SWISS
QUANTUM

IDQ
FROM VISION TO TECHNOLOGY

Quantum-Safe Security

Relevance for Central Banks

June 2018

Outline

- ID-Quantique in short
- The quantum threat
- The solution: quantum-safe cryptography
  - Quantum key generation (QRNG)
  - Quantum Resistant Algorithms
  - Quantum Key Distribution (QKD)
- QKD use cases for Central Banks

Company Profile

Founded in 2001

By 4 quantum physicists from the University of Geneva

Geneva, Switzerland
Seoul, South Korea (SKT Invest.)
Hangzhou, PRC (JV)
Bristol, UK

60 employees in CH, including 30 engineers/scientists

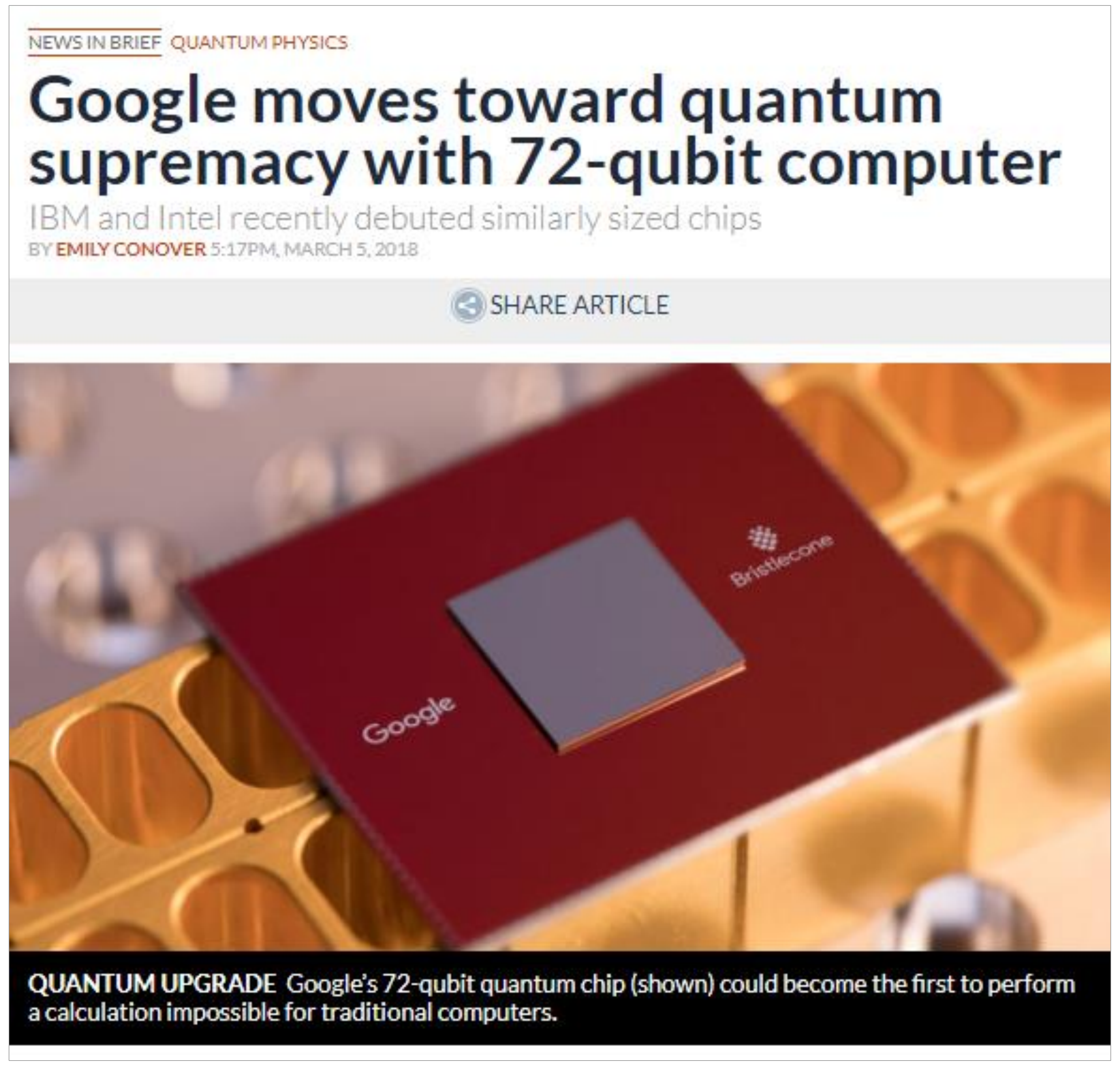
Develops technologies and products based on quantum physics within 2 business units:
- Quantum-Safe Security
- Quantum Sensing

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

Clients: Governments / Banks / Gaming Industry / Universities / IT Security

The Quantum Threat

Quantum Computing: Opportunites & Threats



NEWS IN BRIEF QUANTUM PHYSICS

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

SHARE ARTICLE

QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.

Opportunities:

- **Large data set problems**
- **Needle in Haystack problems**
- **AI**
- **…**

THREATS: **break current public key cryptography (DSA, RSA, ECC…)**

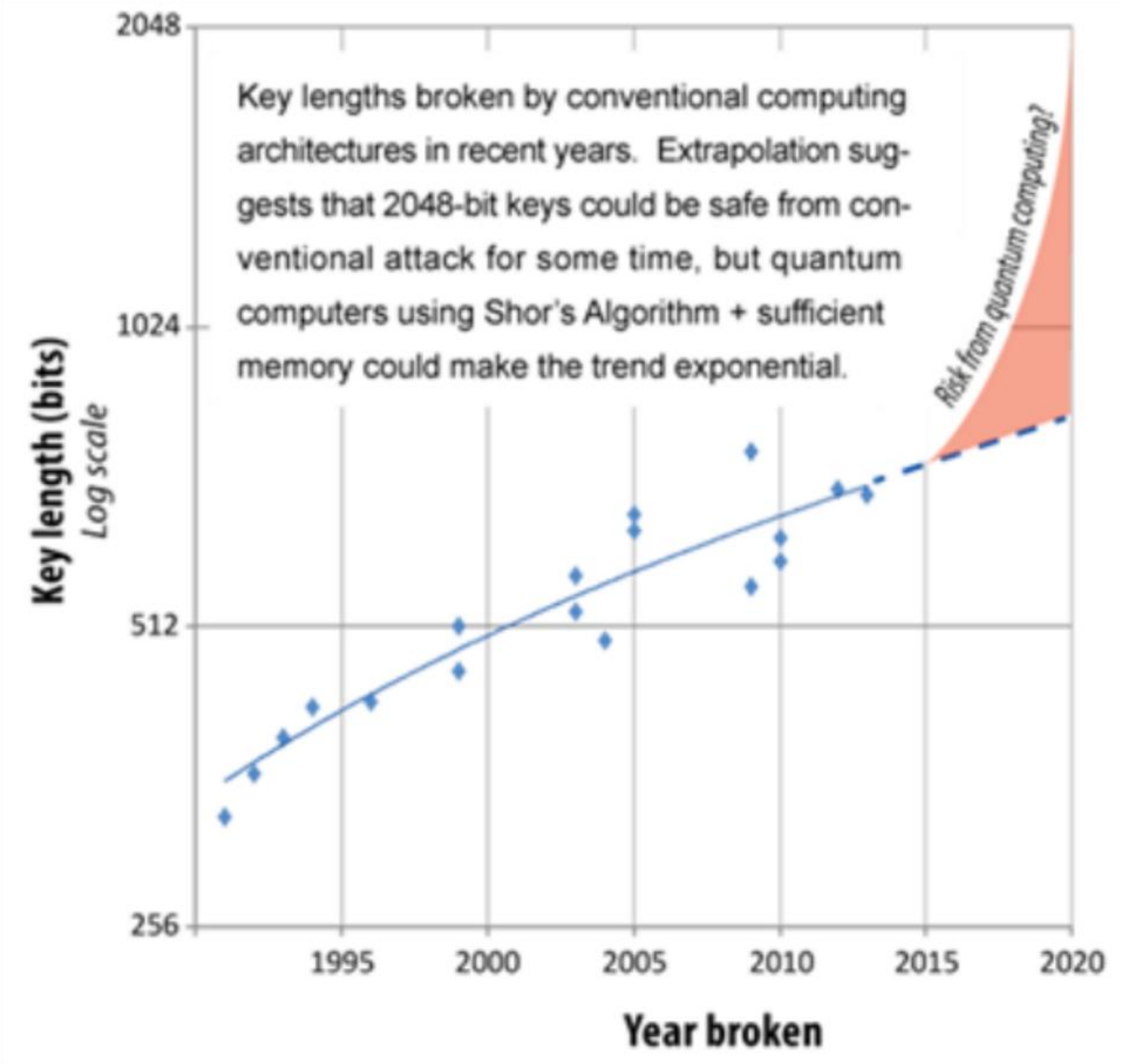
- Huge breakthroughs in quantum computing in recent years
- Massive investment in "quantum supremacy" by Google, Intel & IBM
- “Quantum supremacy can be comfortably demonstrated with 49 Qubits, a circuit depth exceeding 40, and a two qubit error below 0.5%” (Julian Kelly, Research Scientist, Quantum AI Lab, March 2018)

- Computation with Qubits
- Main difference: build **coherent superposition** of states
- But a **measurement** always gives one of the two states only
- Behaves like a massively parallel computer
- Solves problems in much fewer steps

Timeline for the Quantum Computer

- Large-scale quantum computing is 10-15 years away
- 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026
- 1 in 2 chance by 2031

Estimates by Prof. Michele Mosca
Institute for Quantum Computing, University of Waterloo (at ETSI/IQC workshop 09/2017)


Key lengths broken by conventional computing architectures in recent years. Extrapolation suggests that 2048-bit keys could be safe from conventional attack for some time, but quantum computers using Shor's Algorithm + sufficient memory could make the trend exponential.

