OpenQKD
European Quantum Key Distribution Testbed

Florian Fröwis

CERN, 22 January 2020

ID Quantique company profile

Founded in 2001

Geneva, Switzerland
Seoul, South Korea
Bristol, UK
Boston USA

By 4 quantum physicists from the University of Geneva

95 employees including ~45 engineers/scientists

Investments in 2018 by SK Telecom & Deutsche Telekom

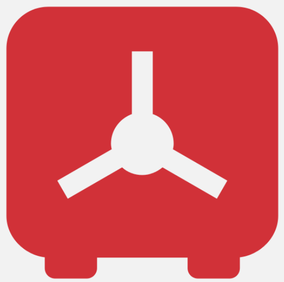
Develops technologies and products based on quantum physics & photonics within 2 business units:
- Quantum-Safe Security
- Quantum Sensing

Performs R&D, production, sales, professional services, integration, support

Clients: Governments / Banks / Gaming Industry / Universities / IT Security / O&G / Telecom

Cryptographic Toolbox: Simplified Overview

Symmetric Cryptography
(secret key)



Asymmetric Cryptography
(public key)

Cryptography before and after Quantum Computing

The hacker’s point of view today…

… and after the
Quantum Computer

IDQ Recommended Path to Quantum Safety

Quantum Random Number Generation (QRNG)

- ✓ **Instantly strengthen your crypto key material**
- ✓ Feed higher quality (Swiss trusted) entropy into key generation servers, HSMs, Linux & crypto applications and connected devices

Crypto agility to move to Post Quantum Crypto

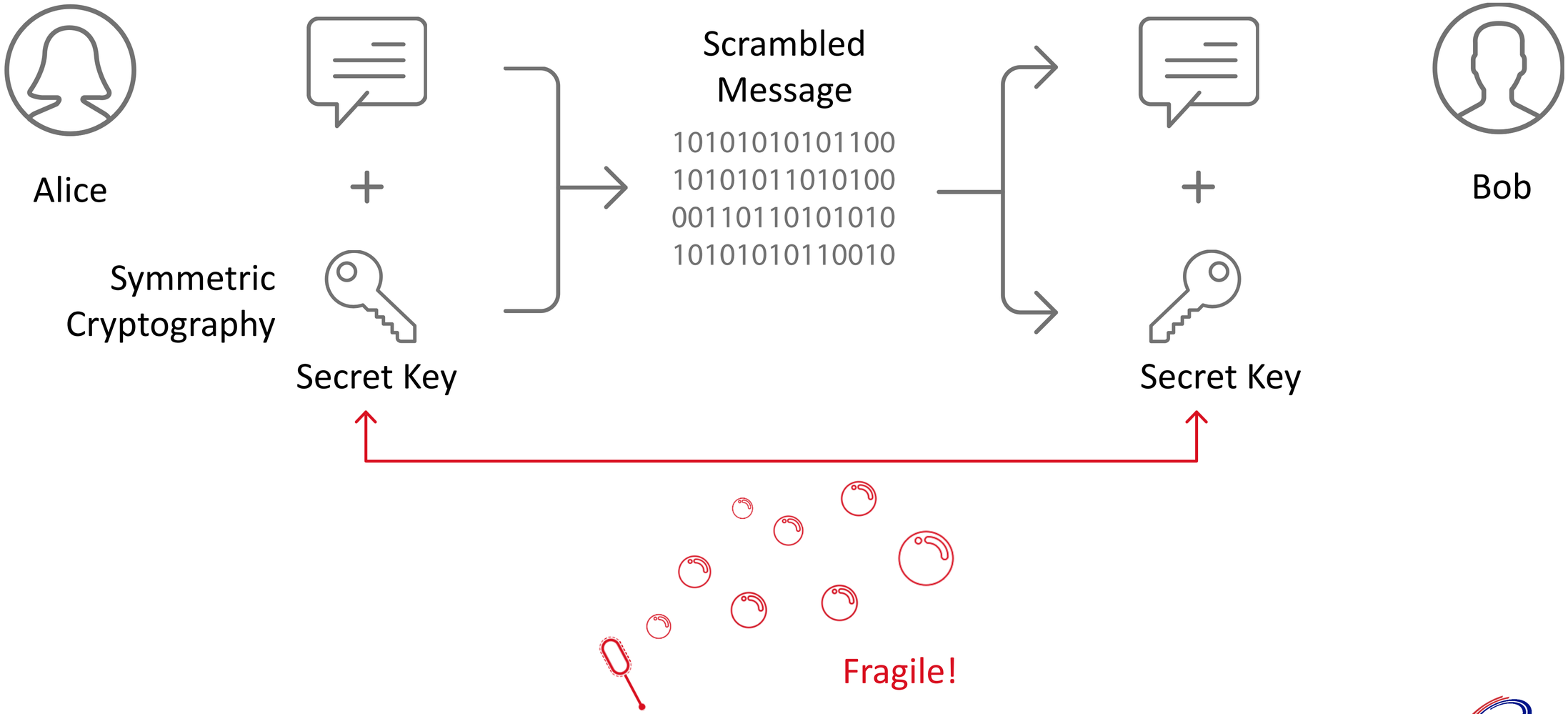
- ✓ Be **crypto-agile** to move to next generation Post Quantum Crypto
- ✓ Be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

