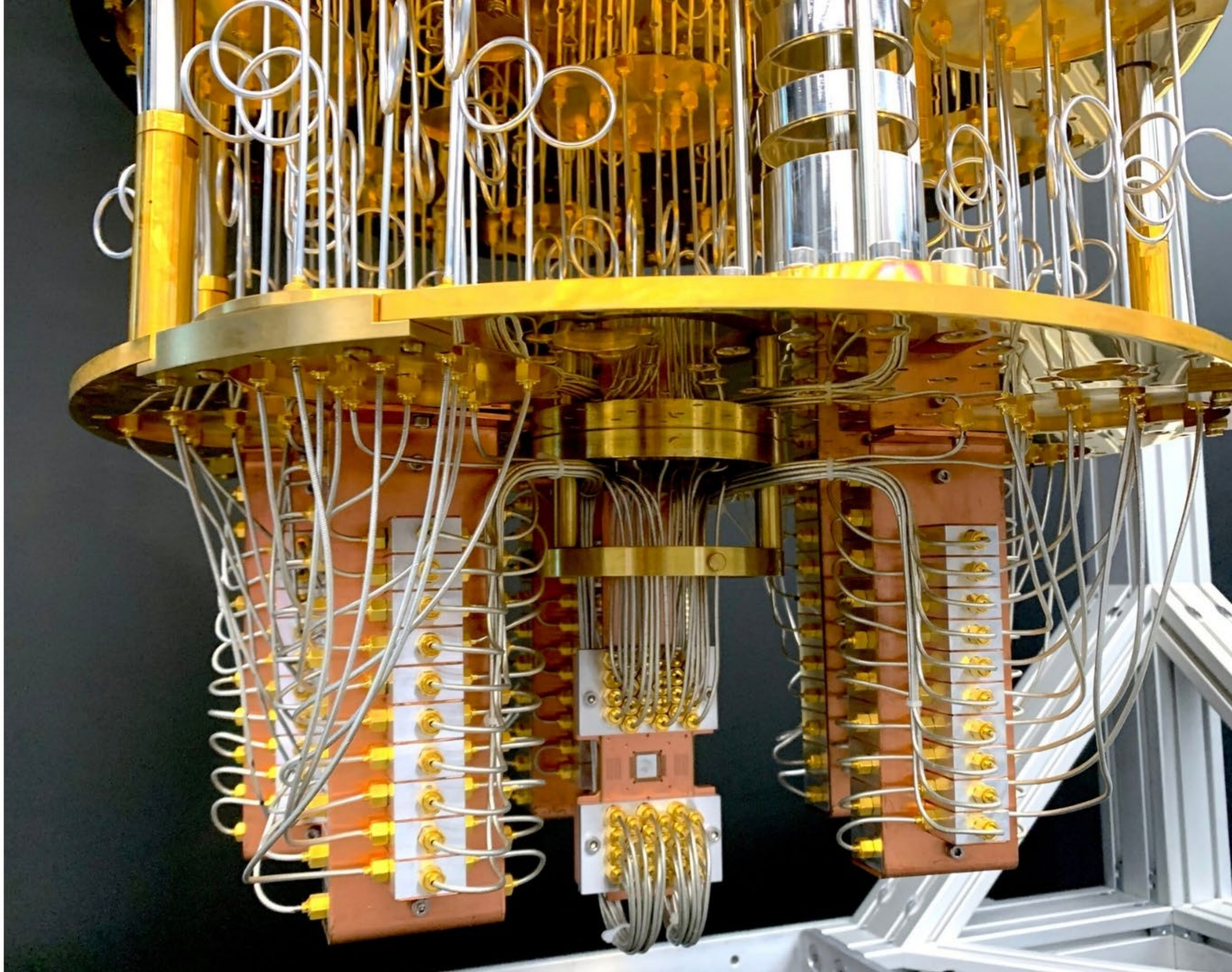
Our project.

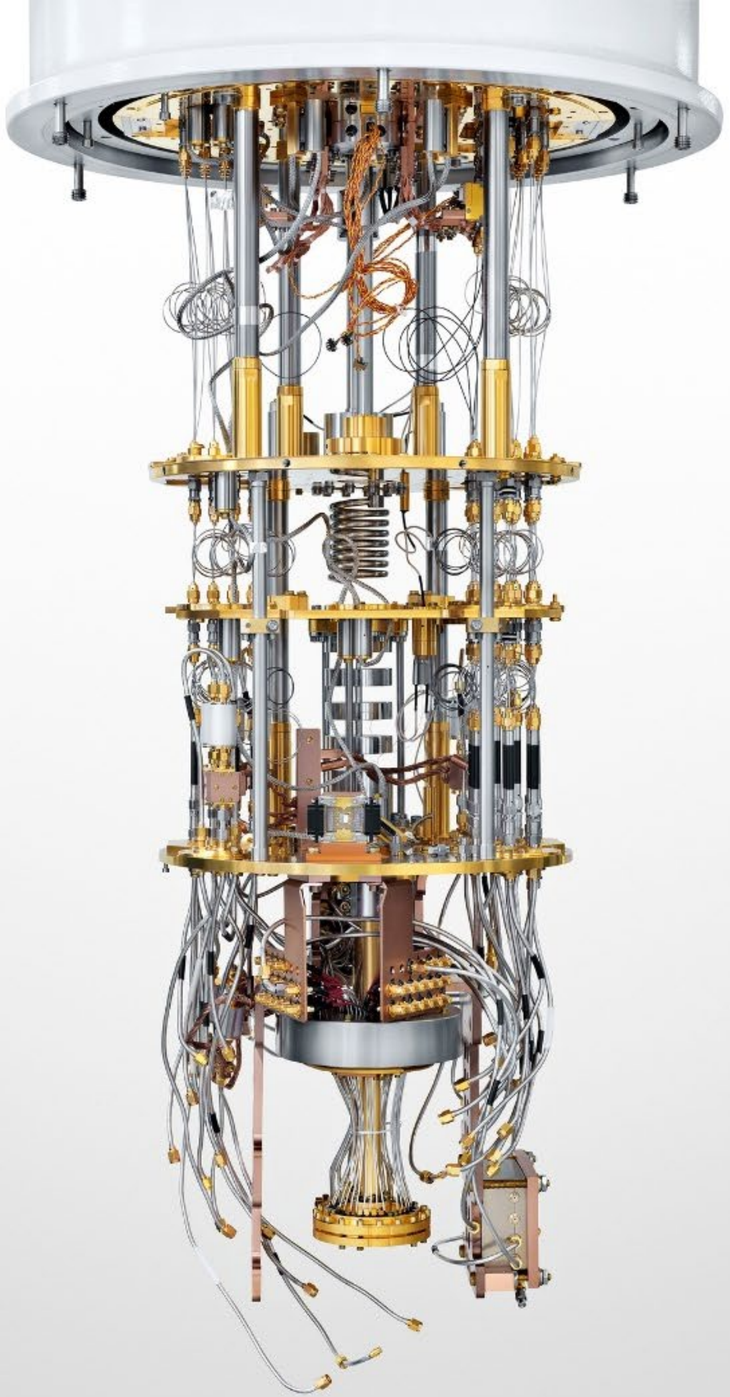
6 | ## QCI - Quantum Communication Infrastructure

The future of the internet.

Quantum Computer

An extension to classical computers





The promise of quantum computers

Complex optimization problems

Traveling salesman

Integrated circuits design optimization

Quantum physics simulation

Optimising the search to superconducting materials at room temperature

More efficient batteries

Biological molecule simuation

Running medical simulations

First 10's then 100's of atoms

Protein folding & interactions

Biological systems simulation (still science fiction)

Simulating a ribosone (100k atoms)

Simulating a entire cell

Shor's algorithm and Q-day

Cryptography likes very difficult problems (and likes them to remain difficult)

Our most used cryptography is based on a difficult problem that a quantum computer could make simple.

Running Shor's algorithm on a powerfull quantum computer breaks our most used encryption

This is Q-day

Quantum resistant cryptography

PQC - Post Quantum Cryptography

New algorithms that are based on difficult problems that remain difficult for a quantum computer

+ Software based, can be run on our current machines

+ easy to upgrade and deploy

- Is one mathematical genius or innovation removed from being broken

QKD - Quantum Key Distribution

Using the quirks of quantum mechanics to create random keys to be used for further encryption

