Overview of the current standardisation landscape on QT

1st AIT Workshop on
Standardisation and certification of QKD systems and QKD networks

On-line, Sept. 28th 2021

Vicente Martin,
Vicente@fi.upm.es

Standards & QT

- Standard: **Consensus documents approved** by a Standard Developing Organization (**SDO**).
  - Provide **rules, guidance, vocabulary**, characteristics of devices, methods, processes…
- They are **based on consolidated results** from science, technology or experience.
  - Their purpose is to **maximize the benefits for a community of producers/consumers.**
- **What to standardize?**
  - **Quantum technologies (QT) cover a very broad TRL spectrum.**
  - **Which QT is mature enough to need an standard?**
  - **Which QT interacts with other technology to need an standard?**

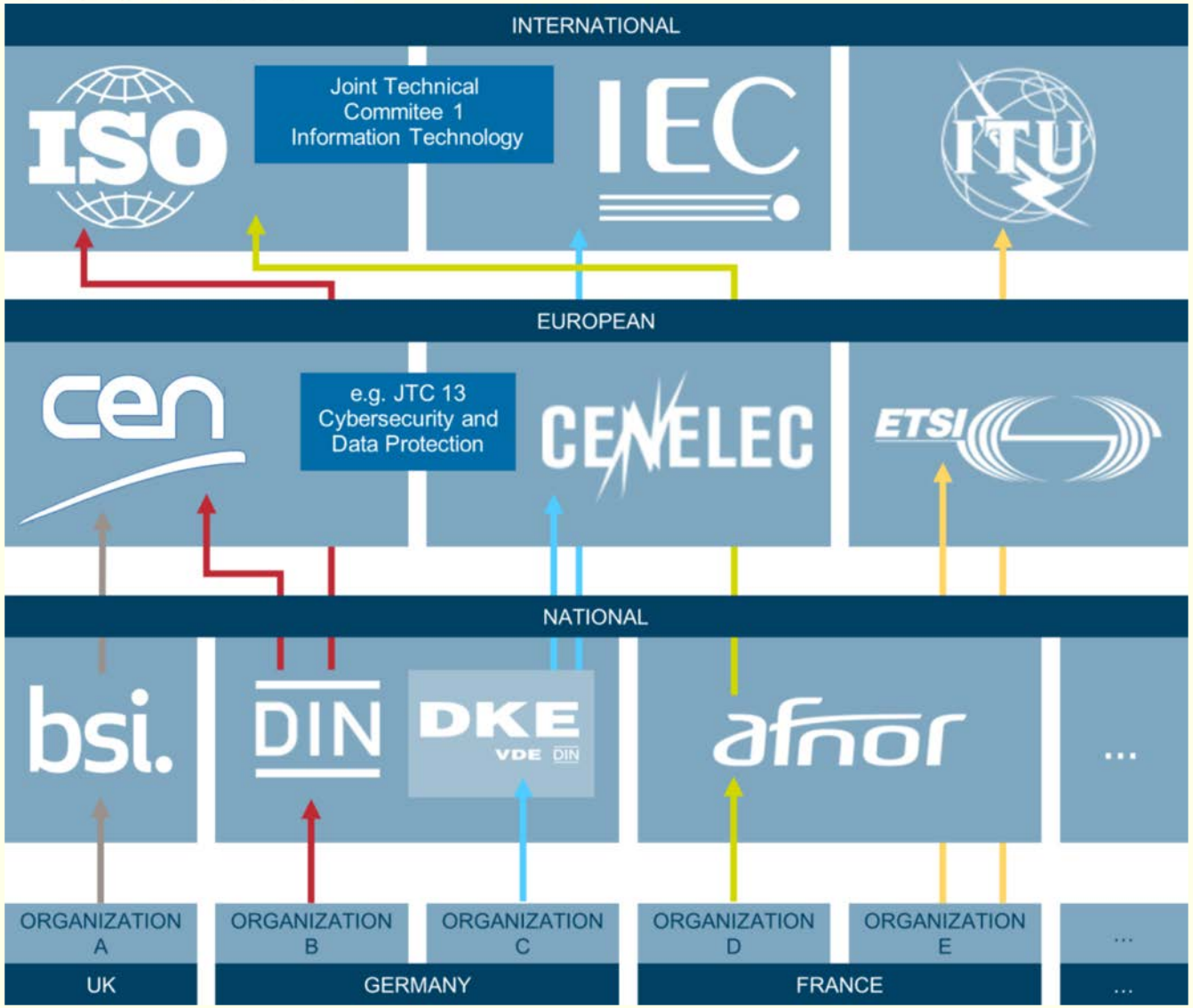
Today's Main themes in QT & standards

- **QKD**
- QKD **Certification**
- General **Quantum Communications**
  - Quantum Internet
- Quantum Networking
- **Quantum Computing**
  - Vocabulary, performance & benchmarking