Quantum Key Distribution (QKD)

- ✓ **Quantum Cryptography** for secure transmission
- ✓ Provide forward secrecy & anti-eavesdropping of private key exchange/back up
- ✓ Ensure **Information Theoretic Security** for confidentiality to guarantee ownership for the next decade (Post-Quantum era)
- ✓ Use QKD today for backend **IP protection**

ID Quantique PROPRIETARY

Quantum Key Distribution (QKD): Basic Idea

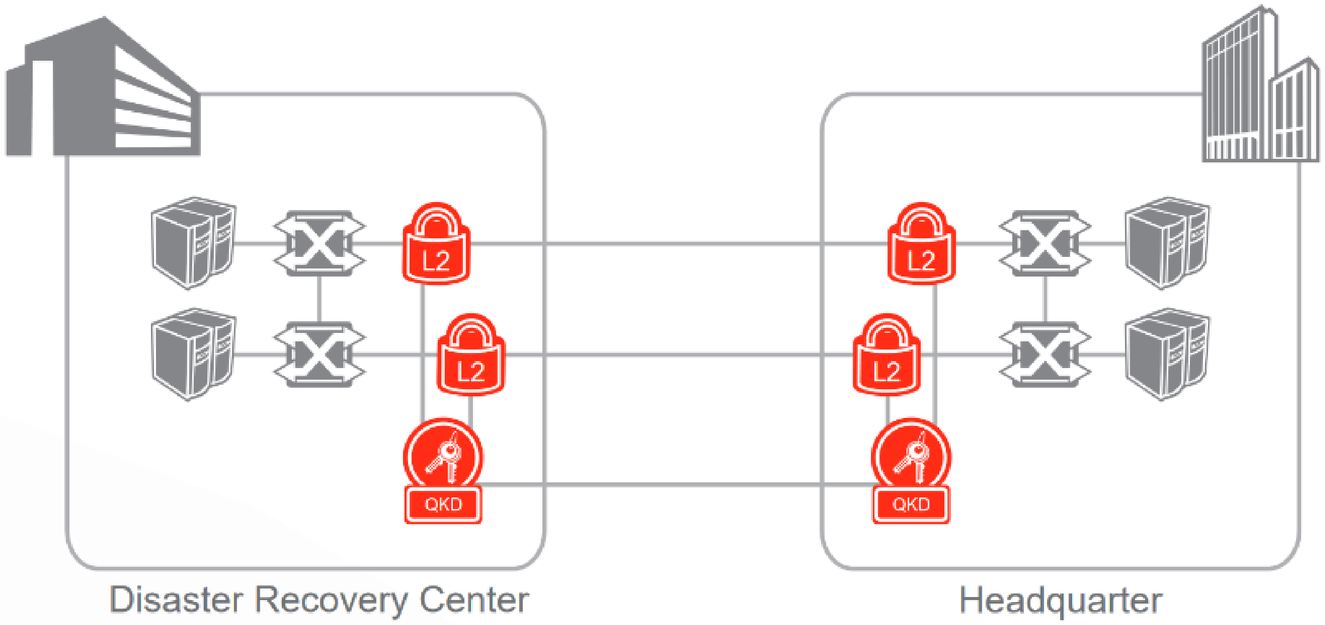