+ Resistant to mathematical innovation

+ Based on the laws of nature

- Still difficult, thus expensive

- No economies of scale

BeQCI network

BeQCI research

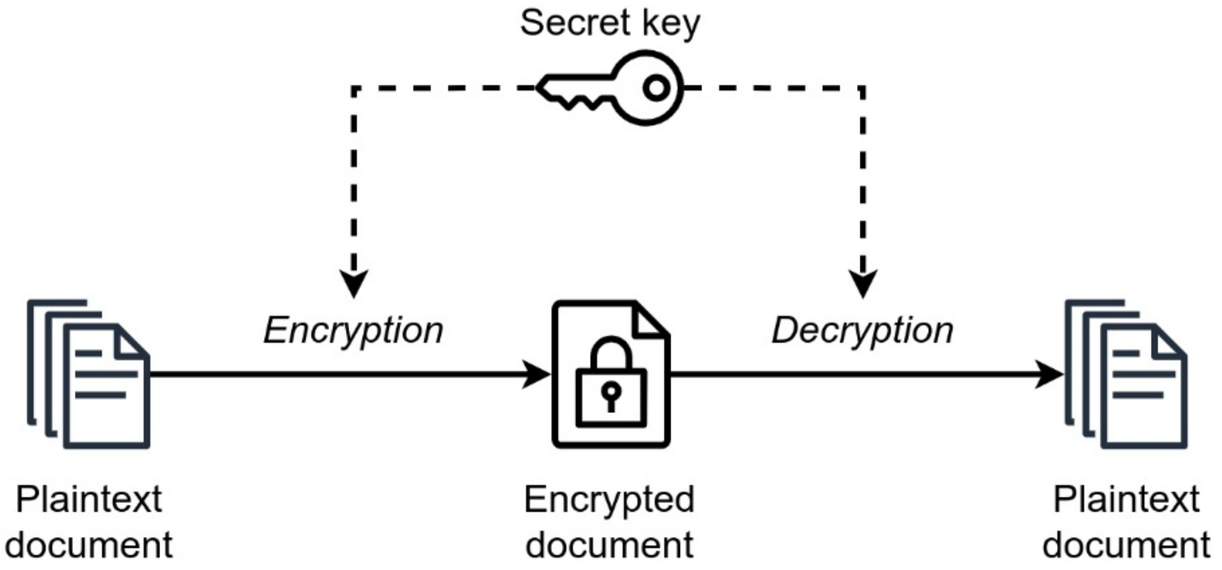
Key distribution

Asymmetric encryption with public & private key

vs

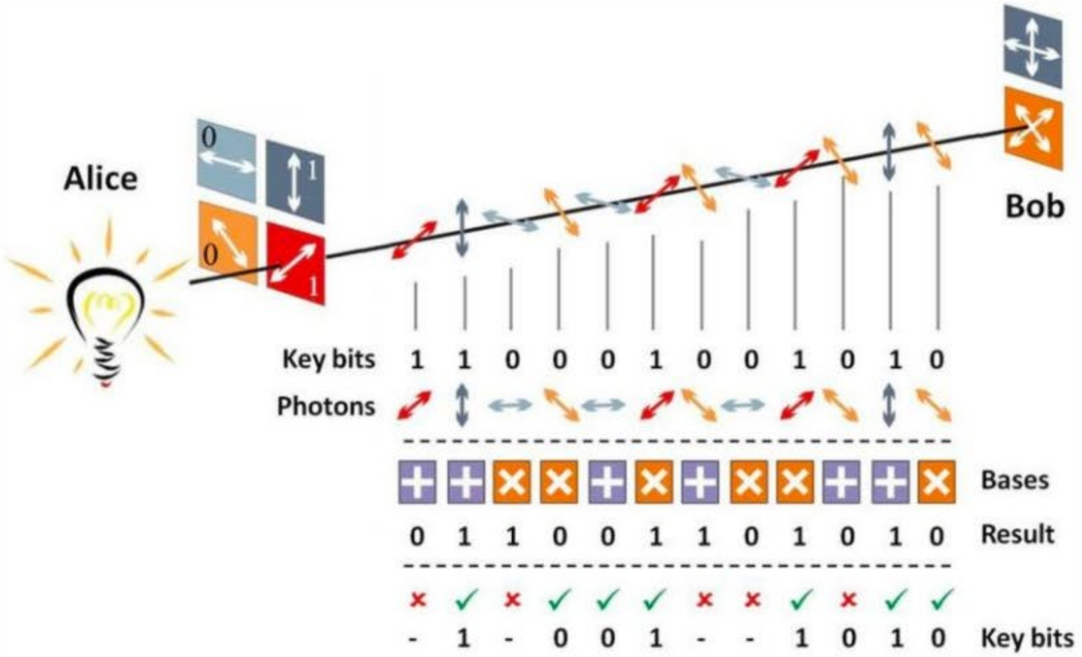
Symmetric encryption with key distribution

What is a key? Just a random sequence of numbers.



Quantum Key Distribution

- **Partial solution to our encryption problems**
  - Only works when having a direct (fiber) connection
  - Point-to-point or Multipoint with one or more central nodes
- **Many flavors**
  - DV, CV, Twin-Field, MDI
- **A word about the BB84 protocol**
  - First protocol invented, DV flavor
  - How can you discover an eavesdropper?



EuroQCI & BeQCI

EuroQCI

belspo

imec

GHENT UNIVERSITY

KU LEUVEN

UHASSELT
KNOWLEDGE IN ACTION

UCL
Université catholique de Louvain

ULB

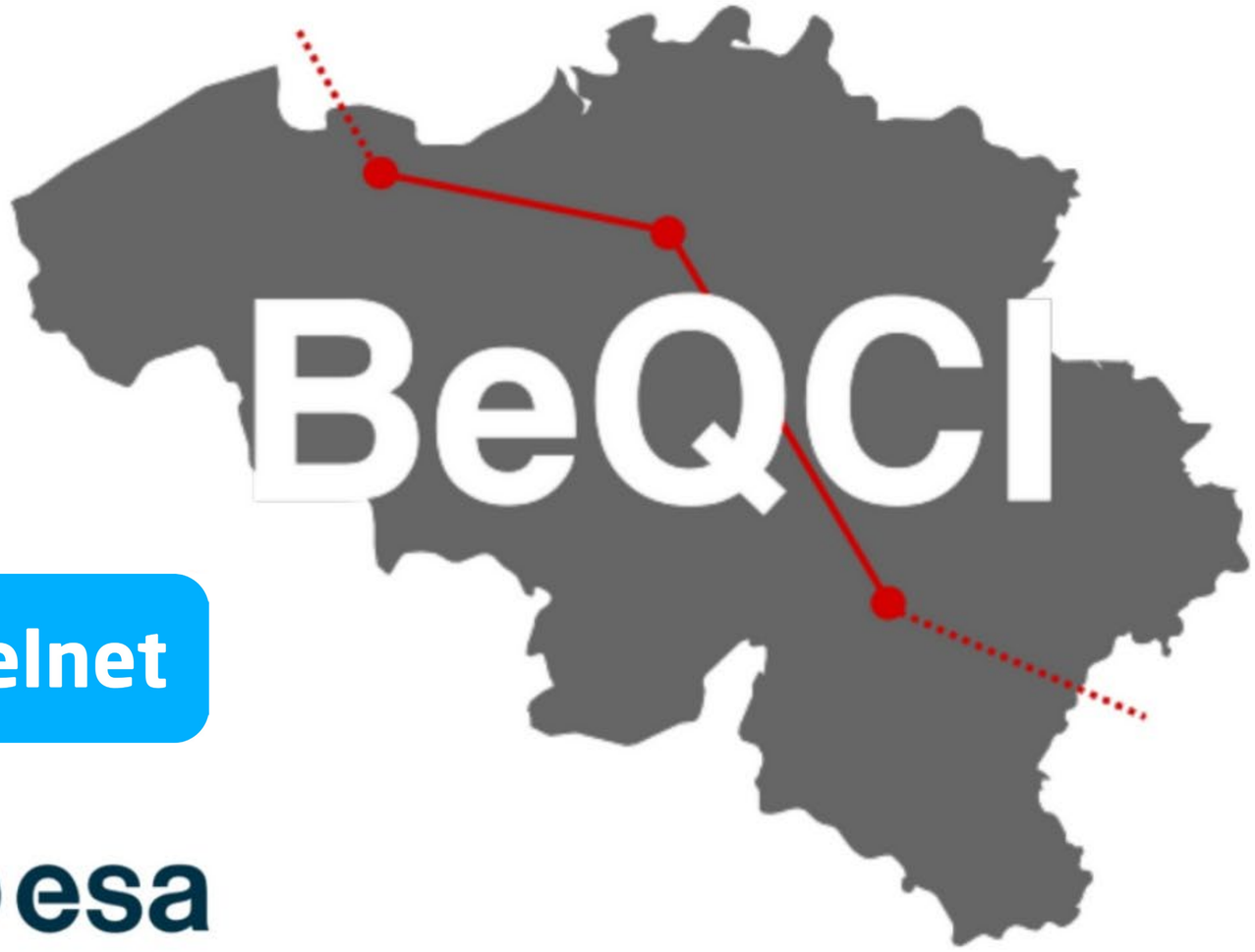
RMA
Royal Military Academy
Brussels

Belnet

Multitel
INNOVATION CENTRE

THALES

esa



BeQCI

Create first Belgian quantum communication testbed

Strengthen QKD & QCI technology trough research

Deploy QKD network

In 4 phases

With 4 different technologies

Use cases

Government

Universities

Private sector

You?

Cross border

Collaboration with Luxembourg

Prepare for the next phase to connect QKD networks over the entire EU

Research

Chipscale transceivers

PQC (Post Quantum Cryptography)