Extract form ETSI White Paper No. 8
"Quantum Safe Cryptography and Security

Fast forward

TLS Protocol Insecure

Digital Signature can be forged
(and Blockchain)

Message Authentication forged

Network Encryption Insecure

Quantum Computing Brings a Paradigm Shift

SWISS QUANTUM

Next generation of cryptographic infrastructure

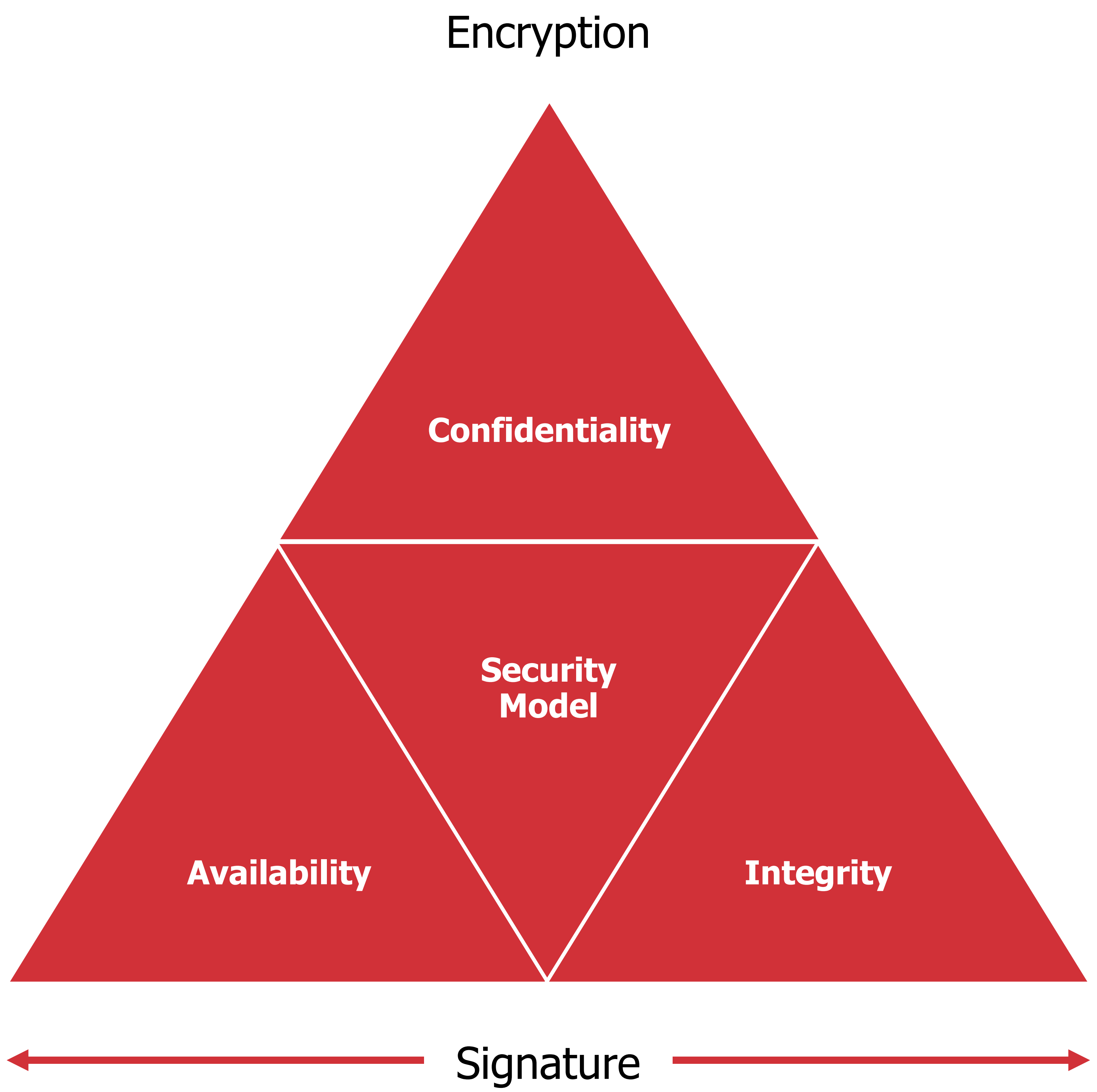
- Must have quantum-safe alternatives
- Should have algorithmic agility built in
- Should be underpinned by strong keys

PKI – Trust Establishment: **Plan now!**

- Need "crypto-agile" or hybrid PKI solutions now
- Can re-sign shortly before the crypto broken by quantum computer

Data Confidentiality: **Act now!**

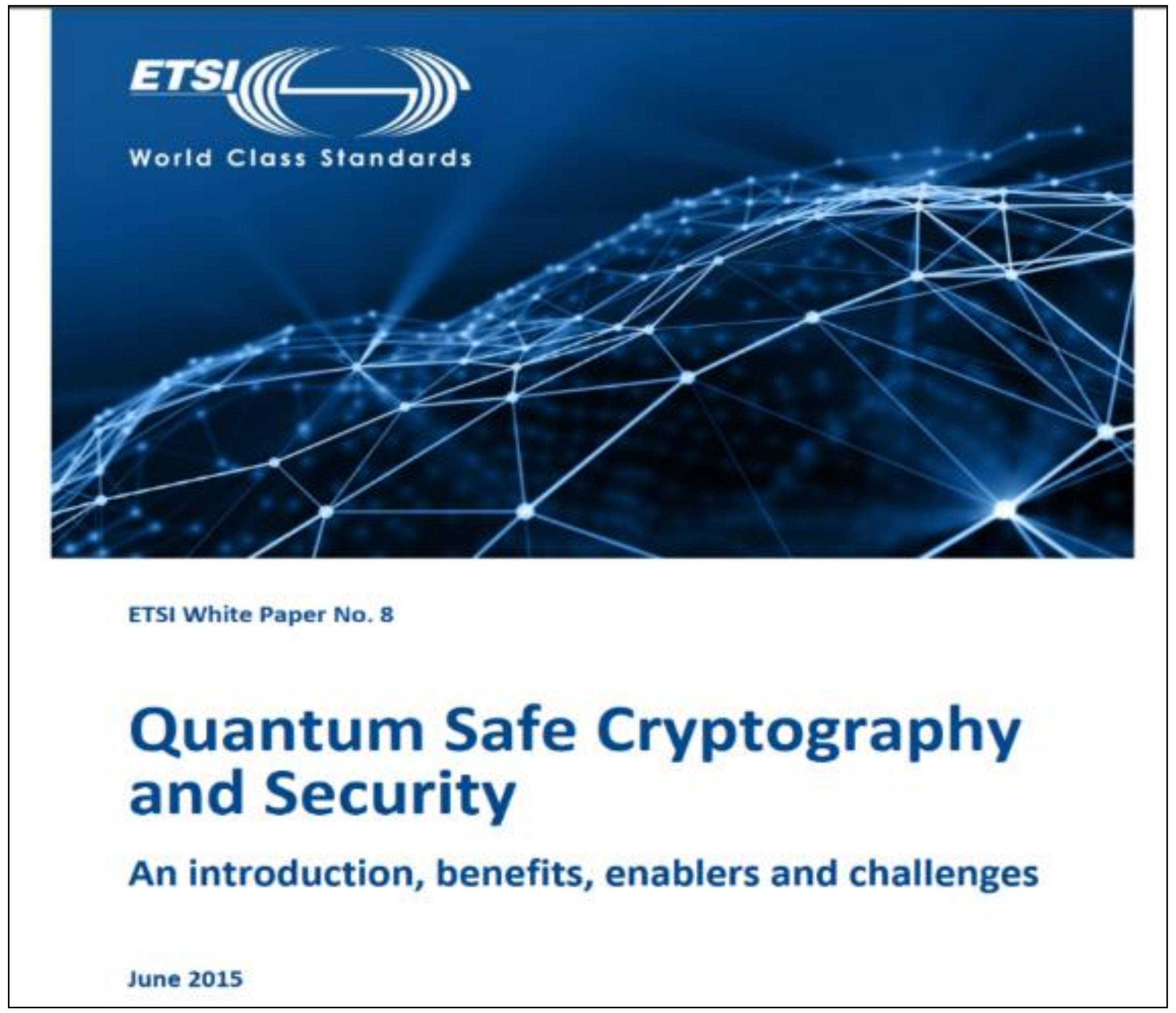
- Threat is "Download Now, Decrypt Later"
- The deadline to be Quantum-Safe depends on the information lifetime of your data