- **General Quantum Technologies**
  - Roadmapping, including: communications, computing, sensing and simulation.

Standards: QKD: Security Certification

- **Security Certification**: Why a consumer should **trust that a given QKD implementation is secure**?
  - **Formal Security** in the QKD context: Information Theoretic Security
    - It is not computational security, as is usual today.
  - **Practical security** in the QKD context: Implementation
    - To what extent the **implementation matches the formal proofs**?
      - Research is still needed.
    - Define requirements that a given implementation has to met for a given use
      → **protection profiles.**
      - Rooted in much conventional experience.

Standards: Organizations



European

International

National Std. Organizations

Entities: companies, etc.

National

From D9.1 OpenQKD

In This meeting: QKD

ISO/IEC: The International Organisation for Standardisation/International Electrotechnical Commission

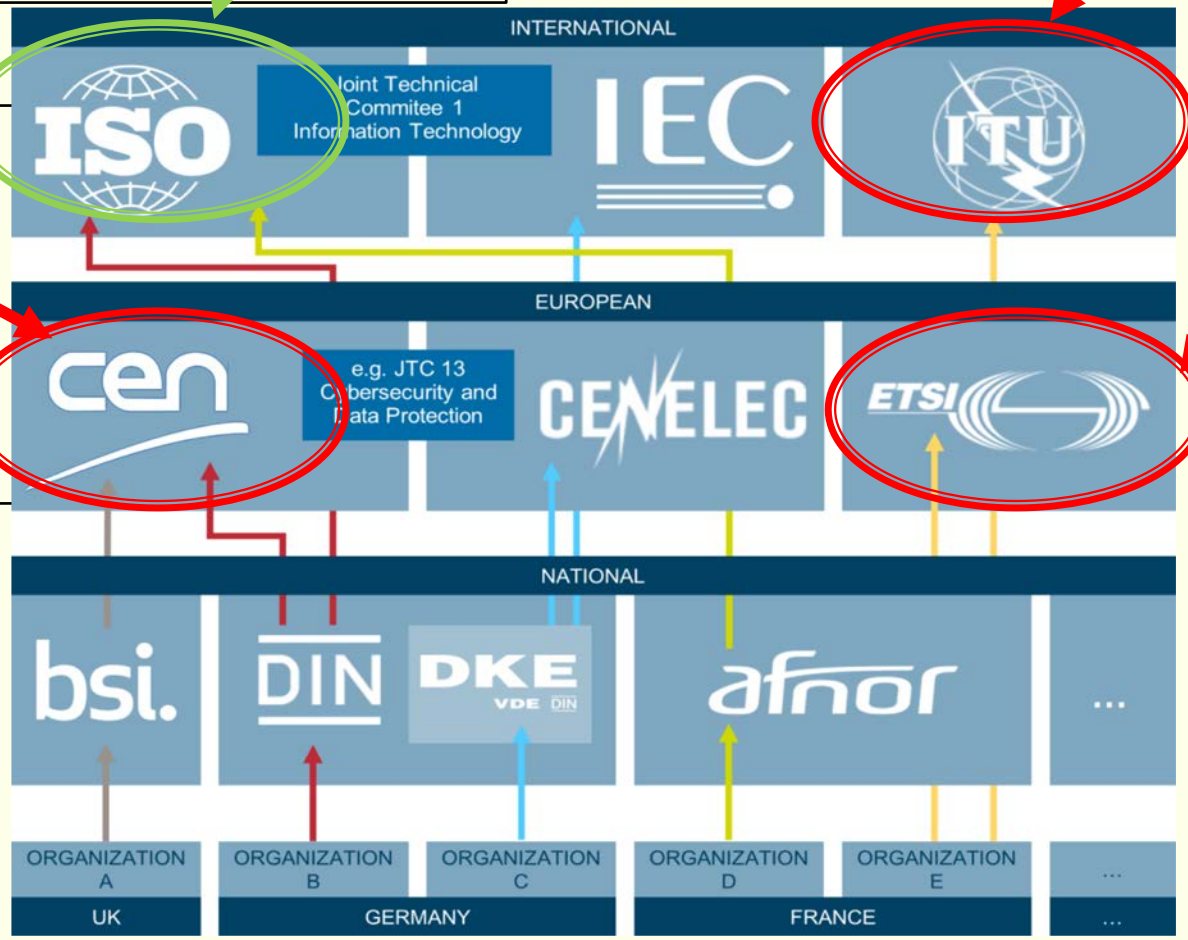
- JTC 1/SC 27 (IT Security)