Fibre-compatible quantum memories

Security analysis of QKD protocols

BeQCI QKD Testbed

Project in 3 phases of 6 months

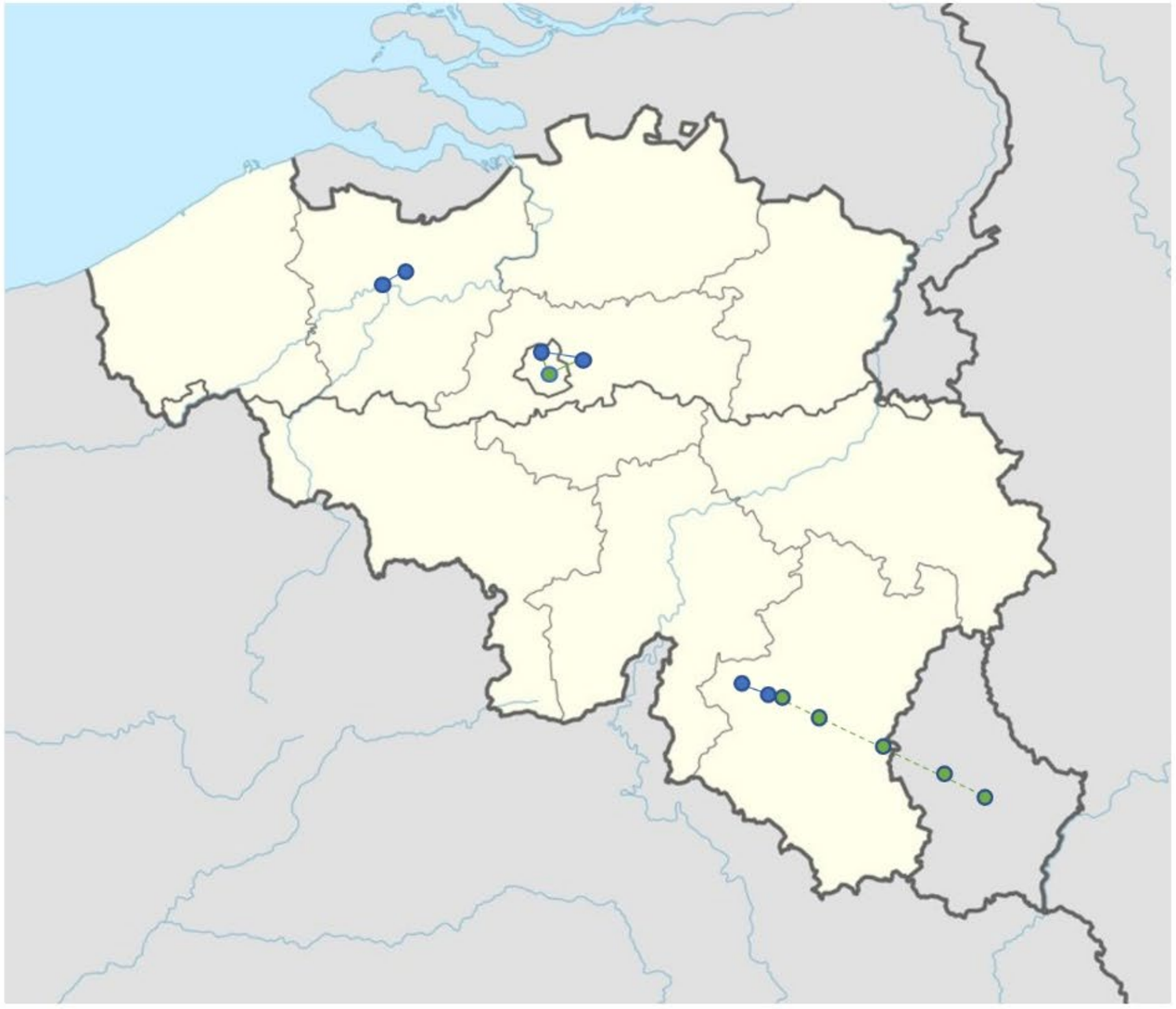
LUXQUANTA (CV)
CONNECTS 2 SITES)

THINKQUANTUM (DV)
CONNECTS 2 SITES

IDQUANTIQUE (DV)
CONNECTS 2 SITES

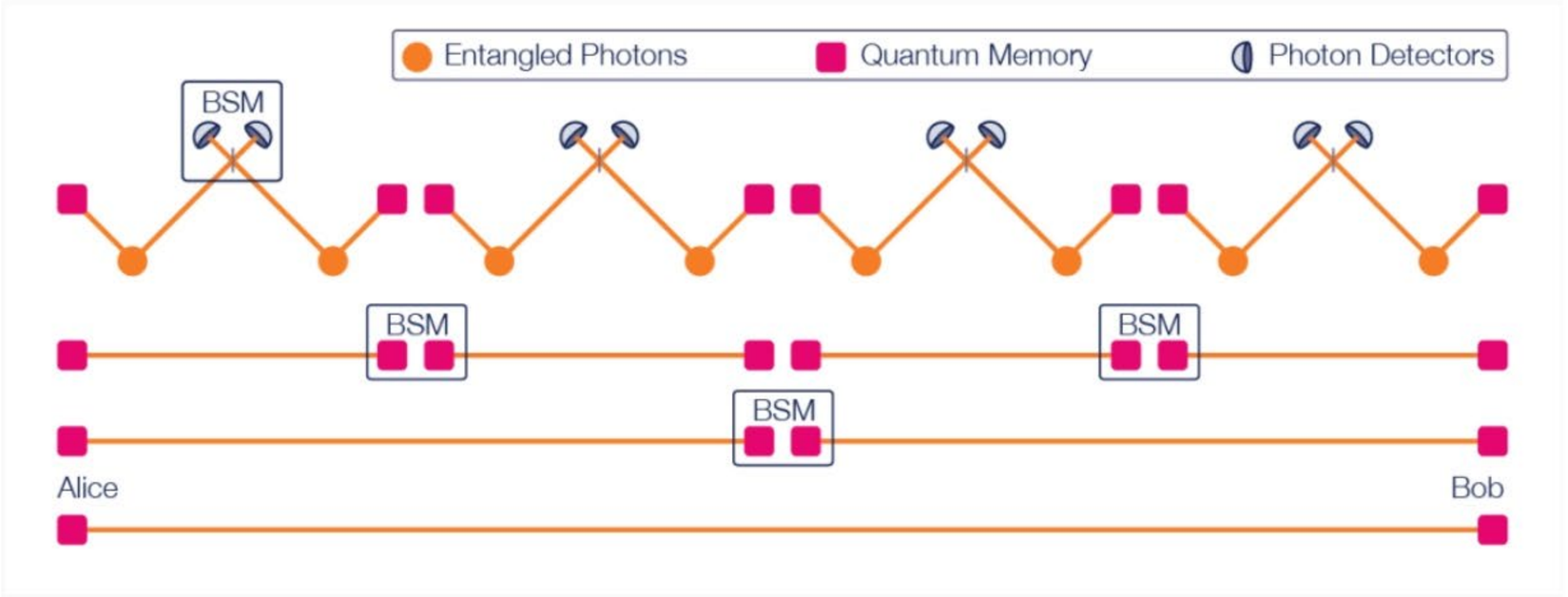
Q*bird
quantum
connectivity

Q*BIRD (MDI)
CONNECTS 5 SITES
ONE STEP CLOSER TO QCI



QCI - Quantum Communication Infrastructure

Quantum Internet



QCI - Quantum Communication Infrastructure

The quantum internet

What

QKD is the first TRL9 QCI technology

Now we can create correlation (QKD)

We need entanglement

What we still need to build

Trustworthy quantum repeaters

Trustworthy quantum memories

QCI-ready ISP (Internet Service Provider)

Has to create a continious stream of entaglement, between arbitrary points in the network, ready for the client(s) to use/consume.

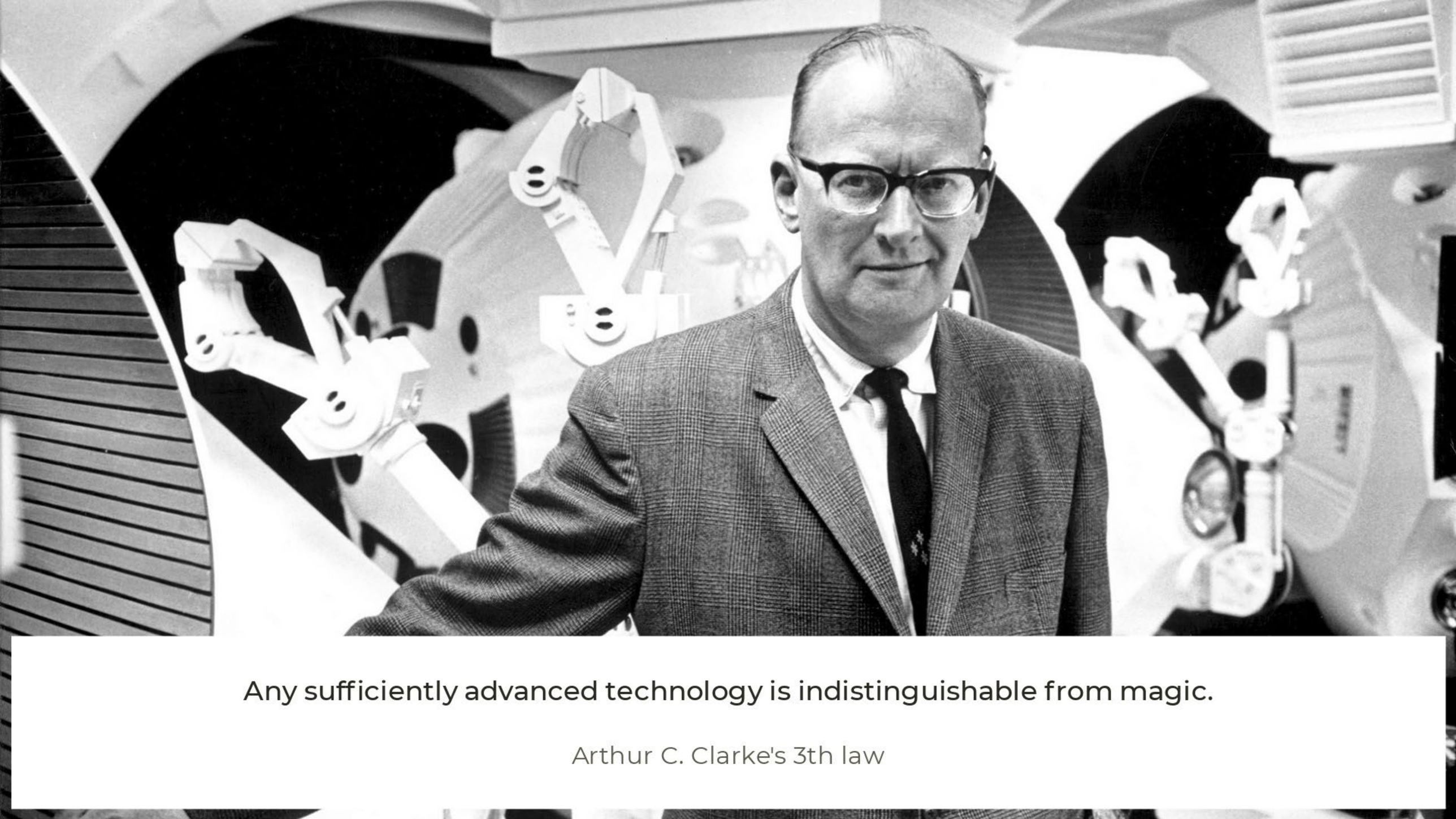
Applications

Distributed quantum computing

Blind delegated computing

Anonymous data transmission

...