ID Quantique PROPRIETARY

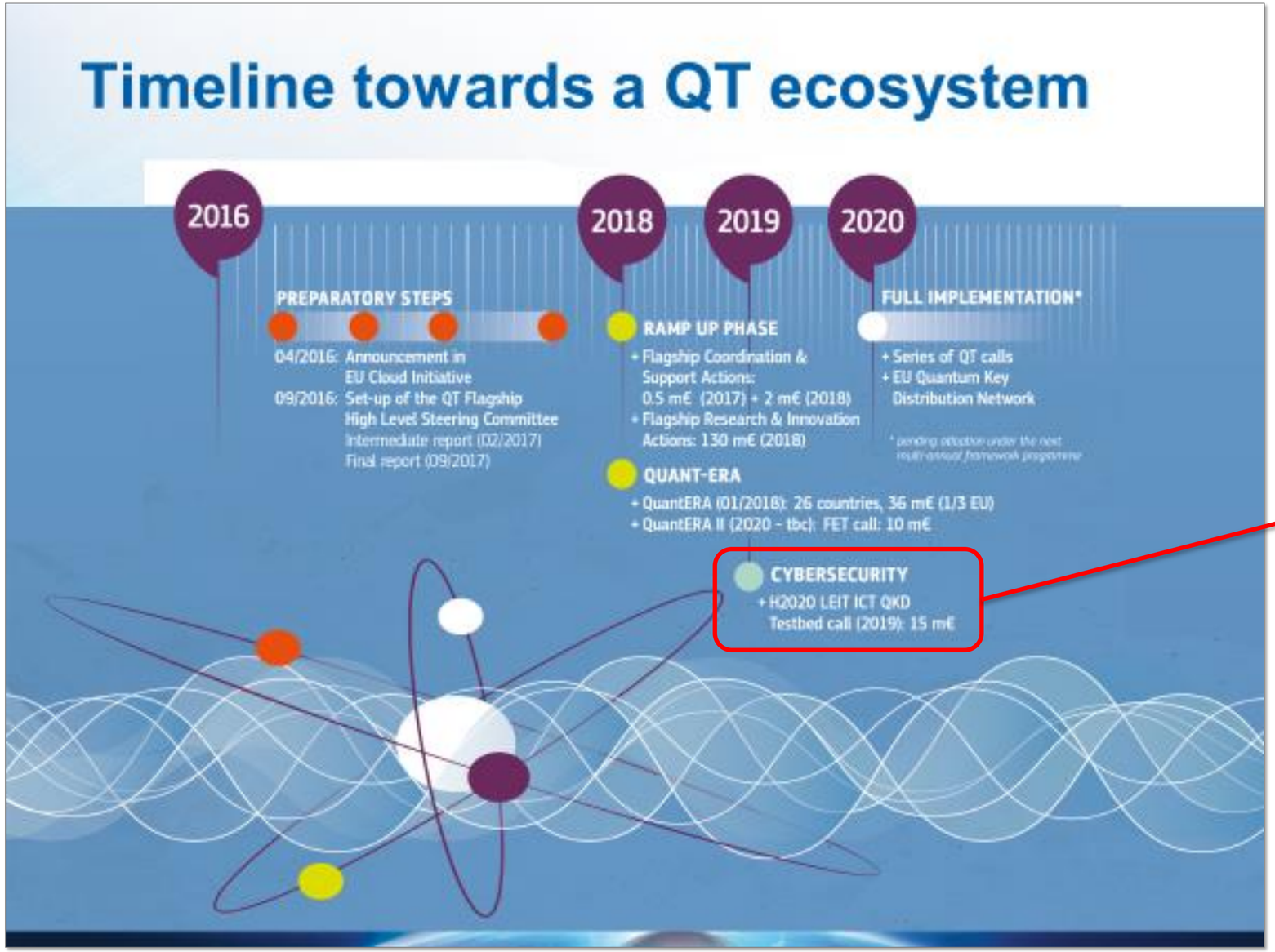
QKD in Data Center Interconnect

Quantum Cryptography-secured data center link

- Business need
  - Atos (e.g. Siemens) acted as managed service provider for a leading financial client
  - Needed to secure DC - DC link for critical information



QT Vision in Europe



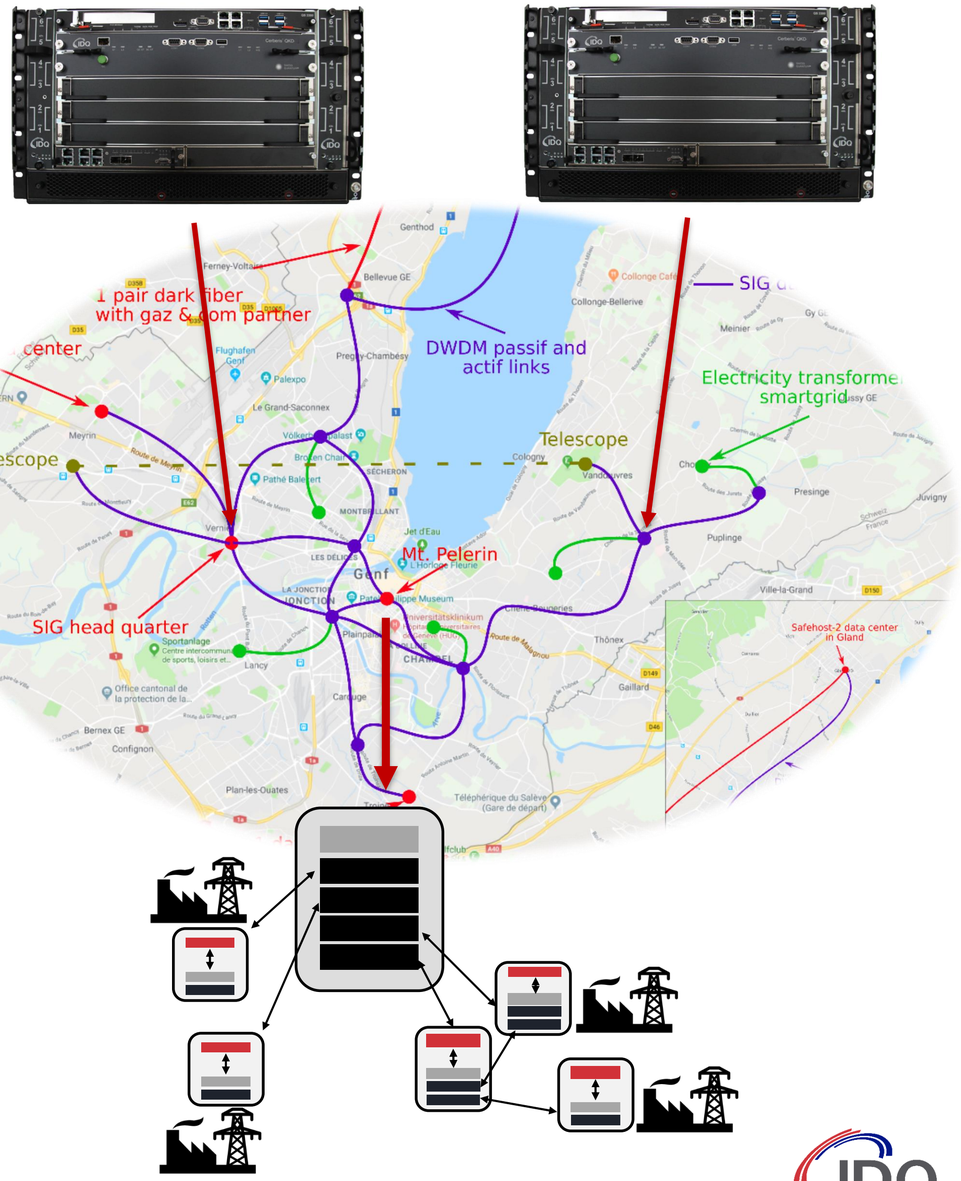
Quantum Flagship (qt.eu)
1B€ for Quantum Technologies
(2018-2027)