IDQ

The Solution:
Quantum-Safe Cryptography

Quantum-Safe Transition



ETSI

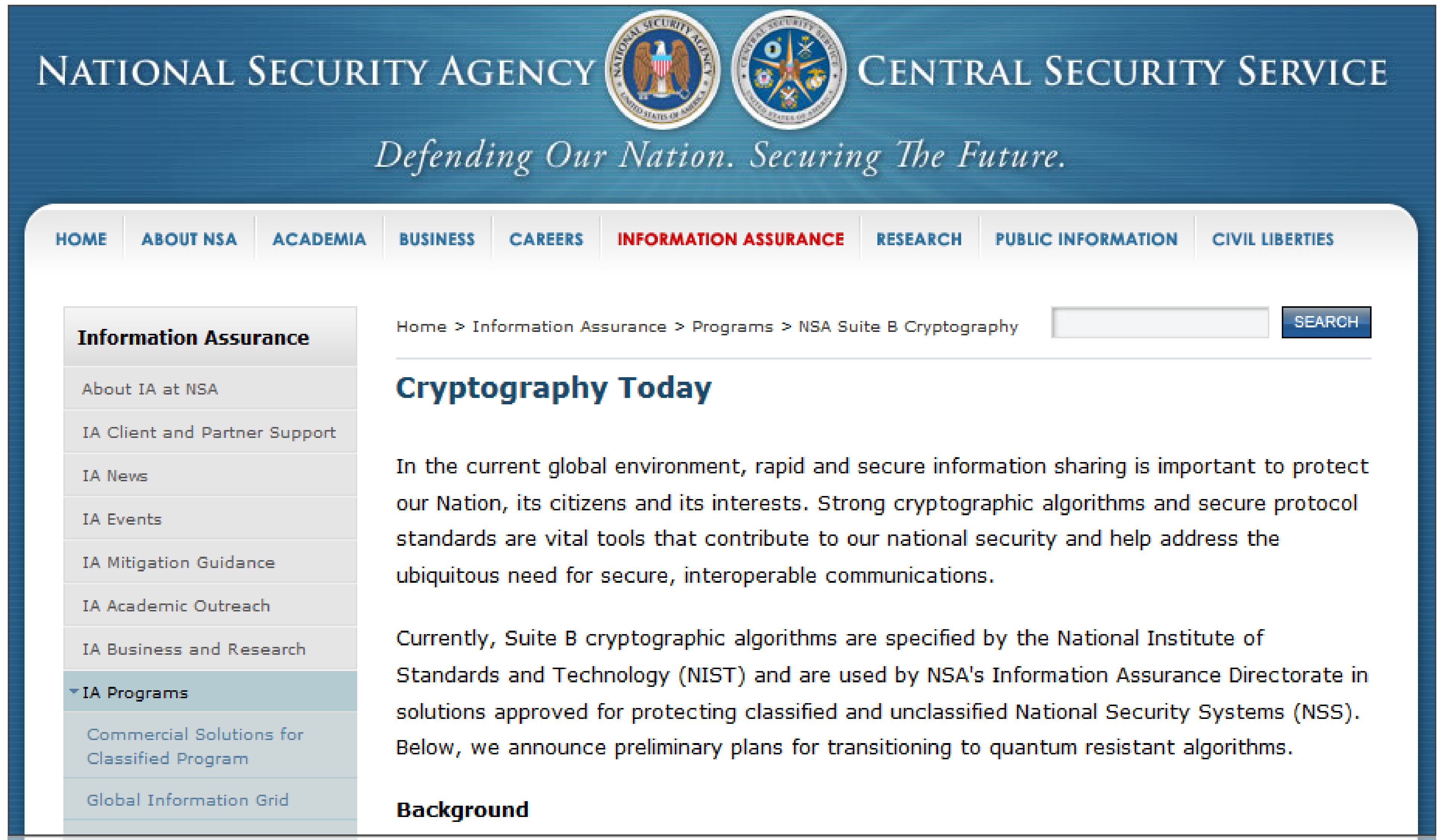
World Class Standards

ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

June 2015



NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

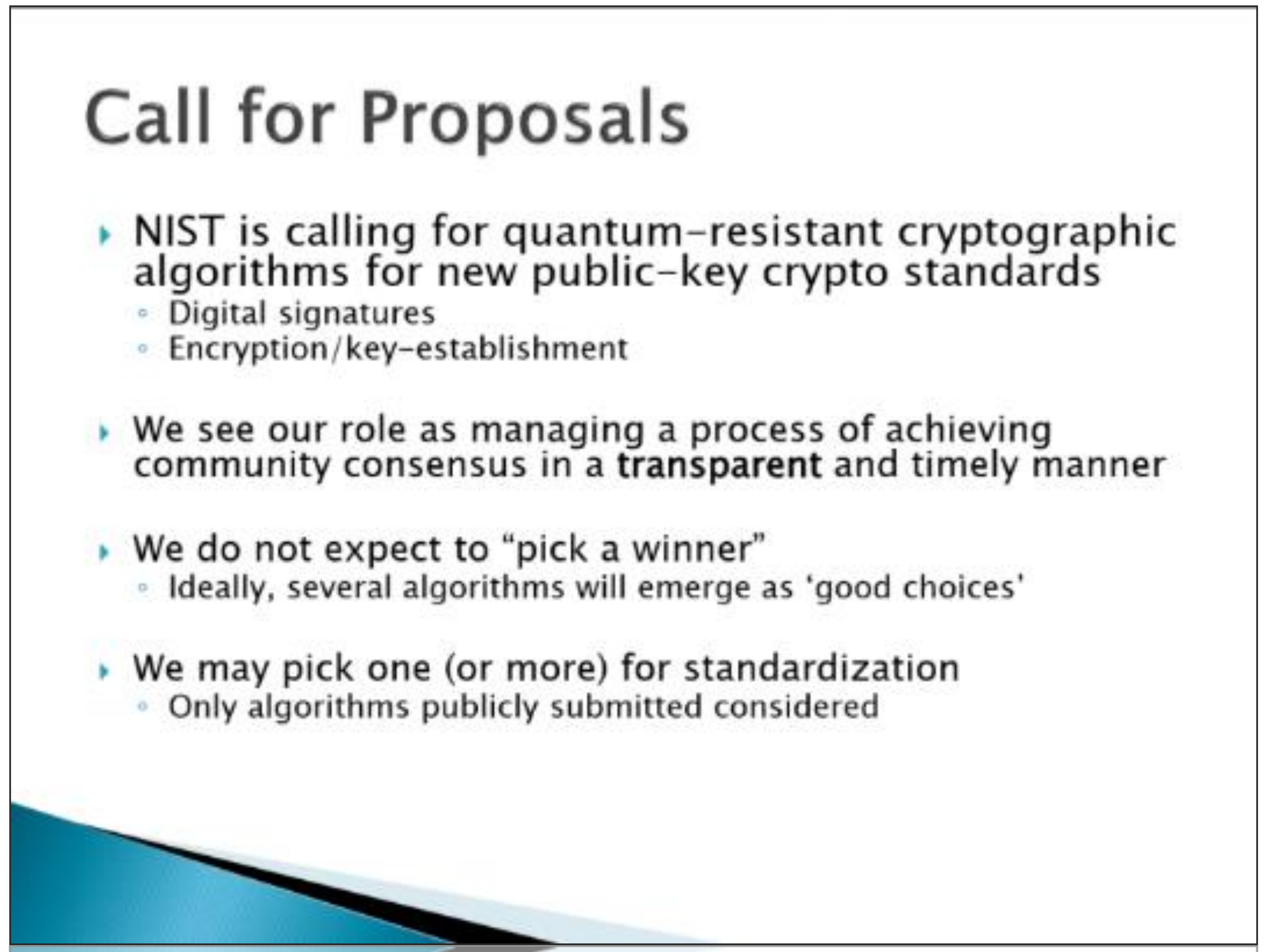
Defending Our Nation. Securing The Future.

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background



Call for Proposals

- NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards
  - Digital signatures
  - Encryption/key-establishment
- We see our role as managing a process of achieving community consensus in a **transparent** and timely manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'
- We may pick one (or more) for standardization
  - Only algorithms publicly submitted considered

« Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure »

"We announce preliminary plans for transitioning to quantum resistant algorithms **to provide security against a potential quantum computer"** - Aug. 2015

IDQ Recommended Path to Quantum Safety

Quantum Random Number Generation (QRNG)

- ✓ Instantly strengthen your network encryption key material
- ✓ Feed higher quality entropy into key generation servers, HSMs, Linux & crypto applications

State-of-the-art and Quantum-ready encryption

- ✓ Only go with AES-256 symmetric encryption and dedicated robust appliances
- ✓ Be **crypto-agile** & be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

Quantum Key Distribution (QKD)

- ✓ Quantum-Safe Network Encryption or **Quantum Cryptography**
- ✓ Provide forward secrecy and anti-eavesdropping of the encryption keys
- ✓ Ensure sovereignty and data ownership for the next decade (Post-Quantum era)