Any sufficiently advanced technology is indistinguishable from magic.

Arthur C. Clarke's 3th law

CEDRIC BRUYNSTEEN - IMEC - U-Gent ID-LAB

2. Beqci - Ghent use case

Beqci - Ghent use case

CEDRIC BRUYNSTEEN

UNIVERSITEIT GENT

GHENT
SMART APPLICATIONS

Universiteit Antwerpen

Vrije Universiteit Brussel

LEUVEN
HEADQUARTERS

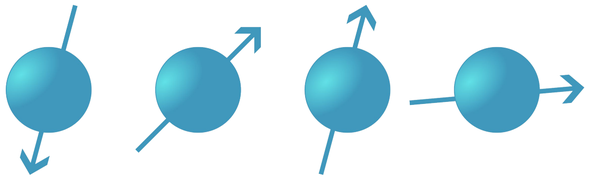
KU LEUVEN

universiteit hasselt

Comparing technologies

Discrete Variable QKD

First protocol established in 1984



Single photons

→ Sensitive to stray light

→ Slow detection speed

+100 km range

Continuous Variable QKD

First protocol established in 2002

Weak coherent optical signal

→ Easier network integration

→ Use of established sub-components

<100 km range

Comparing technologies

TECHNOLOGY OF CHOICE FOR GHENT USE CASES

LuxQuanta® NOVA LQ®

Continuous Variable QKD

First protocol established in 2002

Weak coherent optical signal

→ Easier network integration

→ Use of established sub-components

<100 km range

Overview Ghent use cases

Highlight strengths of CV-QKD technology

→ Co-existence of traditional telecom data with QKD

→ High-speed QKD using custom integrated circuits

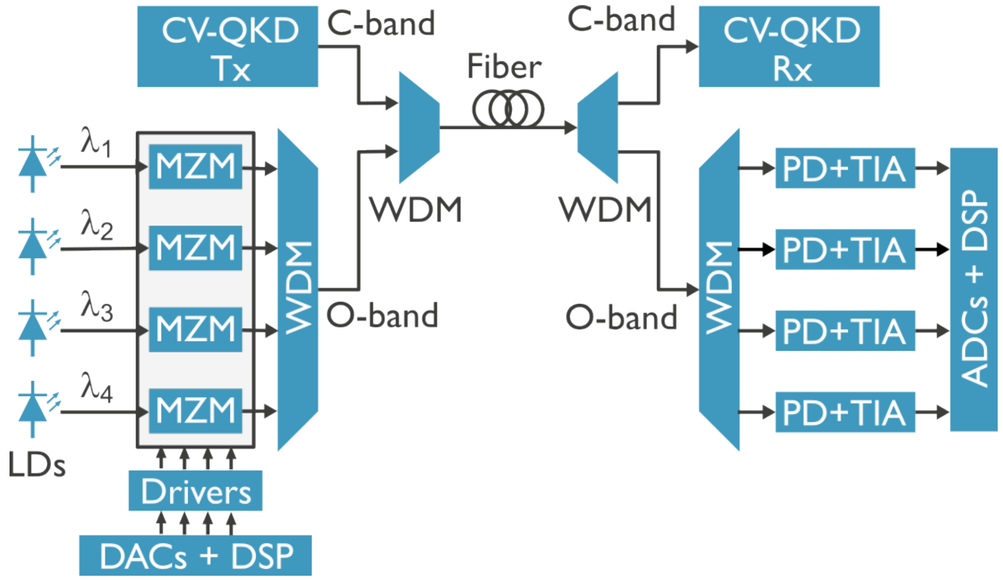
Use case 1: Co-existence

Setup

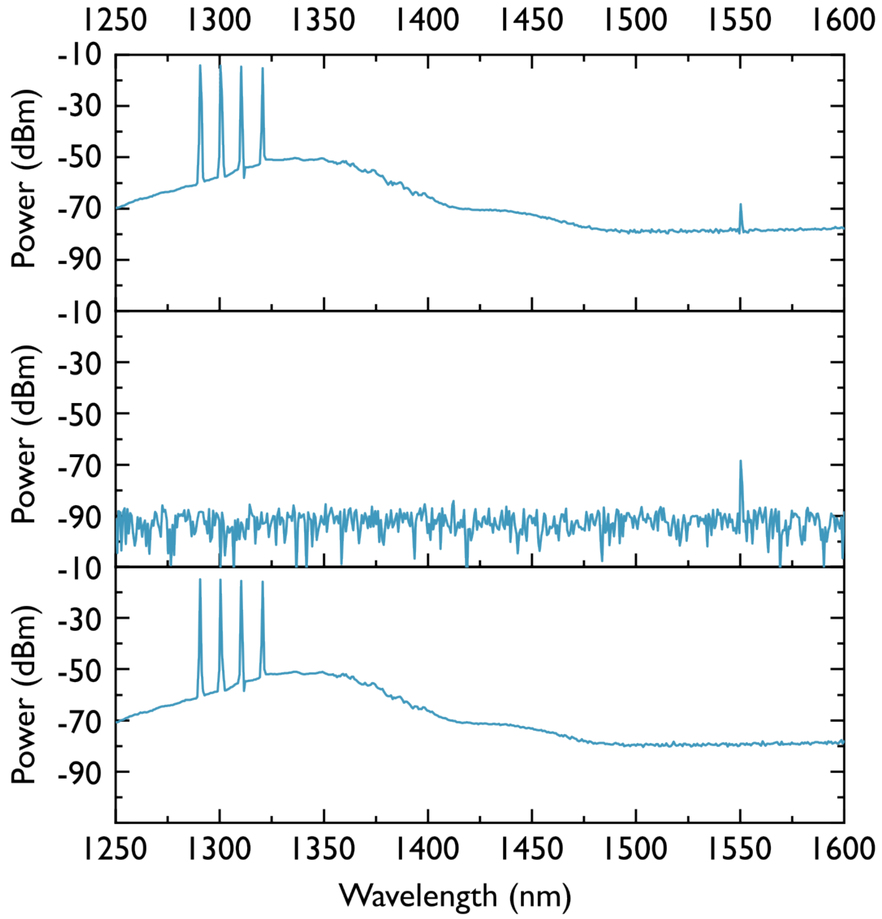
LuxQuanta CV-QKD
(1550nm)

+

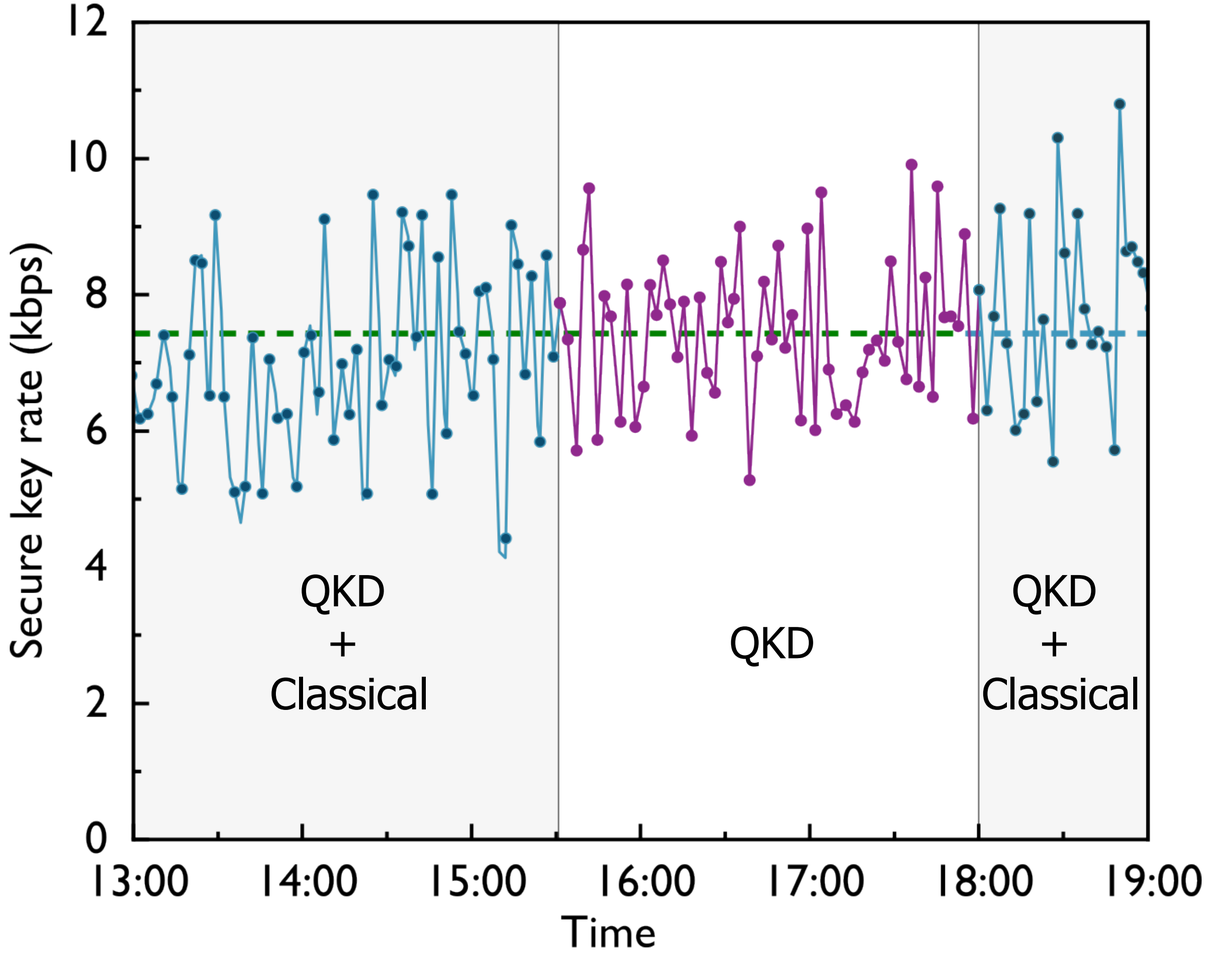
4 x 56 GBaud PAM4
(O-Band CWDM)



Optical spectrum



Use case 1: Co-existence
Results



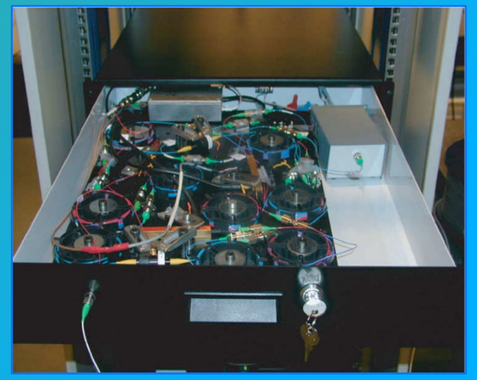
No meaningful impact of the strong classical data channels on the performance of the QKD link!