Testbed – 15M€
2019-2022

ID Quantique PROPRIETARY

Scope of OpenQKD

- System development
- Network integration
- 30+ use cases: testing and evaluation
- Further objectives
  - Innovation for European QC ecosystem
  - Collaboration and open source solutions
  - Prepare pan-European quantum communication infrastructure



OPENQKD eco system

- **QKD suppliers**
- **QKD R&D partners**
- **QKD network developers**
- **Suppliers of network encryption**
- **Fiber infrastructure operators**
- **Telecom operators**
- **Aerospace and satellite industry**
- **Standardisation institutes**
- **Early adopters**

16 OPENQKD test sites

Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

Bratislava CZ
Government

Cambridge UK
Data Centers

Ostrava CZ
High Perf. Comp.

Paris FR
Academic network

Graz AT
Healthcare

Geneva CH
Smart Grid

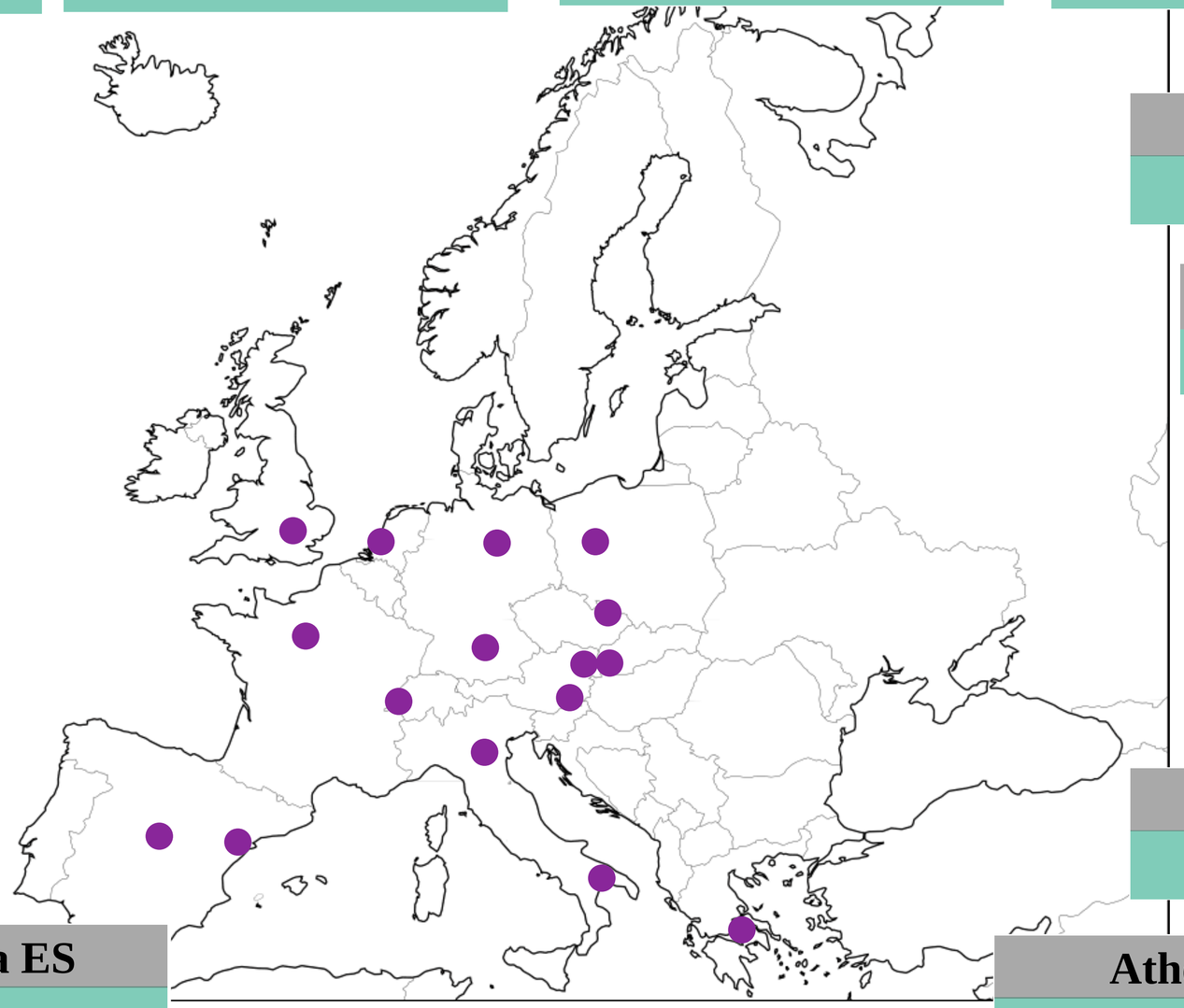
Padua IT
Free-space QKD

Oberpfaffenhofen DE
Satellite QKD

Matera IT
Satellite QKD

Barcelona ES
Video Com

Athens GR
Data Com



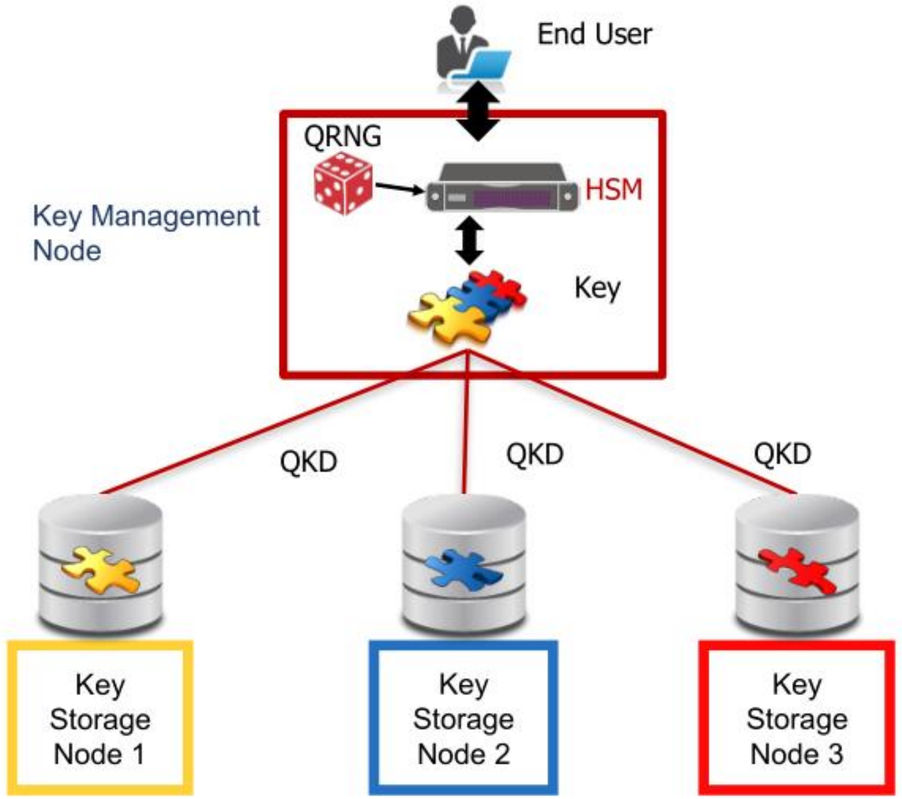
Use case example

Quantum Vault (deployed in Geneva)

- End User wants to securely store a cryptographic asset: protecting against failures and attacks

- Key enabling technology
  - Quantum Random Number Generation (QRNG)
  - Shamir Secret Sharing Protocol
  - Quantum Key Distribution (QKD)

- Partners:
  - Mt Pelerin: blockchain bank*
  - IDQ: QKD supplier
  - SIG: network operator and host
  - PSNC, CERN openlab: host
  - Equinix: host