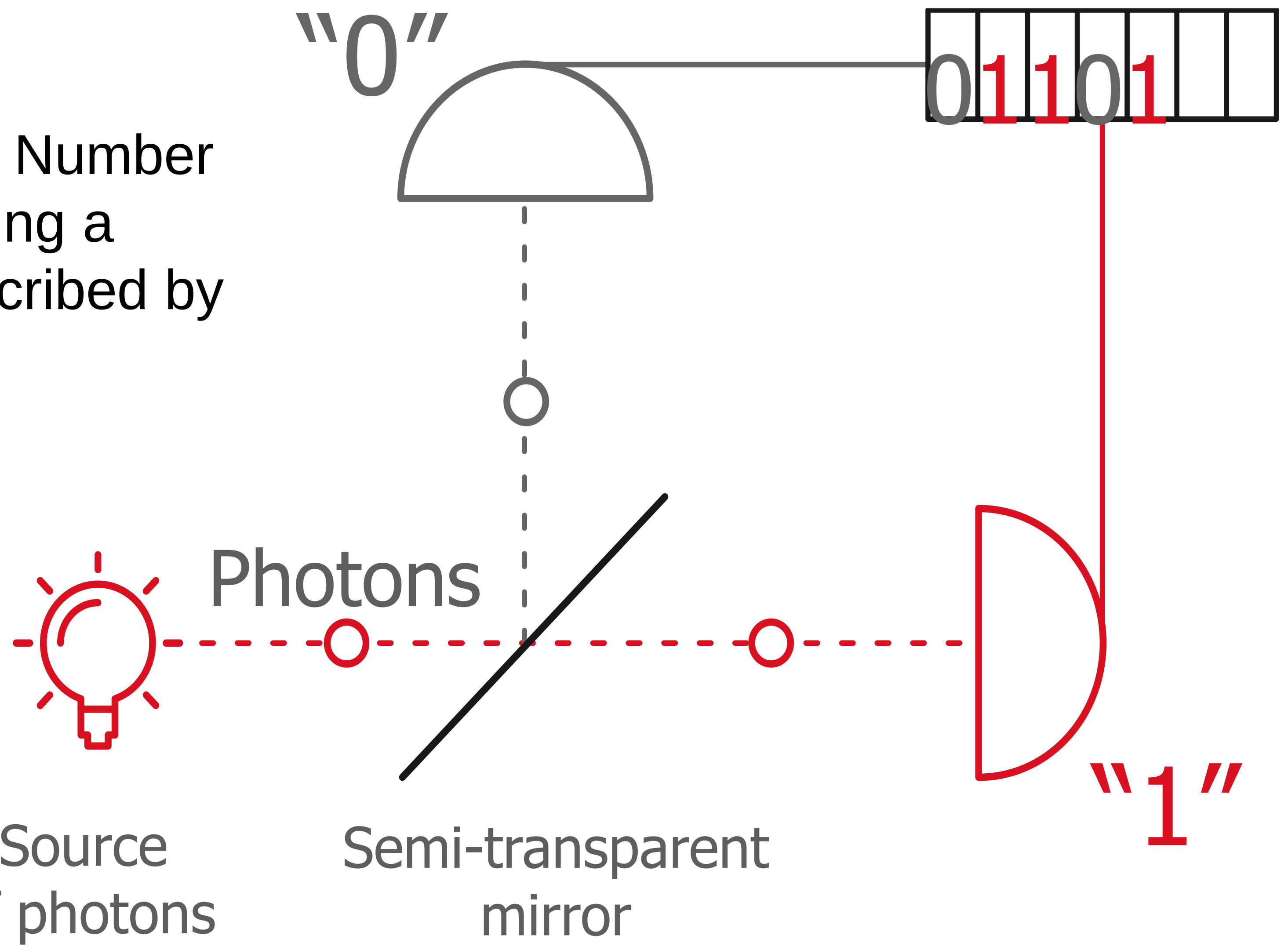
THE TOOLS (1):
QUANTUM KEY GENERATION

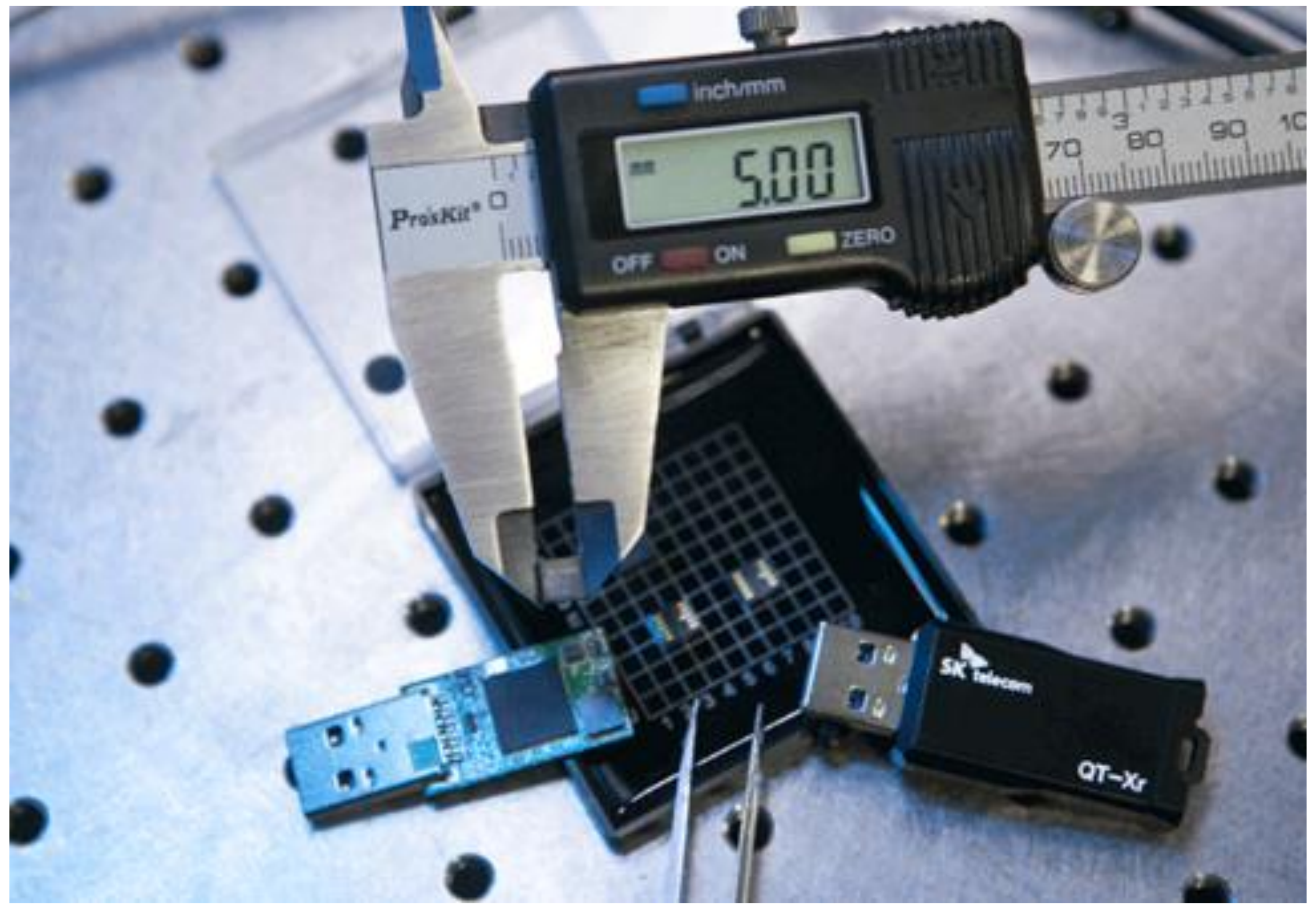
True Random Number Generator based on Quantum Physics

Advantages

- Speed
- Simple process that can be modelled influence of environment can be ruled out
- Live monitoring of elementary components possible to detect total failure
- Instant full entropy and provably random
- Compliance to various global standards
- NIST SP800-90A/B/C
- ISO/IEC-18031
- Performance: 1.5 Mbps (random bits per second)

Physical Random Number Generator exploiting a phenomenon described by quantum physics:





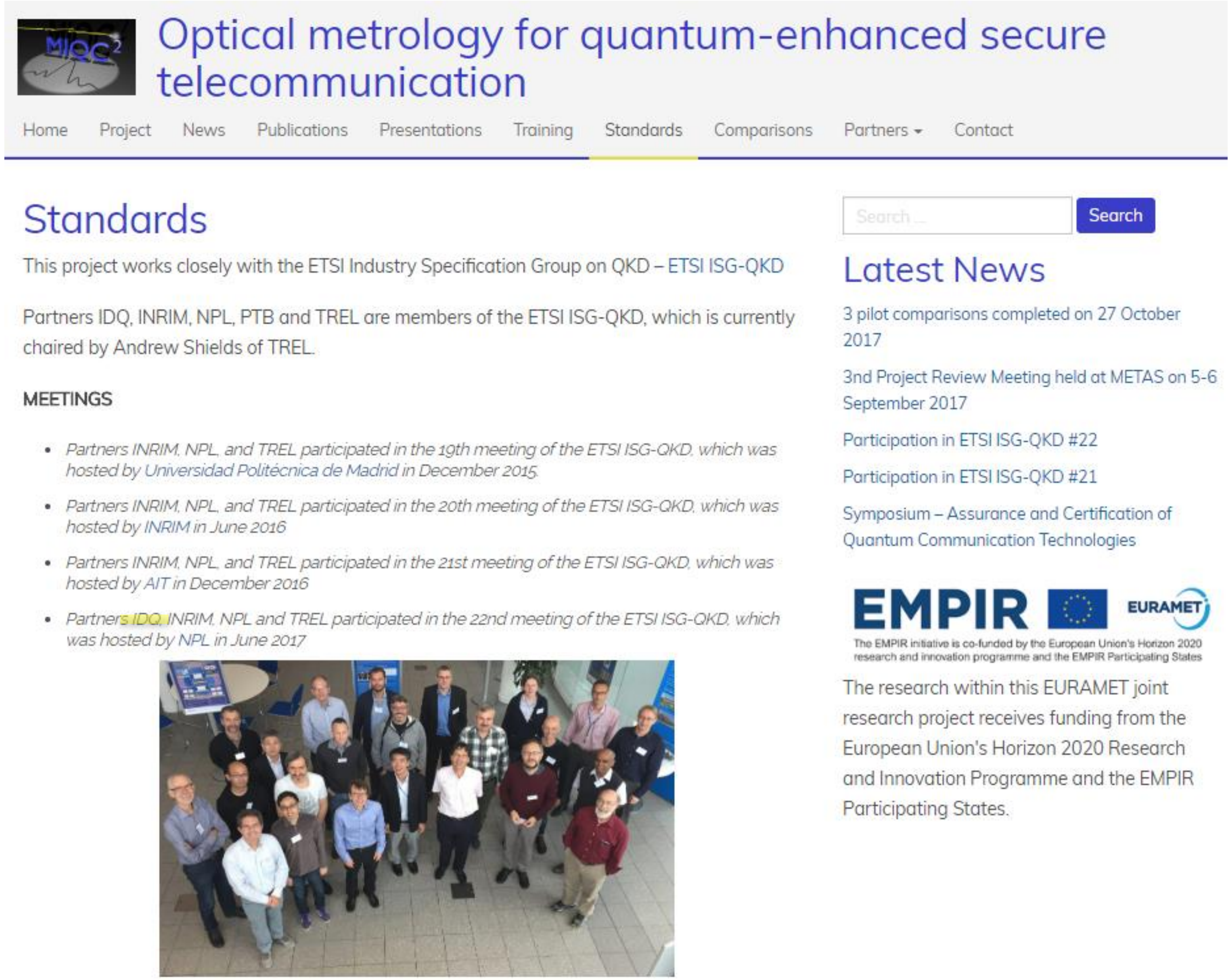
Now 5mm in size

Certifications for Random Number Generators

- Quantis is a highly trusted and tested RNG
  - Poor quality of randomness (= predictability) means poor security for the applications using the random bits

- Quantis Certifications:
  - NIST SP800-22 test suite compliance → NIST
  - Swiss METAS certification → Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
  - CTL Certification → CTL Compliance Testing Laboratory
  - iTech Labs Certificate → iTech Labs
  - BSI AIS31 compliance → Federal Office for Information Security; ANSSI

Standards: ETSI ISG - QKD



Optical metrology for quantum-enhanced secure telecommunication

Standards

This project works closely with the ETSI Industry Specification Group on QKD – ETSI ISG-QKD

Partners IDQ, INRIM, NPL, PTB and TREL are members of the ETSI ISG-QKD, which is currently chaired by Andrew Shields of TREL.

MEETINGS

- *Partners INRIM, NPL, and TREL participated in the 19th meeting of the ETSI ISG-QKD, which was hosted by Universidad Politécnica de Madrid in December 2015*
- *Partners INRIM, NPL, and TREL participated in the 20th meeting of the ETSI ISG-QKD, which was hosted by INRIM in June 2016*
- *Partners INRIM, NPL, and TREL participated in the 21st meeting of the ETSI ISG-QKD, which was hosted by AIT in December 2016*
- *Partners IDQ, INRIM, NPL and TREL participated in the 22nd meeting of the ETSI ISG-QKD, which was hosted by NPL in June 2017*

Latest News

3 pilot comparisons completed on 27 October 2017

3nd Project Review Meeting held at METAS on 5-6 September 2017

Participation in ETSI ISG-QKD #22

Participation in ETSI ISG-QKD #21

Symposium – Assurance and Certification of Quantum Communication Technologies

The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

The research within this EURAMET joint research project receives funding from the European Union's Horizon 2020 Research and Innovation Programme and the EMPIR Participating States.