Use case 2: Integrated QKD
Motivation

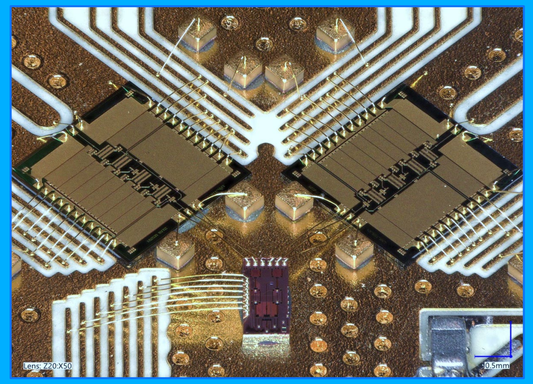
Integration

Table-top experiments

Discrete components in rack



Chip based solution



Currently commercially available

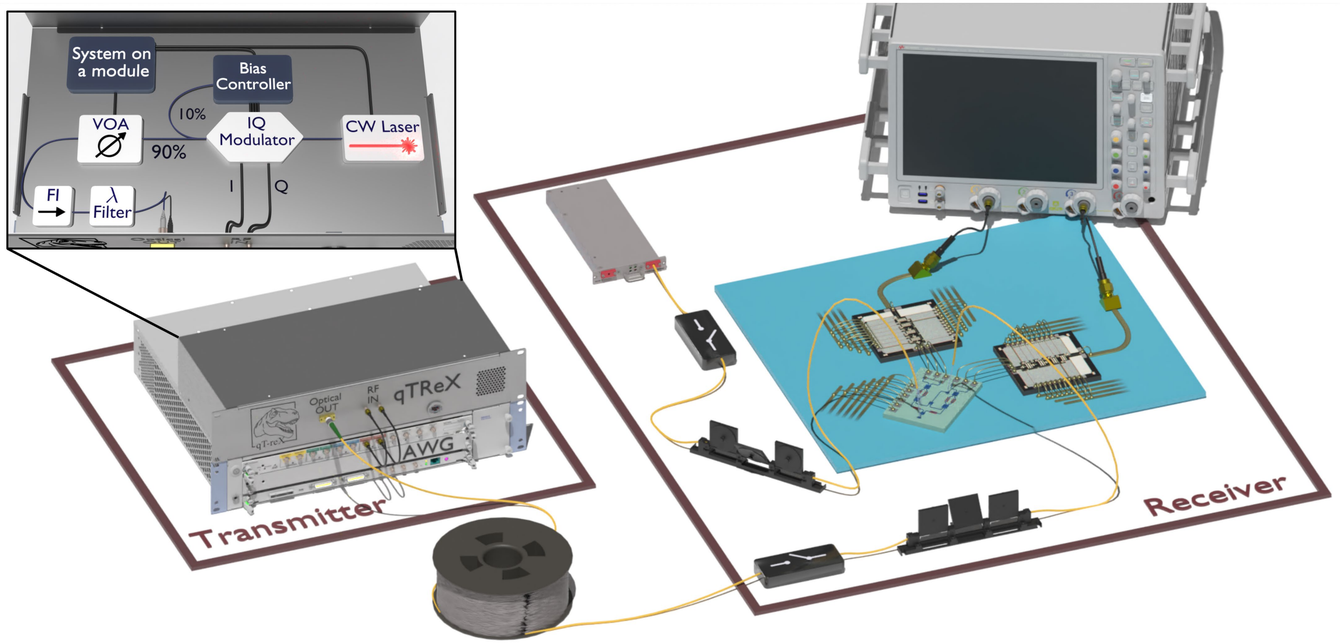
- More robust
- Compact
- Higher speed
- Lower noise
- Cost effective

Use case 2: Integrated QKD
Previous results

Standard telecom modulation schemes

High symbolrate
- 8 GBaud & 10 GBaud

Secret Key Rate
- 737 Mb/s @ 5km
- 315 Mb/s @ 10km



embracing a better life

imec IDLab INTERNET & DATA LAB UNIVERSITEIT GENT Universiteit Antwerpen

Lotfi Guedria - CETIC

3. BeQCI CETIC's QKD PoC

BeQCI CETIC's QKD PoC:

QKD enabled communications for Industrial IoT middleware

Lotfi GUEDRIA

R&D Department Manager

Embedded & Communicating Systems

June 5th , 2024

www.enmieux.be

FEDER UNION EUROPEENNE

Wallonie

LE FONDS EUROPÉEN DE DÉVELOPPEMENT RÉGIONAL ET LA WALLONIE INVESTISSENT DANS VOTRE AVENIR

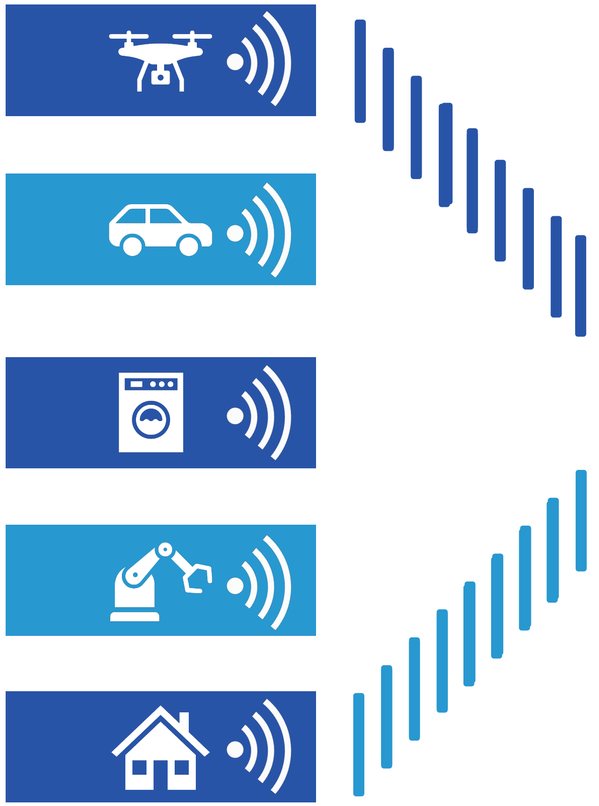
official partner | digital wallonia .be

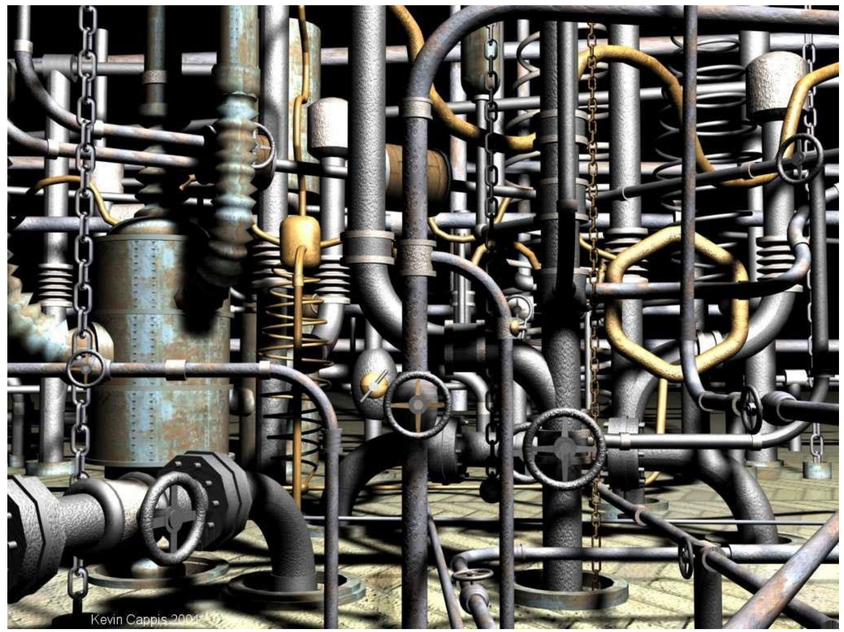
Centre d'Excellence en **Technologies** de l'**Information** et de la **Communication**

www.cetic.be

DMWay middleware overview

(I)IOT data sources





(I)IOT data consumers

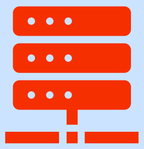
Need for evolvability (evolution capable) : What it means?