Timeline in 2020

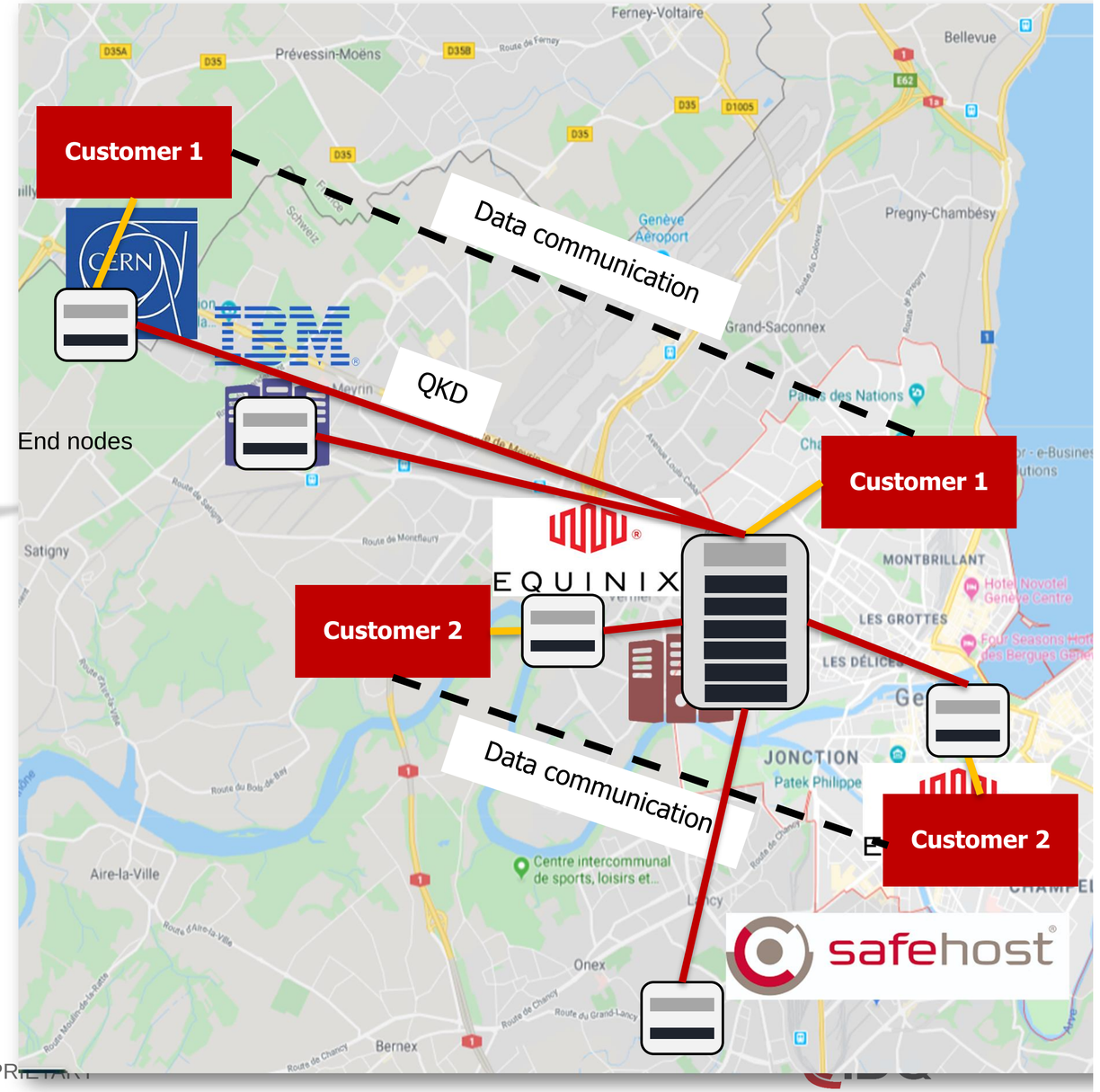
Quantum Vault use case:

- January: deploy infrastructure
- March: fully operational
- September: use case report

Open call initiative of OpenQKD

- February: call opens
  - **CERN openlab and IDQ apply**
  - **Any other third partner also welcome**
- June: project start
- Project length: 6 months

Open Calls!!!



ID Quantique PROPRIETARY

Let’s stay entangled …

Send an email to alice@openqkd.eu or bob@openqkd.eu

Follow us https://twitter.com/openqkd | @openqkd

Connect with us www.linkedin.com/in/openqkd | OPENQKD Project

Find information https://openqkd.eu/

For more information

http://www.idquantique.com/

florian.froewis@idquantique.com

Improvements on system level

Fibre-based: high TRL

- Cost of ownership I:
  - Smaller
  - Cheaper components (integrated photonics)
  - “Plug and play”
- Increase of distance from ≈50km to ≈150km
- Increase rate from kb/s to Mb/s
- Device independent

Free-space: low TRL

- Proof of concept

Cerberis 3: COW protocol,
ATCA chassis

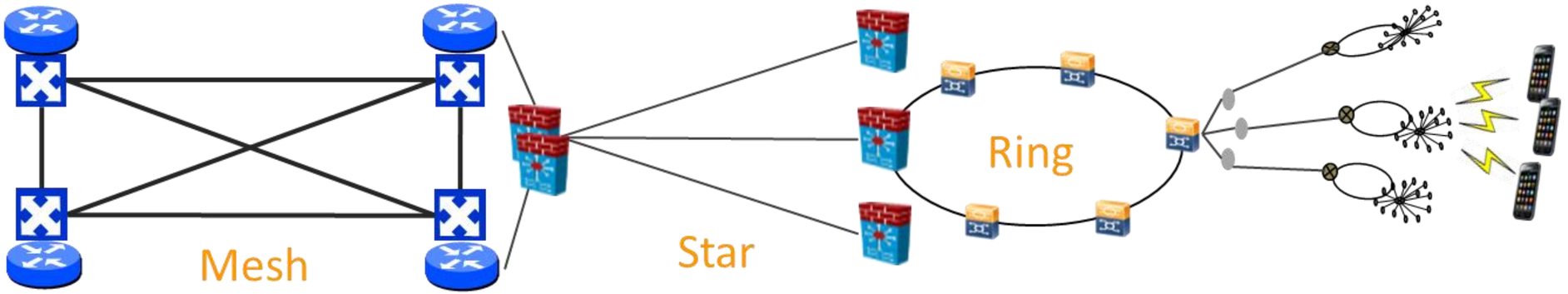
Quantum Access Network (Short-Range)