Korea's SK Telecom and Deutsche Telekom have announced the formation of the Global Quantum Alliance at MWC 2017

THE TOOLS (2):

QUANTUM RESISTANT ALGORITHMS

Quantum-Resistant algorithms

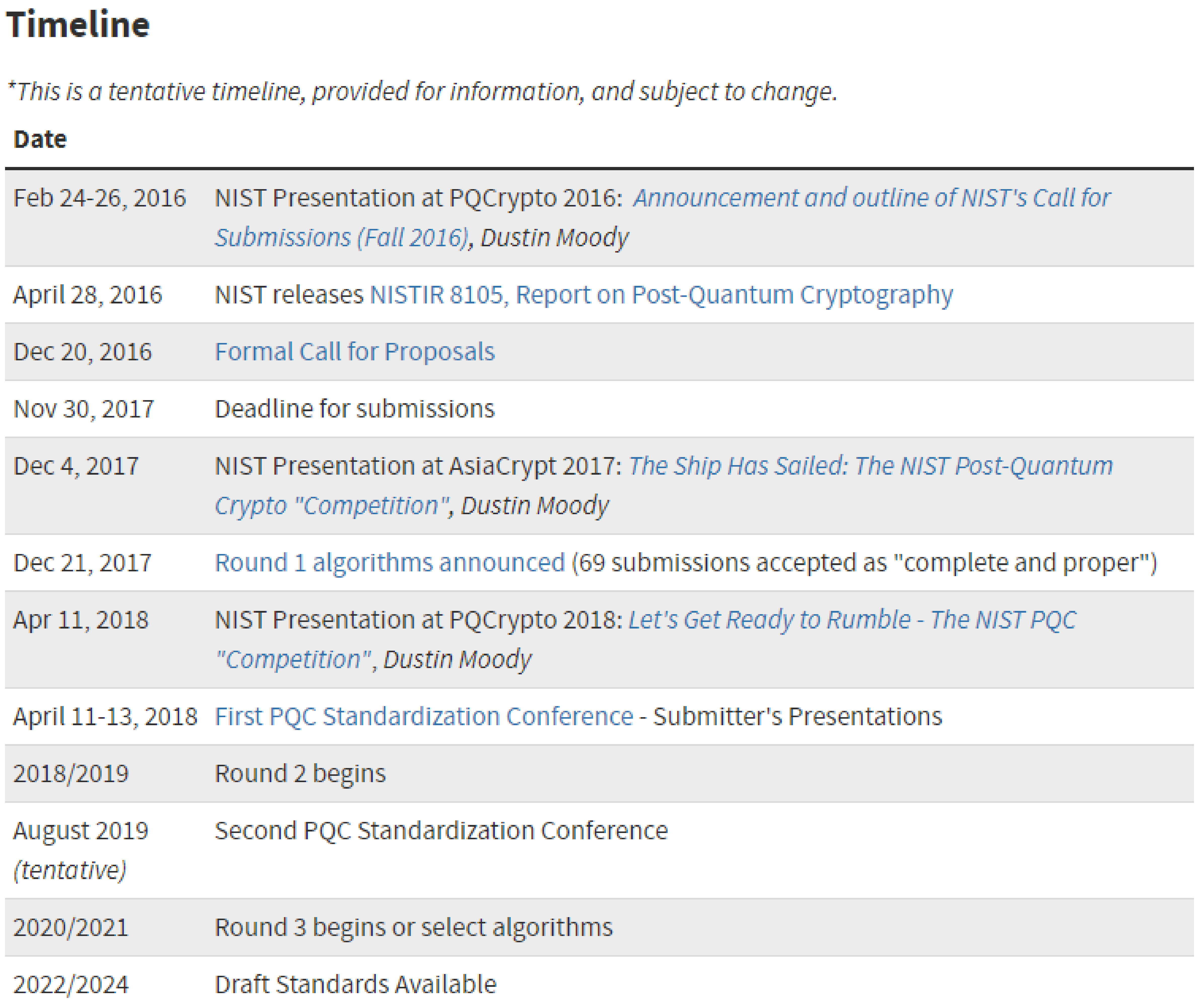
SWISS QUANTUM

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based (Mc Eliece)	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure
RSA	Public Key	Signatures, Key establishment	No Longer secure
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure

High level of confidence

Under investigation

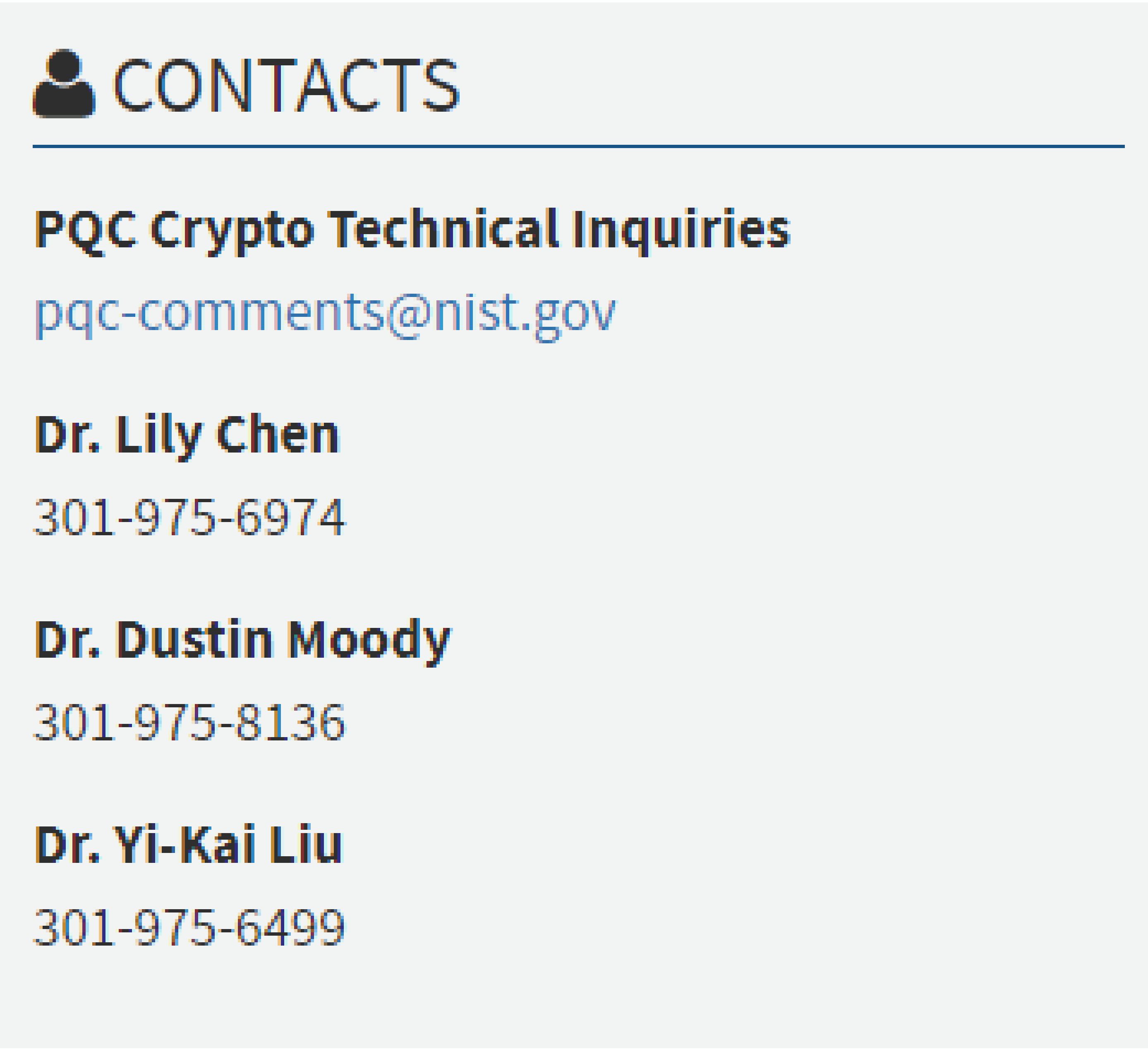
Timelines for NIST PQ Standards – Might be too slow!



Timeline

**This is a tentative timeline, provided for information, and subject to change.*

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016), Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition", Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition", Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
2018/2019	Round 2 begins
August 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available