Able to follow/support the life cycle (of a solution):

Assessment, implementation, PoC, adoption/mainstreaming, operation

Offering adaptability mechanisms: extensibility and interfacebility:

(Easily) Add, modify or remove/replace features



Ability for system to develop / grow in a controlled way (Natively "scalable")

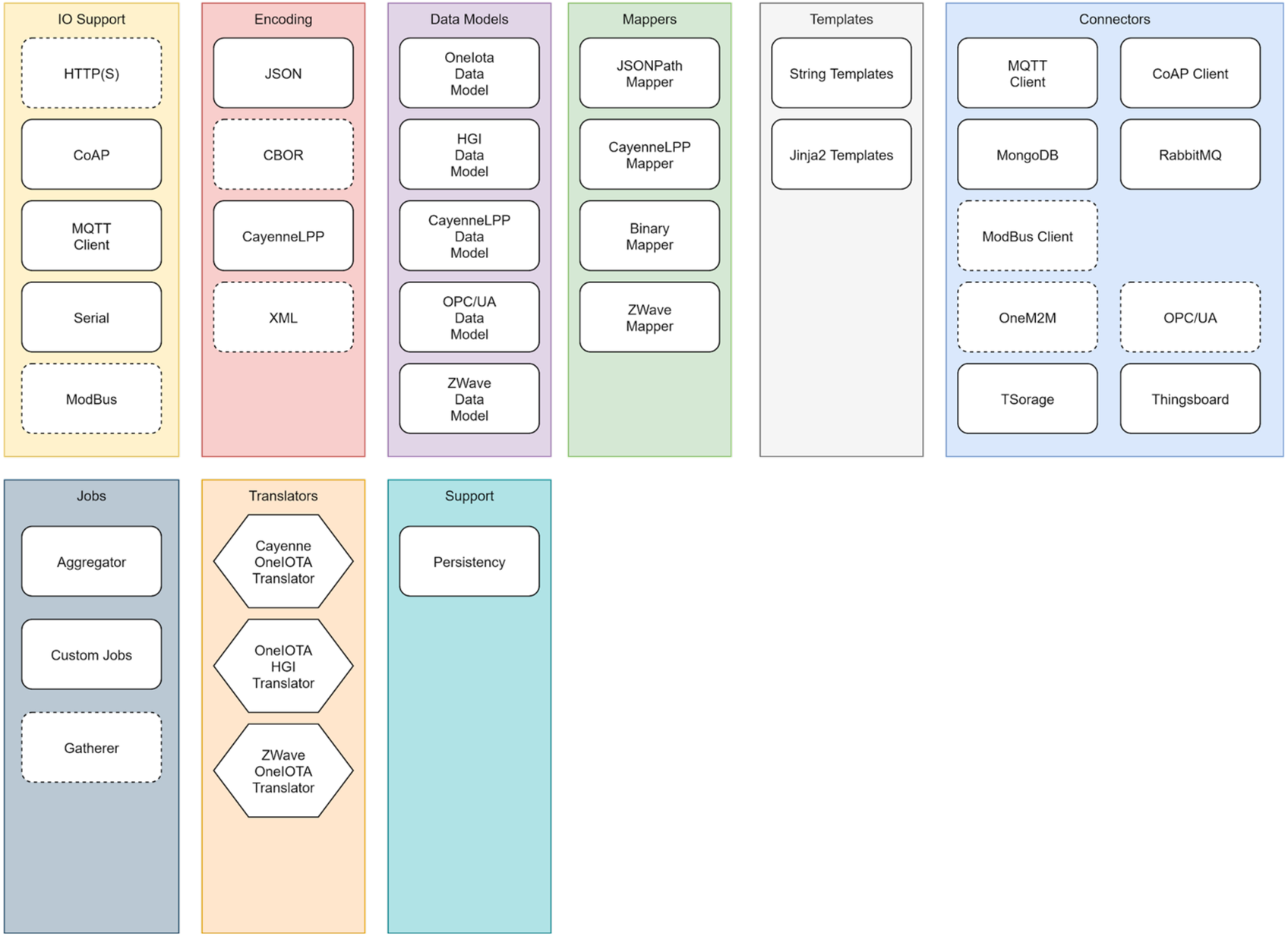
➔ Keeping complexity under control

The Universal (I)IoT Data Manager At The Edge

dmway
IoT's Universal Connector

DMWay – Specialized modules

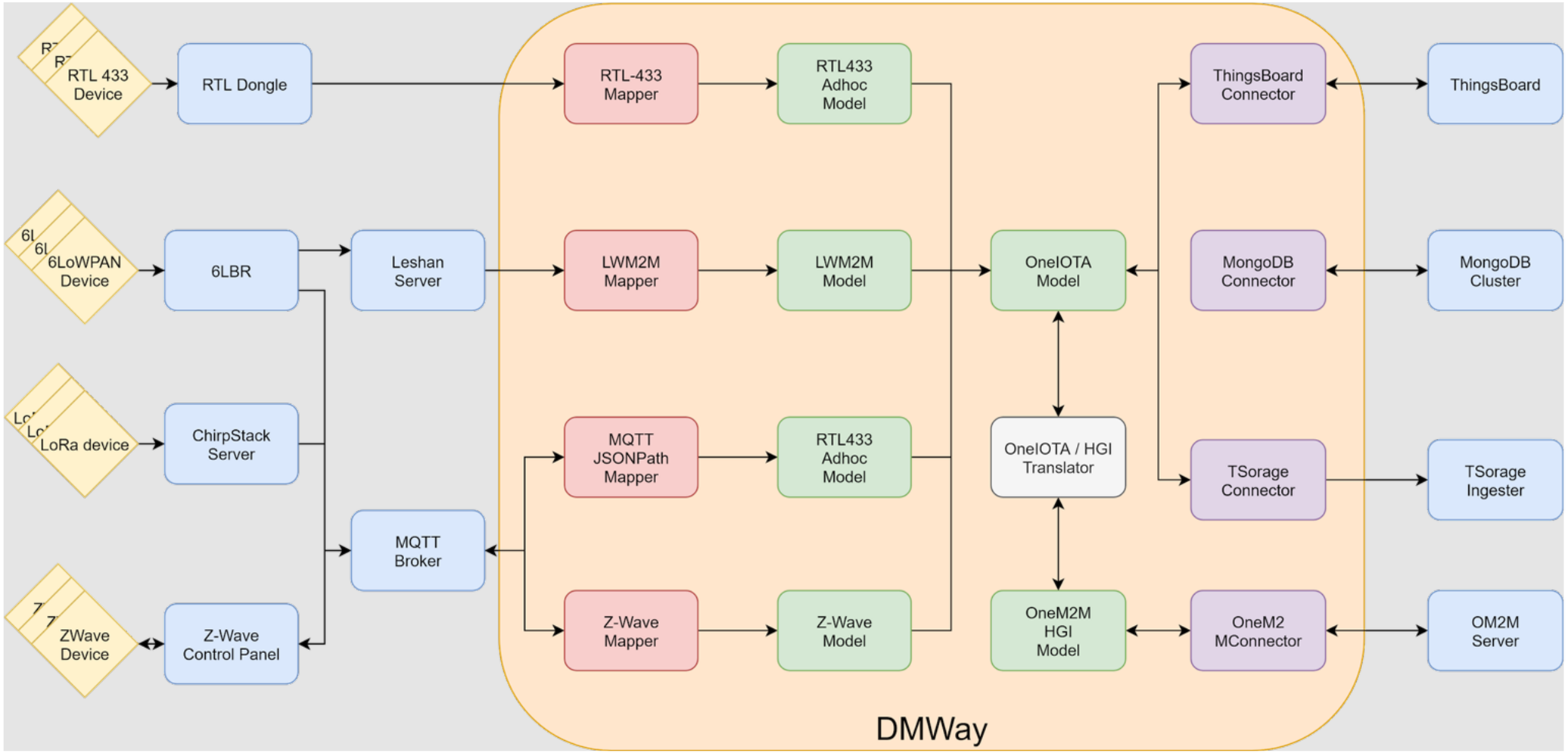
dmway
IoT's Universal Connector



- Built-in data modelling
- Specific data semantics handling
- Encoders/decoders, Mappers and translators
- Connectors
- Custom jobs
- Persistancy

…Enabling to easily build evolvable and flexible setups for (I)IoT data management and integration… mainly by configuration

dmway
IoT's Universal Connector



CETIC/DMWay – Specialized middleware for management of heterogenous (I)IoT data modular, composable, interfaceable

Heterogenous objects exposing data points

- ✓ sensors / actuators using a variety of interfaces & protocols

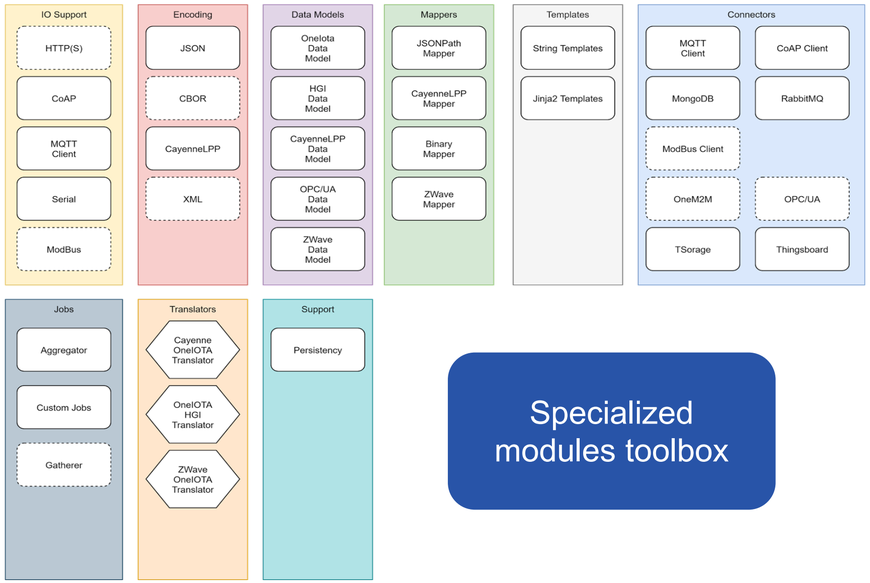
Data

- ✓ Multiplexing
- ✓ Working
- ✓ Augmentation

Distribution

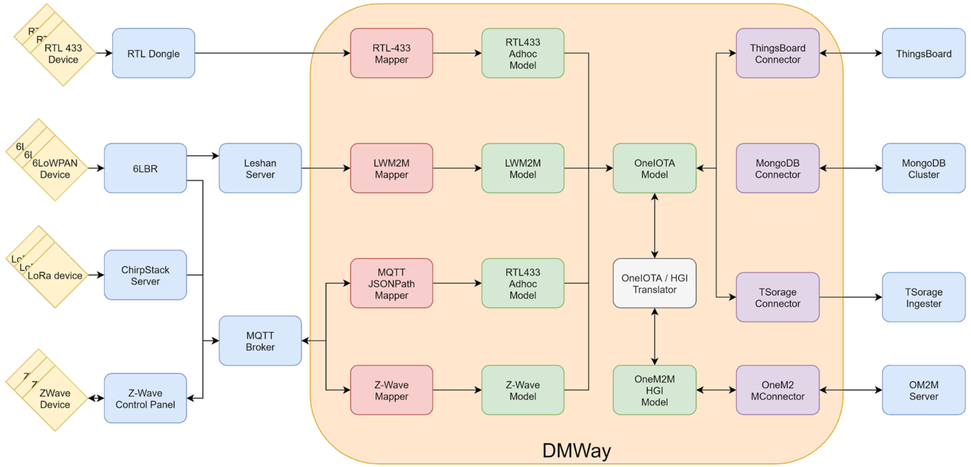
- ✓ Remote applications
- ✓ Databases
- ✓ …