- 19” 6U chassis
- Maximum transmission loss (typ.): 12dB (Premium 18dB upon availability)
- Secret key rate (typ.): 3 kb/s after 50 km

ID Quantique PROPRIETARY

Modern communication networks

Backbone	Core	Access



SK telecom

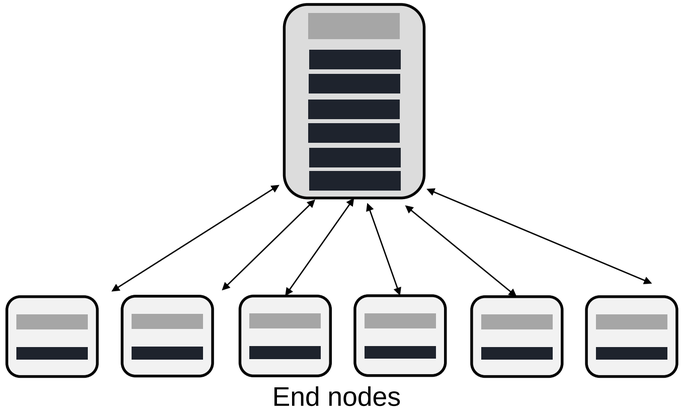
Quantum Key Distribution

5G standard security & QRNG

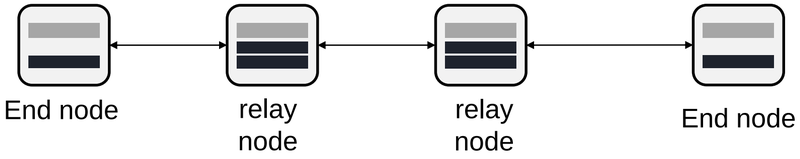
Examples of QKD network topologies

Point to point

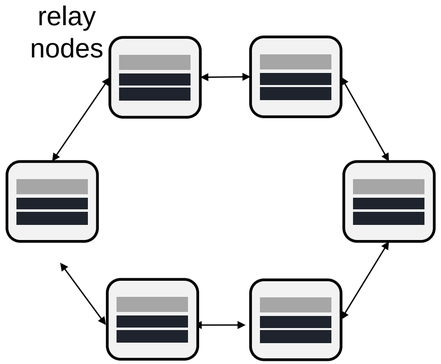
Hub and spoke



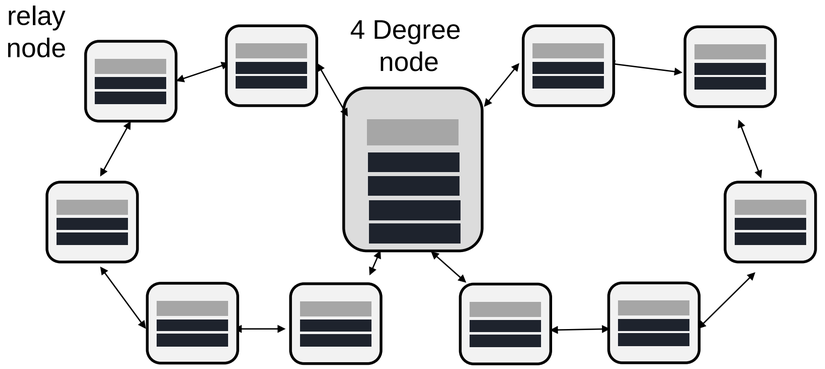
Point to point (with relay for long distance)



Ring network



2-Ring network



Optical blade (Alice or Bob)- 2U

KMS blade -1U

Quantum channel (dark fiber or wavelength in O-band)

KMS Channel (logical mux possible)