CONTACTS

PQC Crypto Technical Inquiries
pqc-comments@nist.gov

Dr. Lily Chen
301-975-6974

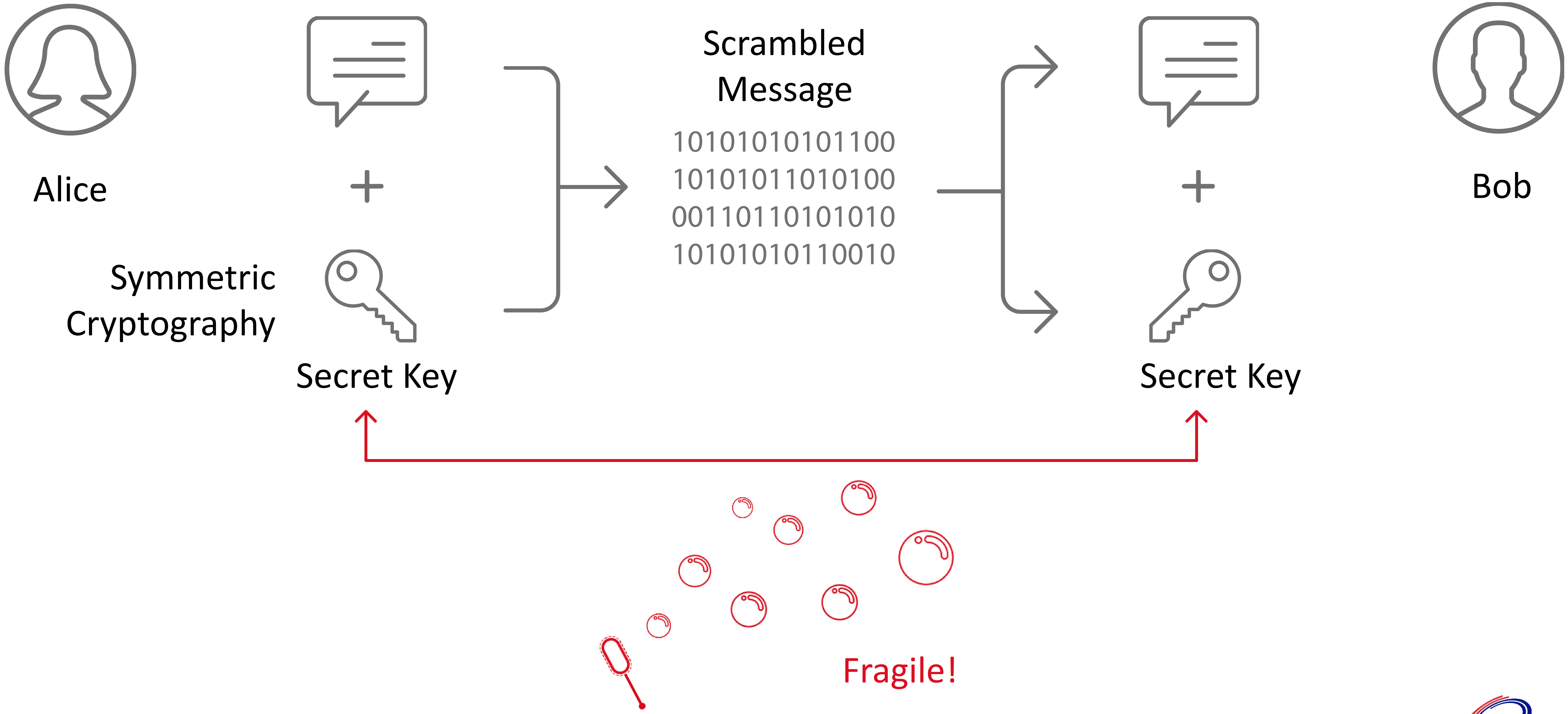
Dr. Dustin Moody
301-975-8136

Dr. Yi-Kai Liu
301-975-6499

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

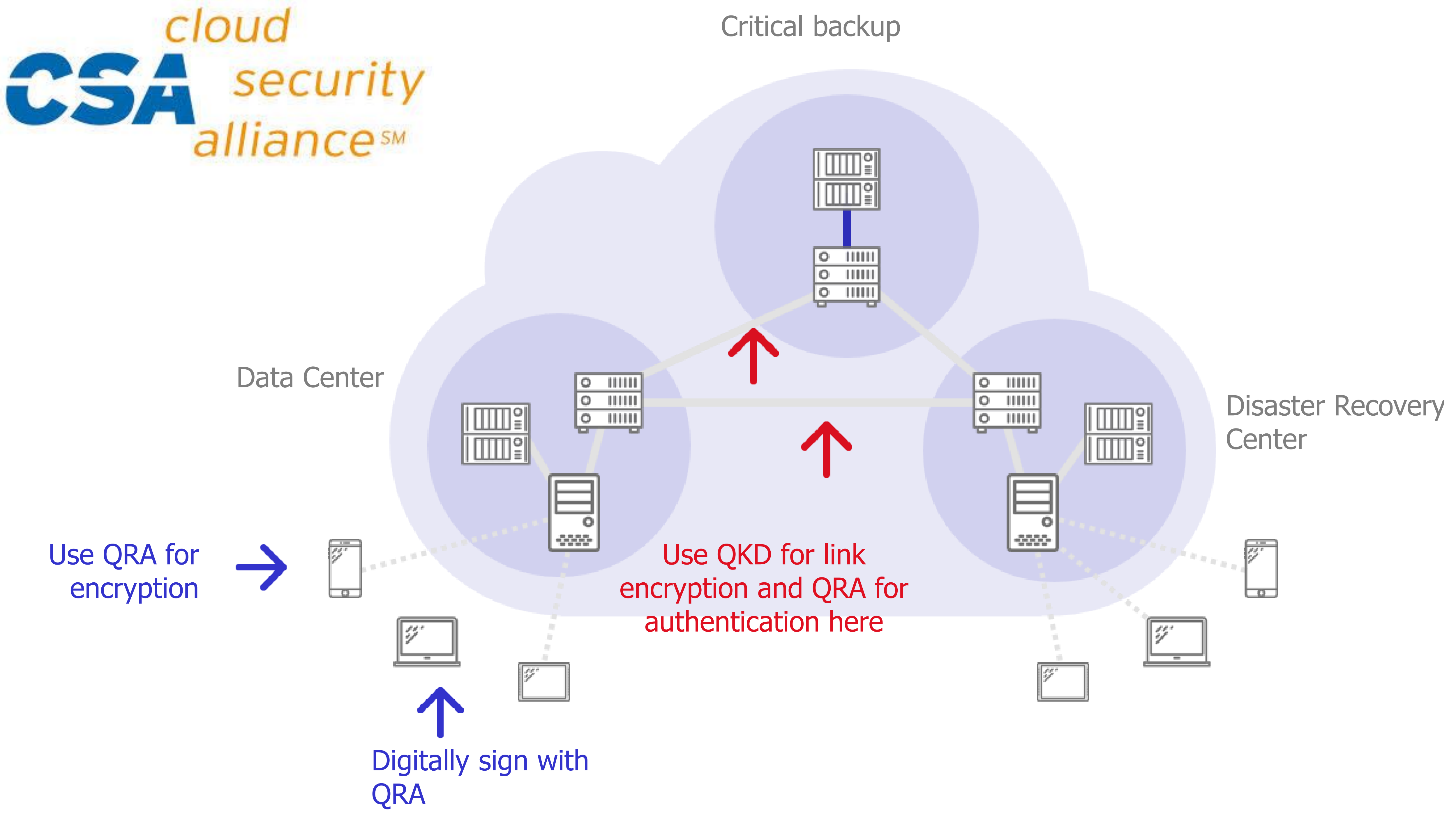
THE TOOLS (3):
QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD): Basic Idea



CSA Recommendations & EU's QT Flagship Agenda

cloud security alliance℠



Critical backup

Data Center

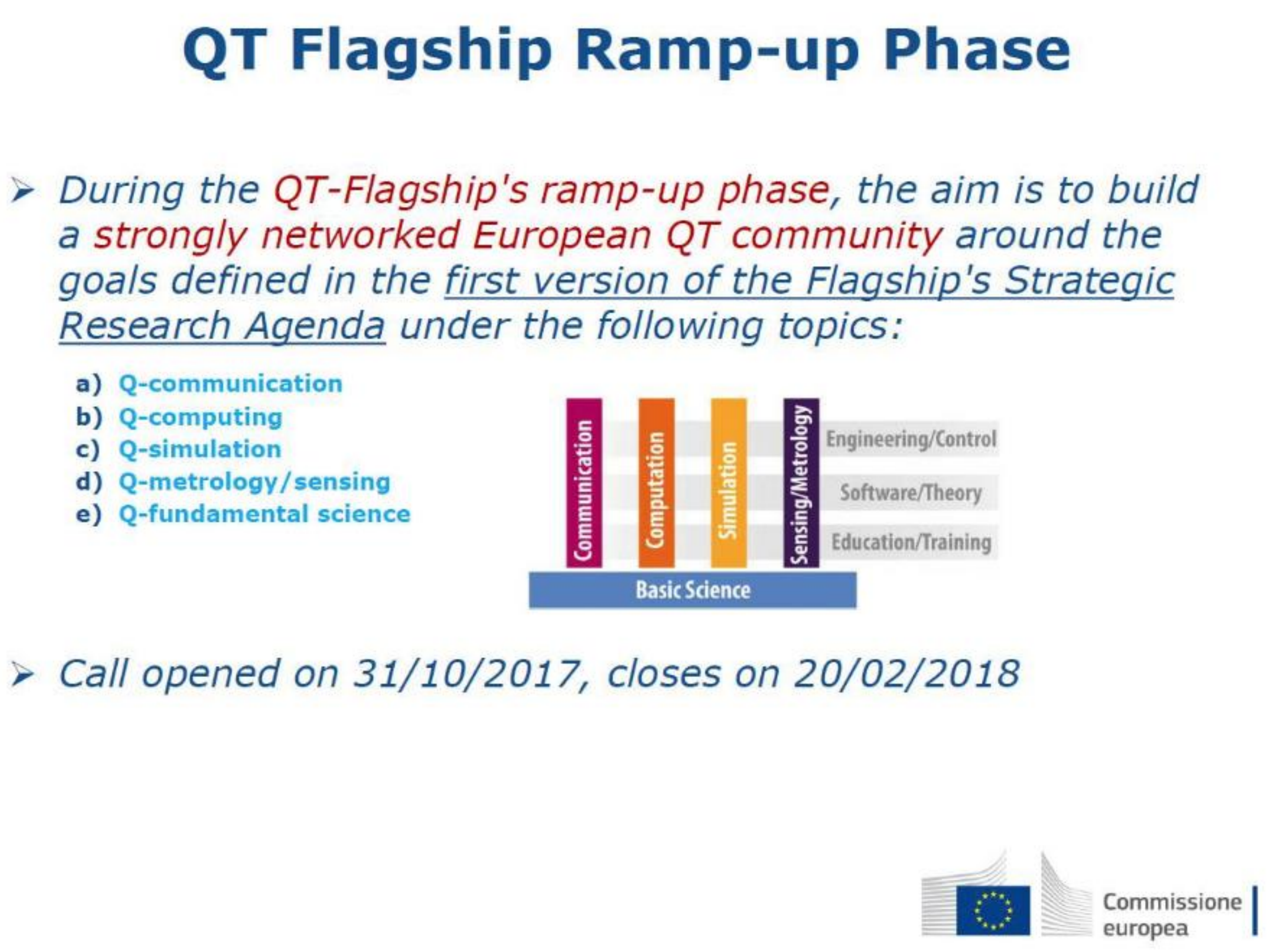
Disaster Recovery Center

Use QRA for encryption

Use QKD for link encryption and QRA for authentication here

Digitally sign with QRA

- The links between data centres and users are protected by **QRA** for encryption and signature
- **QKD** is used for specific and critical links, for example between data centers and DRC, and for all links where long term privacy is a requirement



QT Flagship Ramp-up Phase

- *During the QT-Flagship's ramp-up phase, the aim is to build a strongly networked European QT community around the goals defined in the first version of the Flagship's Strategic Research Agenda under the following topics:*

  a) Q-communication
  b) Q-computing
  c) Q-simulation
  d) Q-metrology/sensing
  e) Q-fundamental science

Communication
Computation
Simulation
Sensing/Metrology
Engineering/Control
Software/Theory
Education/Training
Basic Science