https://www.cetic.be/dmway



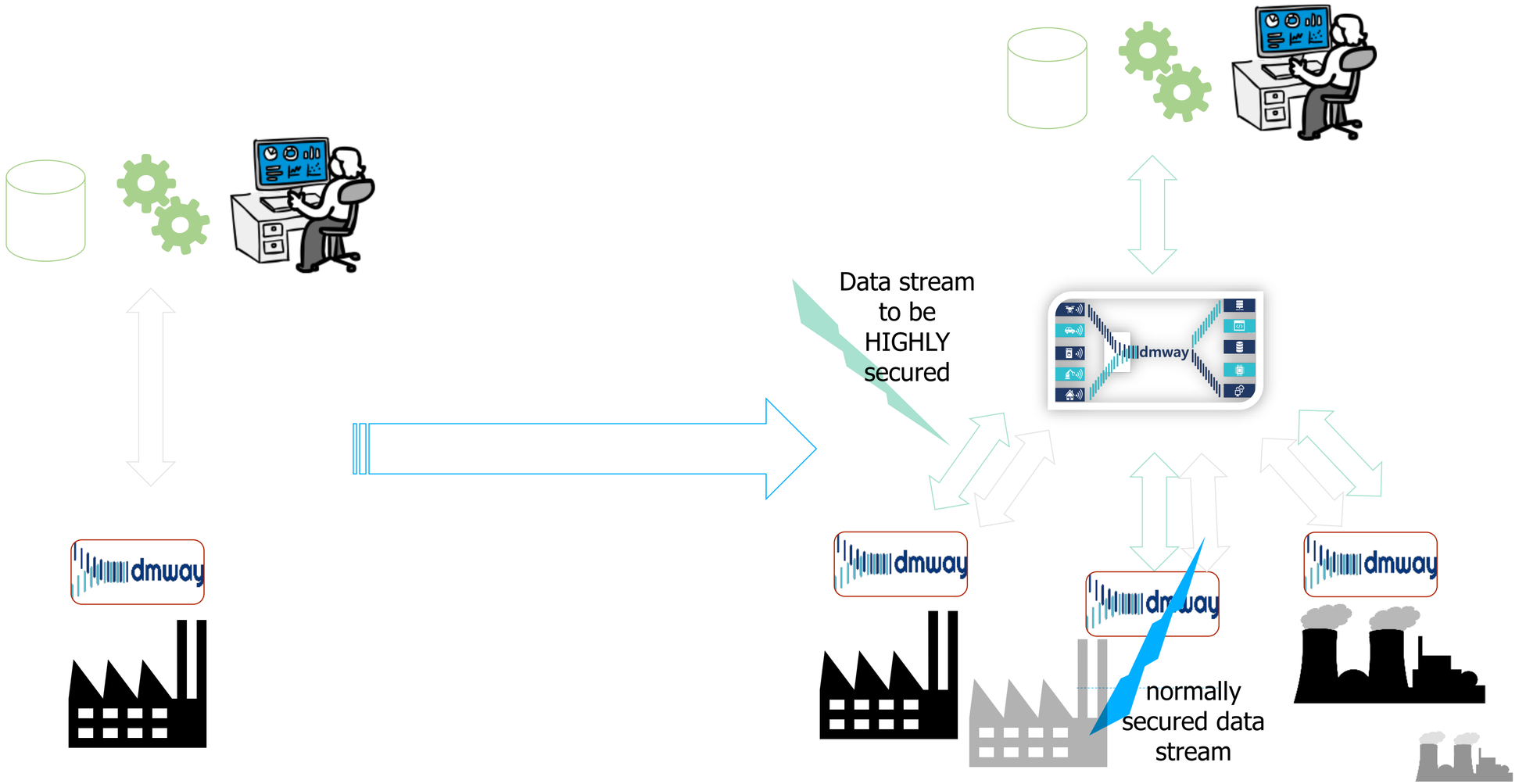
Specialized modules toolbox

Easily connectable and composable modules



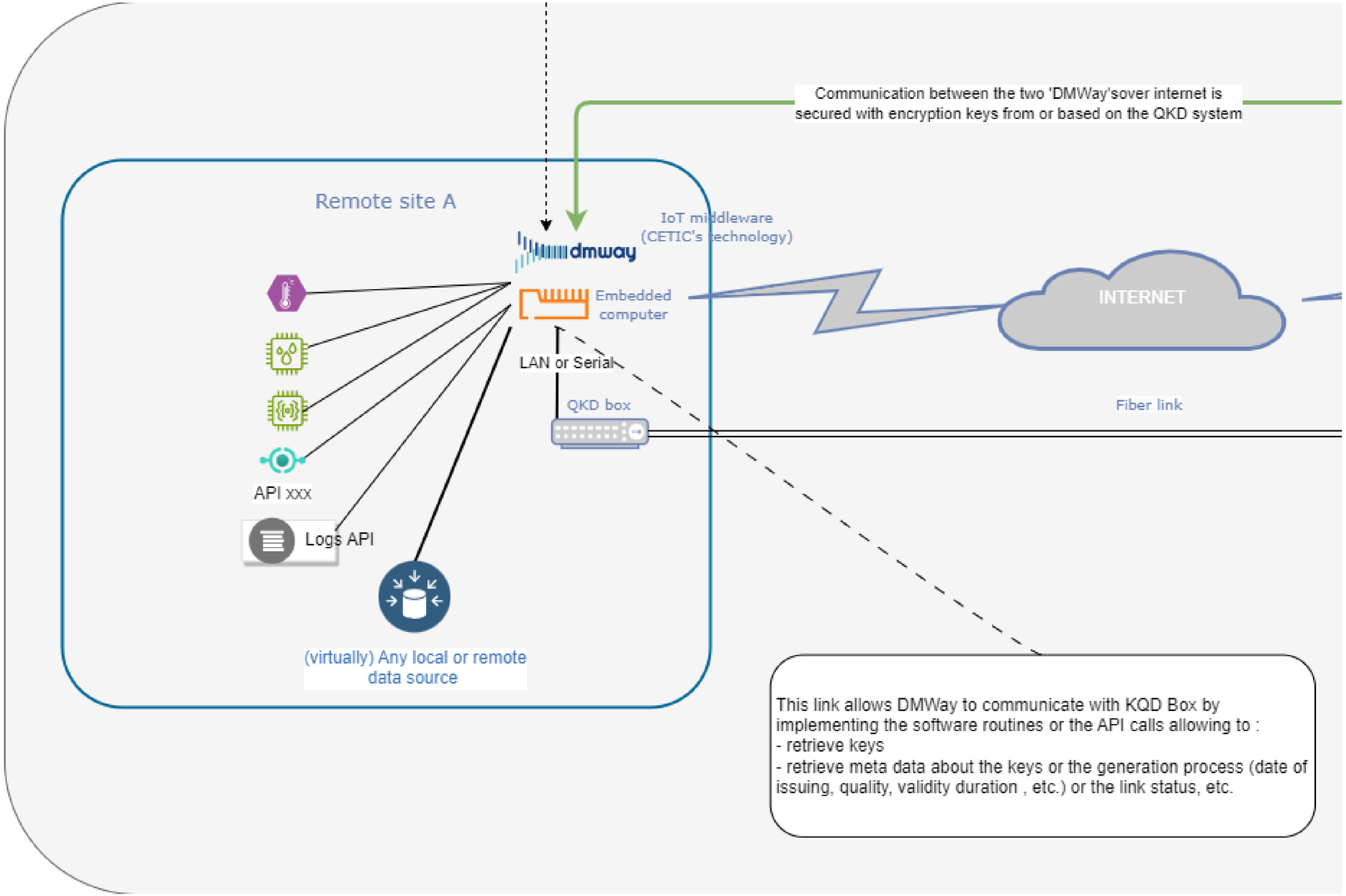
QKD &
DMWay middleware-based communications