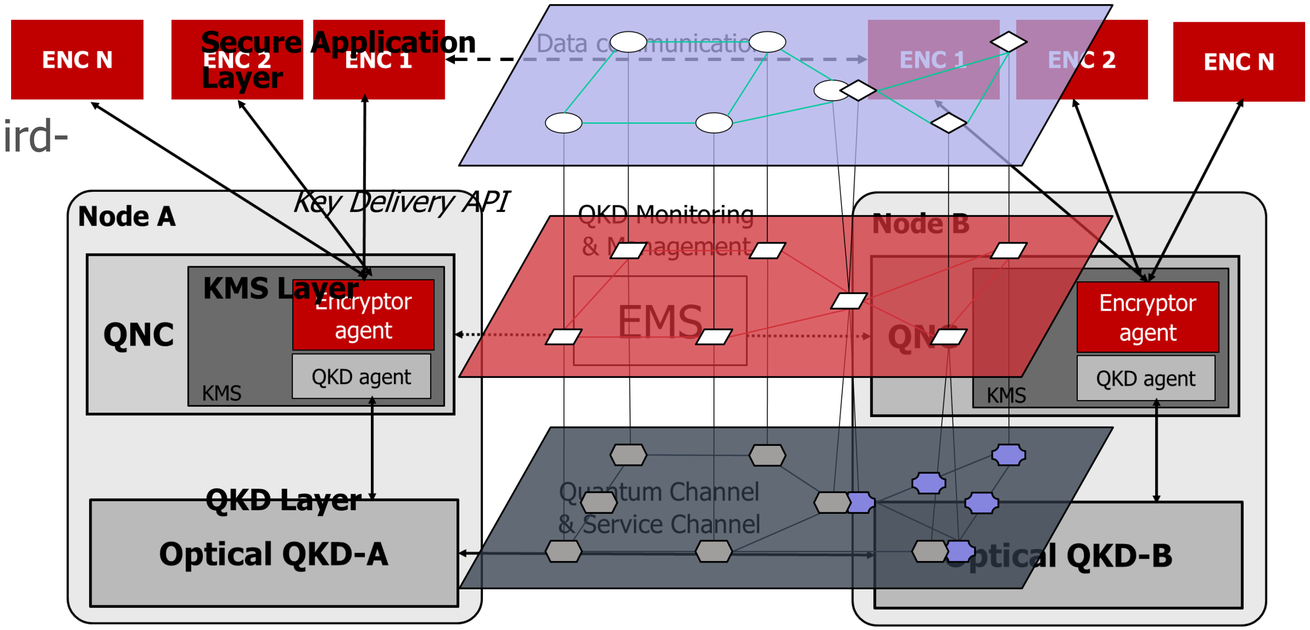
Service channel (C-band)

QKD location (node), One KMS per node.
May host several 6U-chassis depending on degree (number of optical blades)

ID Quantique PROPRIETARY

Network integration

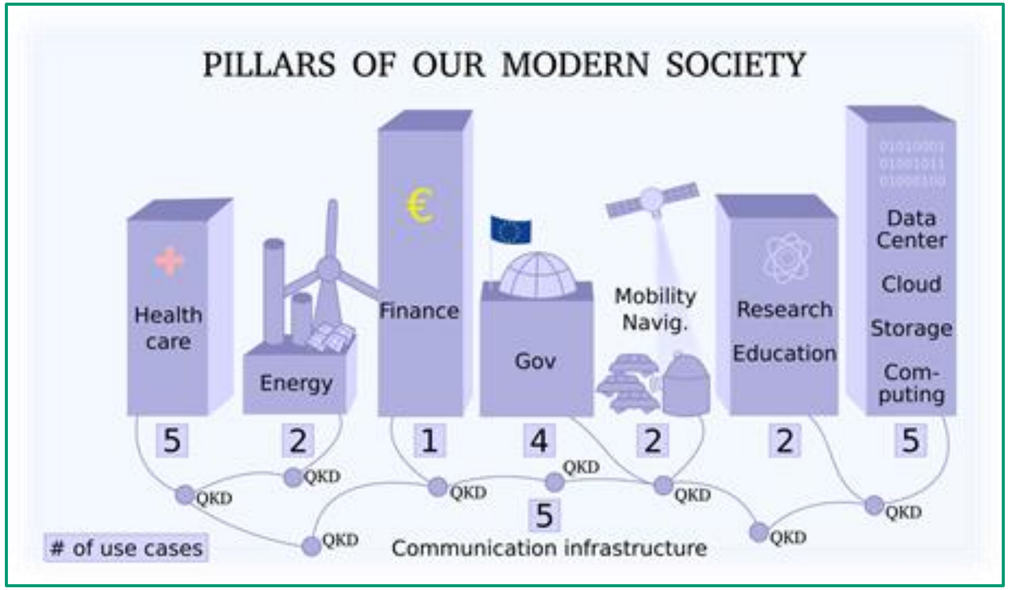
- Total cost of ownership II:
  - Multiplexing of QKD signals on fibres with third-party traffic
- Interoperability
  - Between QKD and encryptors
  - Between QKD links from different vendors
- →Standards
- Key management system → SDN
- 5G (network slicing, …)
- Different network topologies



Use cases

Operation of use-cases deriving from Secure Societies needs

- Demonstration of more than 30 use-cases for QKD featuring:
  - realistic operating environments
  - end-user applications and support



Range of use-cases:

- Secure and digital societies
  - Inter/Intra datacenter comm., e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography
- Healthcare
  - Secure cloud storage services and securing patient data in transit
- Critical infrastructure
  - QKD for telecom networks, 5G infrastructure and securing smart grids

Open Calls!!!

OPENQKD Metadata

Call:H2020-SU-ICT-2018-3, Innovation action
Topic: SU-ICT-04-2019 Quantum Key Distribution testbed
Grant Agreement No.: 857156

Estimated project cost: **~18M**
Requested EU Contribution: **~15M**

Start Date: **02 September 2019**
Duration: **36 months**

13 EU and associated countries: AT, BA CZ, DK, FR, DE, IL, IT, NL, PL, ES, CH and UK

Coordination:
AIT Austrian Institute of Technology

Partners: **38**

© 2016 ID Quantique SA, Switzerland | page 20

ID Quantique PROPRIETARY