International Telecommunications Union

- Focus Group on Quantum Information Technologies for Networks
- SG 13: Future Networks
- SG 17: Security

European Committee for Standardization:

- Focus Group on Quantum Technologies



European Telcommunications Standards Institute:

- Quantum Industry Specification Group

International

European

National Std. Organizations

National

Entities: companies, etc.

From D9.1 OpenQKD

Standards

- Other Relevant organizations.
  - **ANSI**: American National Standards Institute.
    - Private, oversees US standards ("US CEN"?)
  - **NIST**: National Institute of Standards and Technology
    - Physics & Tech lab. Not Regulatory
    - However FIPS (Federal Information Processing Standards) came from here (e.g FIPS-120). The PQC call. NIST-800 (e.g. On key management)
  - **IETF**: Internet Engineering Task Force
    - Not for profit. Non-mandatory standards (but widely used: RFCs come from here)
    - IRTF: Internet Research Task Force (longer term, research oriented)
      - QIRG: "Quantum Internet Research Group" (2018)

Standards

- Other Relevant organizations.
  - **IEEE-SA**: Institute of Electrical and Electronic Engineers – Standards Association
    - Not endorsed by any government to produce standards.
      - Industry participated.
      - Examples IEEE 802.3 (ethernet) 802.11 (WiFi), 754 (Floating point), 1363 (Public Key Crypto), 1588 (Precision Time Protocol)
    - P1913 “SW Defined Quantum Communications” (2016)
    - P7130 “Quantum Technologies Definitions” (2020)
    - P7131 “Quantum Computing Performance Metrics & Performance Benchmarking” (2020)
  - **GSMA**: “Group Special Mobile” Association.
    - Not a group doing standardization, but highly influential.
    - White paper “Quantum Computing, Networking and Security “

SDOs with Q. Activities. Timeline

The Q-ambrian Explosion of Life…

2008

ETSI ISG-QKD

. . .

2016

IEEE-SA P1913

8 years

2018

ITU-T (SG13, SG17)

2019

* ITU-T (FG-QIT4N)

* ISO/IEC JTC 1/SC 27

* IRTF

2020

CEN/CENELEC FG

Q. Computing +

Q. Communications

Thank you!

1st AIT Workshop on
Standardisation and certification of QKD systems and QKD networks

Vicente Martin,
Vicente@fi.upm.es

EU H2020 Grant 820466

EU H2020 Grant 857156