- *Call opened on 31/10/2017, closes on 20/02/2018*

Commissione europea

QKD USE CASES

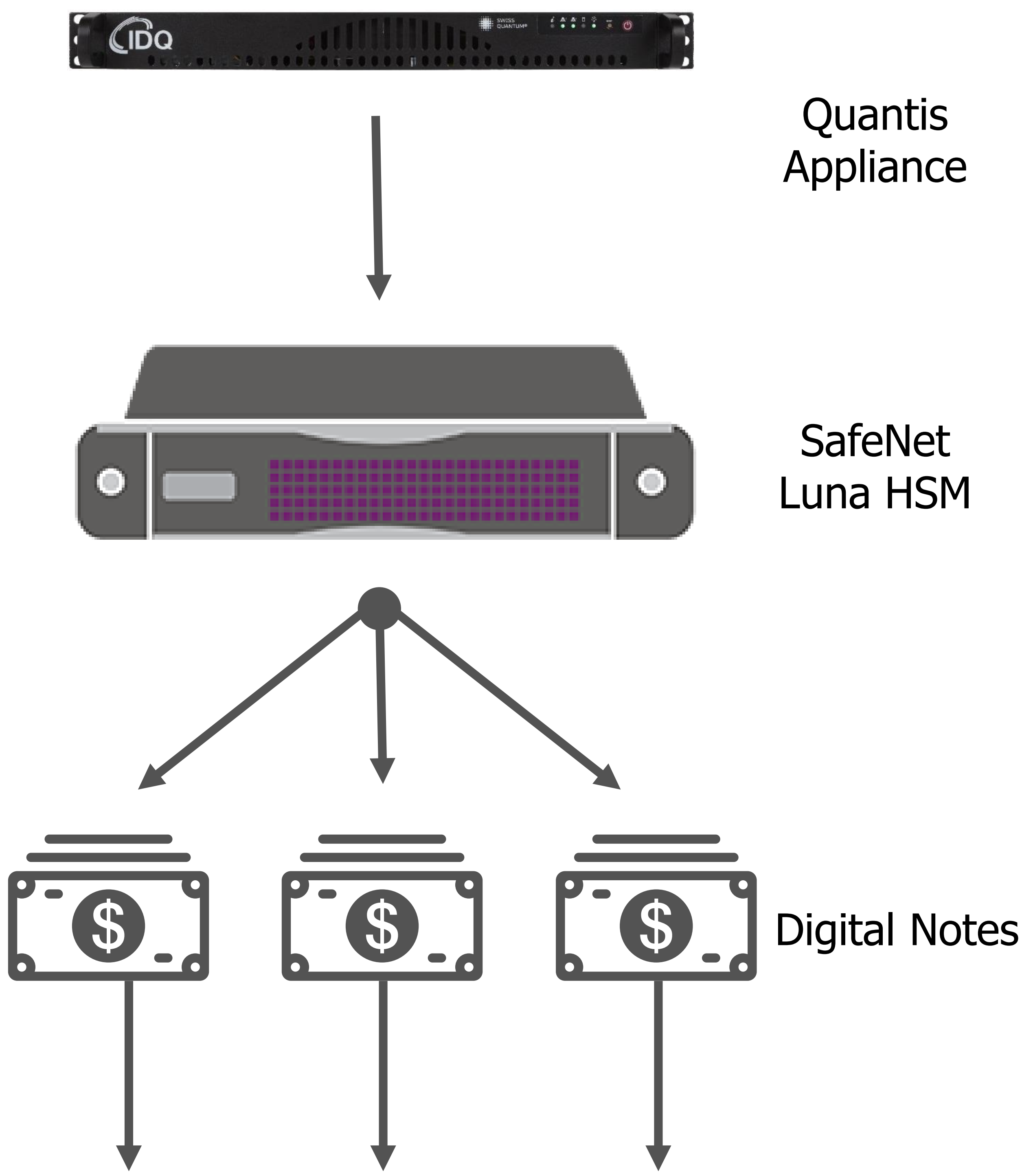
Digital Trust Platform

Digital money generation for central bank

- Business need
  - Development of digital fiat currency for central bank
    - Secure architecture design & implementation
    - Crypto customisation & agility

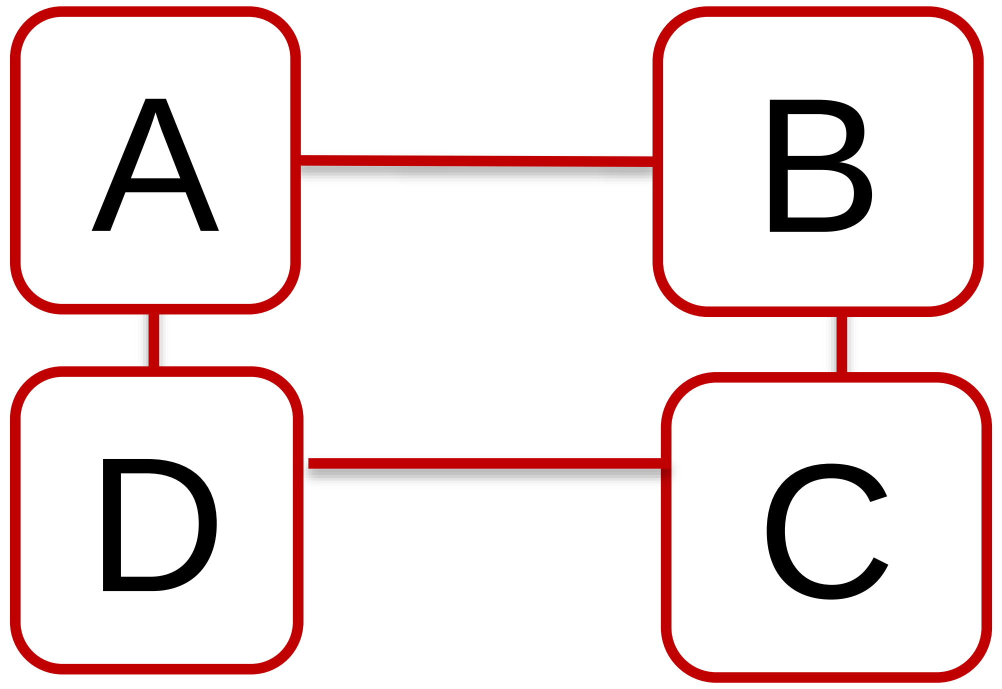
- Solution
  - Digital bank note generation platform producing authenticated validated digital tokens with assigned monetary value
  - Quantis QRNG appliance feeds entropy into SafeNet (Gemalto) hardware security module for higher security of token generation and authentication
  - Customised authentication based on bespoke (non NIST) elliptic curves (developed with Uni Trento & implemented on HSM)

- Benefit
  - Credibility of innovative solution based on Swiss trust and security



Q4 2018: National Bank Testbed for MAN

- 4 nodes Metro Area Network



- IDQ commercial Cerberis QKD Blade with Adva FSP 3000
  - Option 1: WDM for metro area network with 40 data channels (tested in 2016)
  - Option 2: 20 bidirectional data channels on one fibre & quantum keys on 2nd fibre (planned Q4 2017)
- Full scale implementation: Ring topology with full redundancy