Deployment example with architecture evolution support

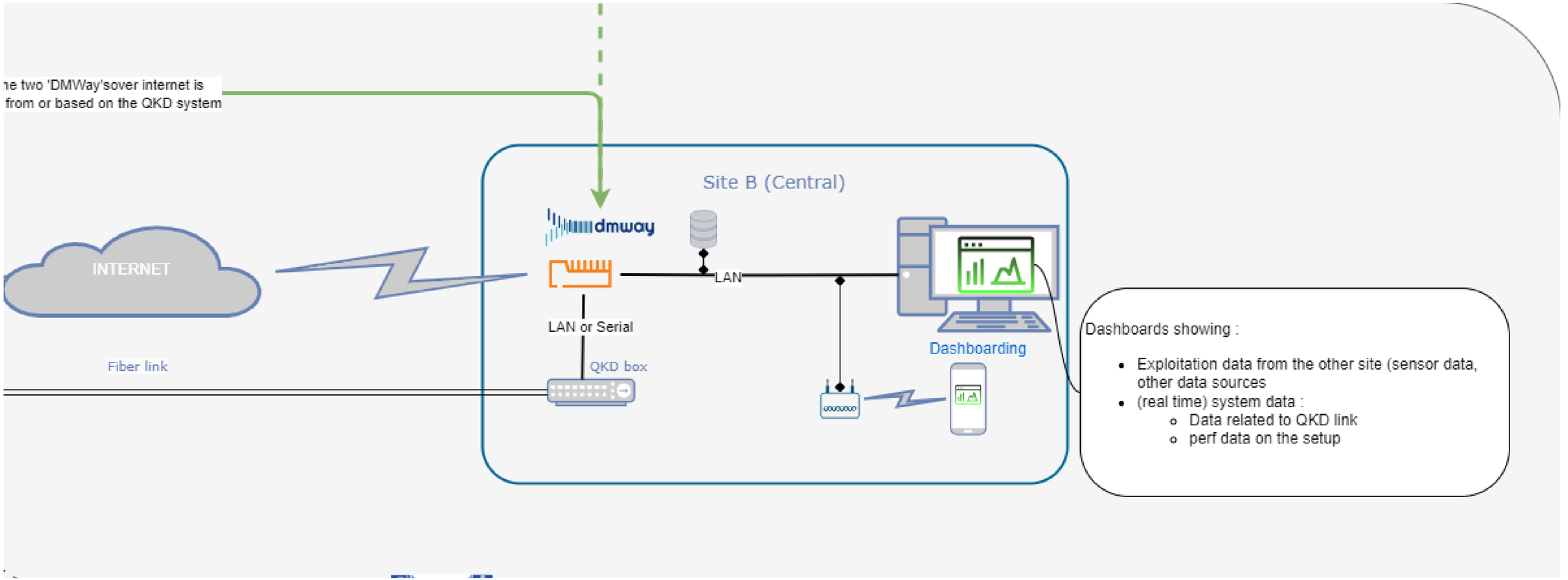


PoC Overview

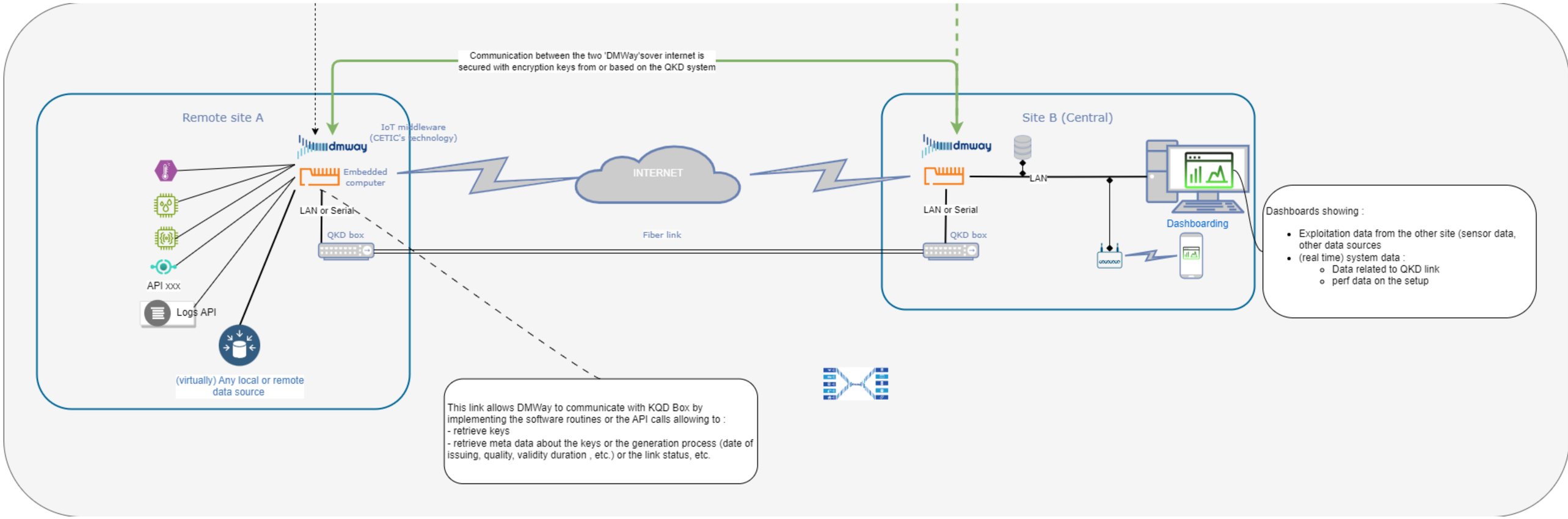
QKD enabled communications with DMWay middleware
Site A



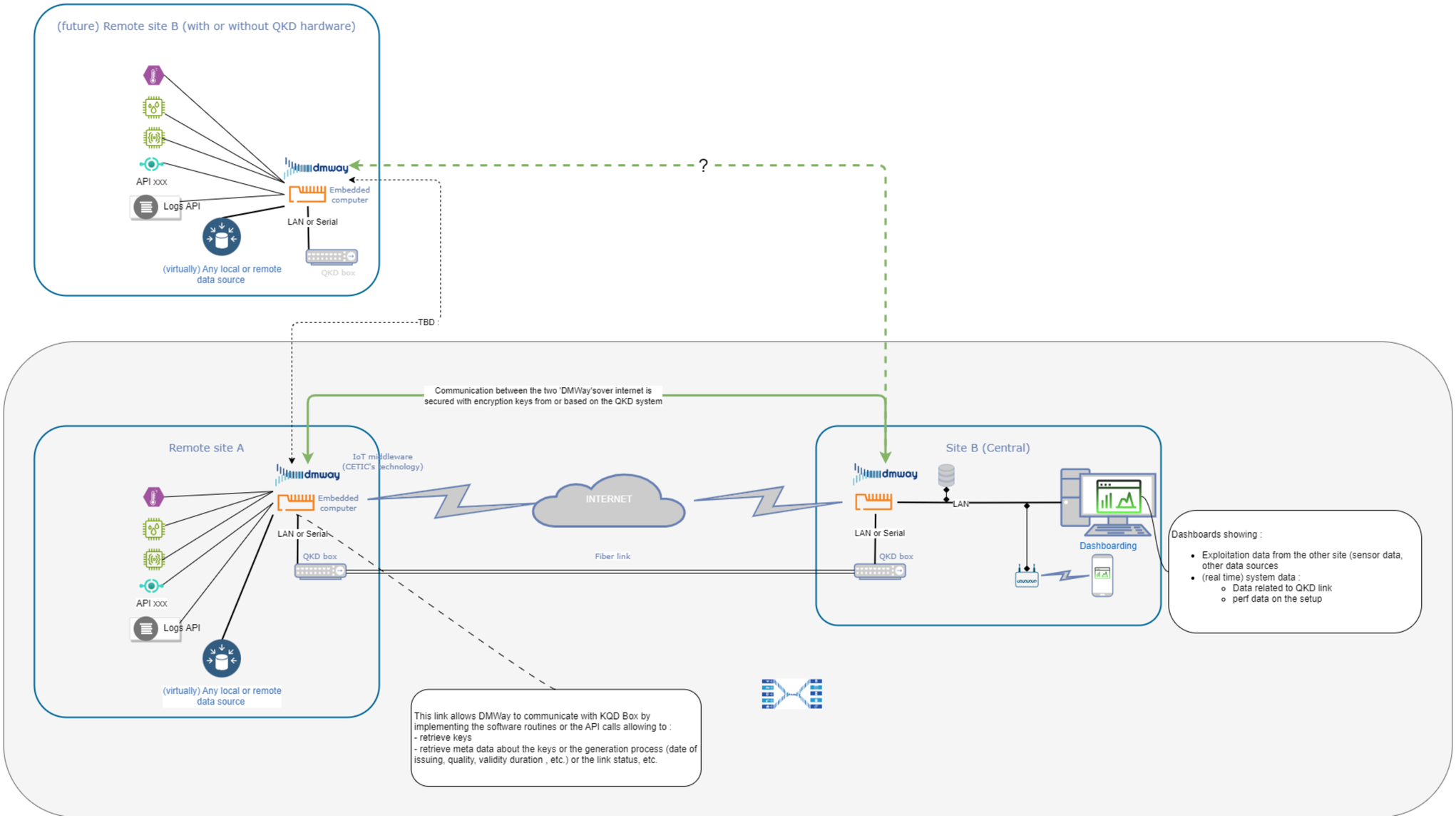
QKD enabled communications with DMWay middleware Site B



QKD enabled communications with DMWay middleware
Full PoC



QKD enabled communications with DMWay middleware
Full PoC – multi (>2) site



USECASE:
KQD enabled security for inter-middleware communications

- Showcase goal : QKD support for secured communication between geographically distributed instances of DMWay middleware

- demonstrator involving DMWay instances communicating through secure links and exploiting quantum keys:
  - One master and 1 slave; (further slaves/sites in the future)

  - Showcase management of different streams of data exploiting QK :
    - (Sensor) data collected from remote instance of DMWay
    - (System monitoring) data with figures on the Quantum Keys exchanged:
      - id,
      - lifespan,
      - other attributes that make sense coming from QKD system

cetic

Your Connection to ICT Research

Thank You

Aéropole
Avenue Jean Mermoz 28
6041 Charleroi - Belgique

Lotfi GUEDRIA

R&D Department Manager

+32 488 238 283

Lotfi.Guedria@cetic.be

twitter.com/@CETIC
twitter.com/@CETIC_be

linkedin.com/company/cetic

info@cetic.be

+32 71 159 362

Q&A

Thanks to all !!