Adva FSP 3000

Long Distance QKD with Trusted Nodes

SWISS QUANTUM

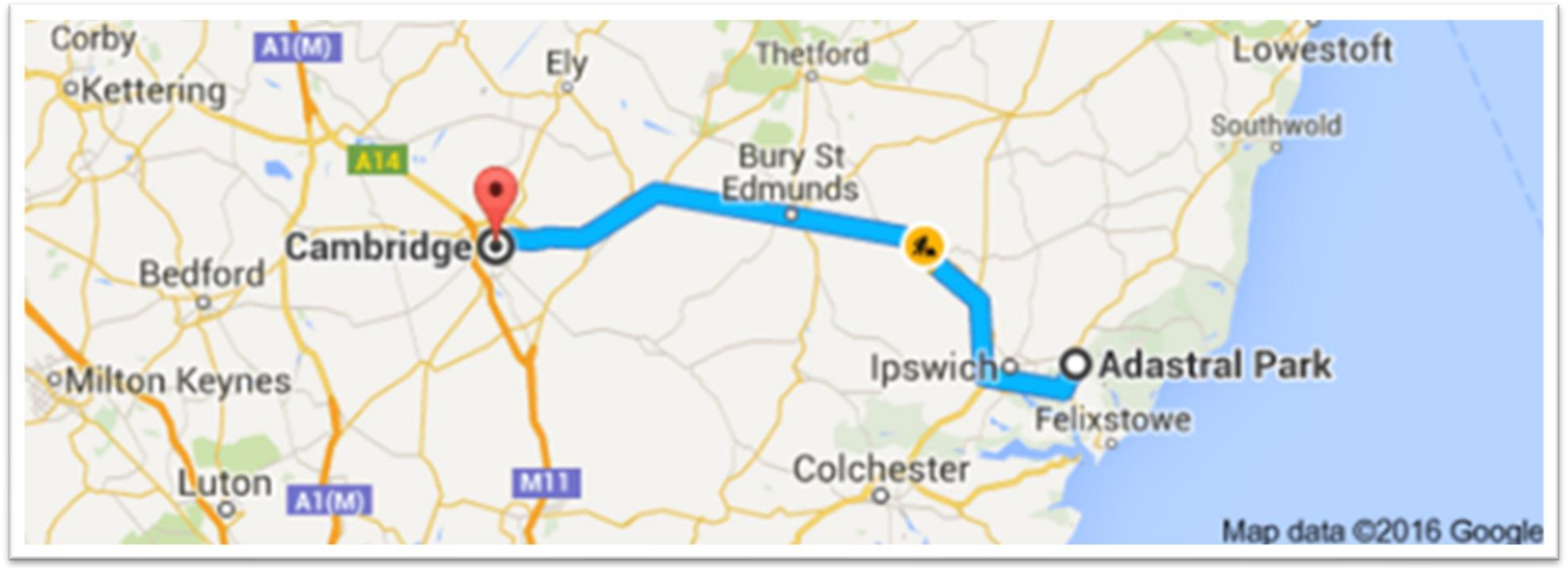
QUANTUM COMMUNICATIONS HUB

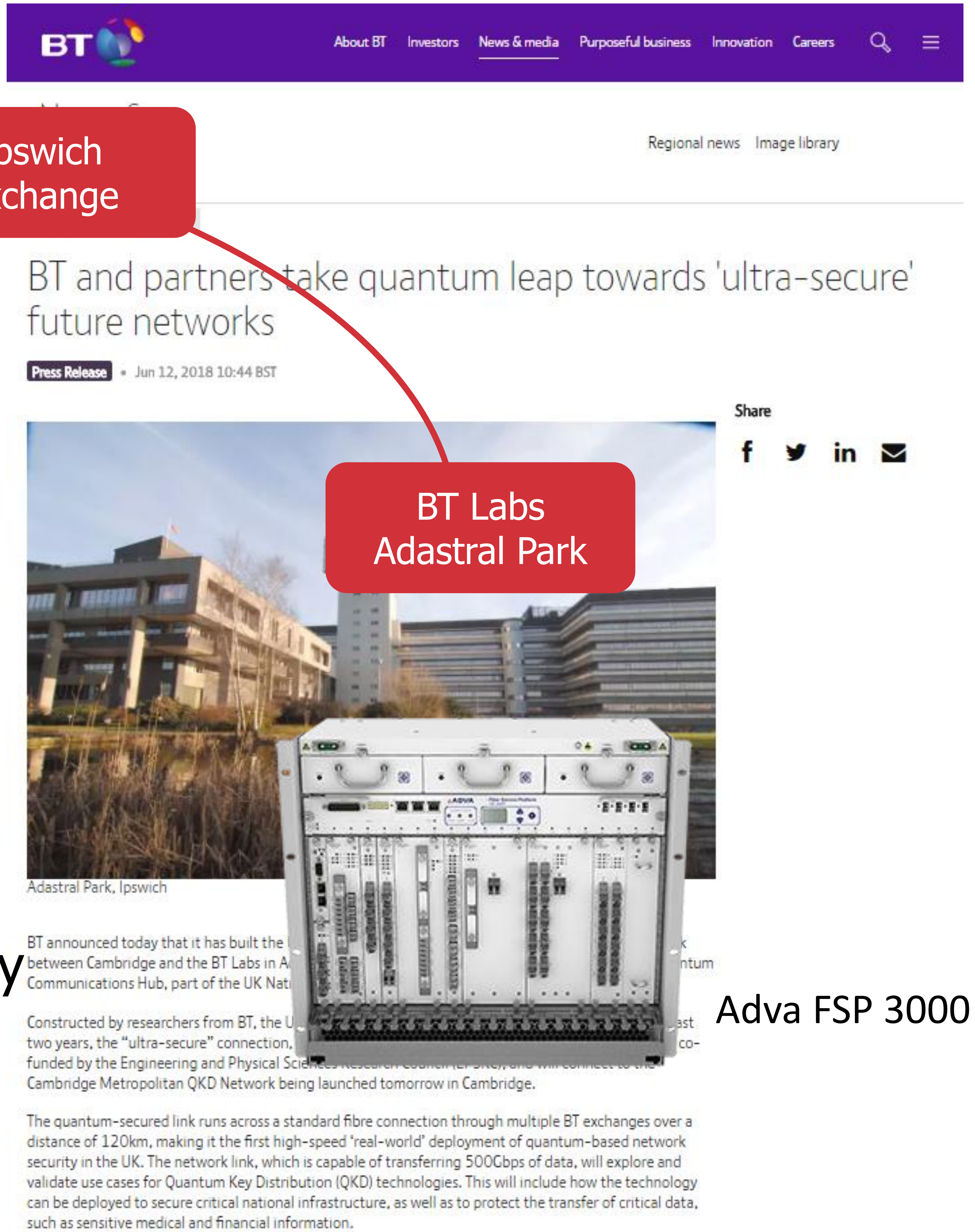
Cambridge University

Cambridge Exchange

Ipswich Exchange

BT Labs Adastral Park





BT and partners take quantum leap towards 'ultra-secure' future networks

Press Release • Jun 12, 2018 10:44 BST

Adastral Park, Ipswich

BT announced today that it has built the … k between Cambridge and the BT Labs in A… ntum Communications Hub, part of the UK Nat…

Constructed by researchers from BT, the U… ast two years, the "ultra-secure" connection, … co-funded by the Engineering and Physical Scie… Cambridge Metropolitan QKD Network being launched tomorrow in Cambridge.

The quantum-secured link runs across a standard fibre connection through multiple BT exchanges over a distance of 120km, making it the first high-speed 'real-world' deployment of quantum-based network security in the UK. The network link, which is capable of transferring 500Gbps of data, will explore and validate use cases for Quantum Key Distribution (QKD) technologies. This will include how the technology can be deployed to secure critical national infrastructure, as well as to protect the transfer of critical data, such as sensitive medical and financial information.

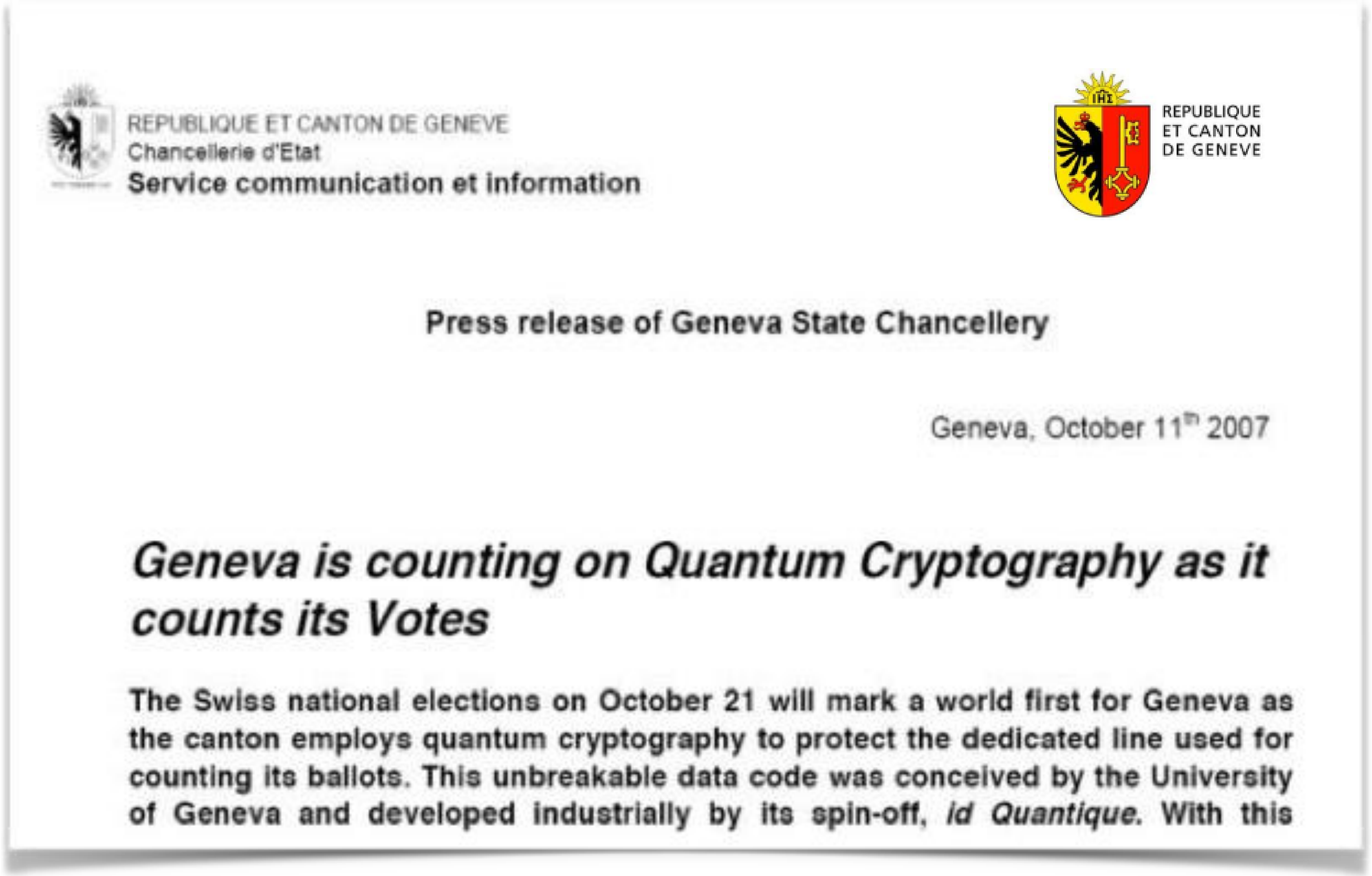
Adva FSP 3000

- Testbed between BT Labs at Adastral Park and Cambridge University

Example: First QKD Deployment

Practical QKD in Government & Public Administration

- In 2007 Geneva government installed QKD
- Confidentiality & integrity of data during federal & cantonal elections



REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Service communication et information

REPUBLIQUE
ET CANTON
DE GENEVE

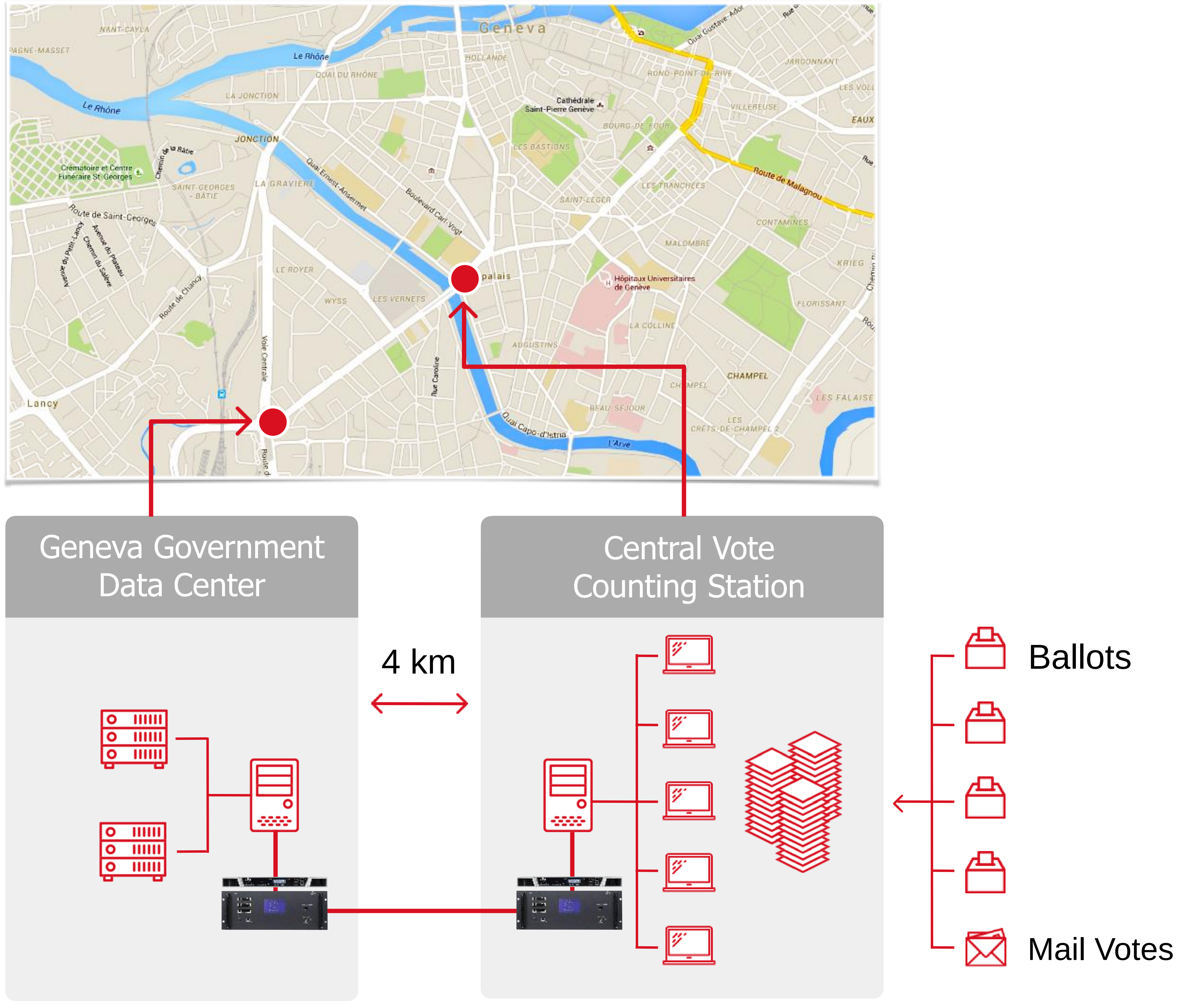
Press release of Geneva State Chancellery

Geneva, October 11th 2007

Geneva is counting on Quantum Cryptography as it counts its Votes

The Swiss national elections on October 21 will mark a world first for Geneva as the canton employs quantum cryptography to protect the dedicated line used for counting its ballots. This unbreakable data code was conceived by the University of Geneva and developed industrially by its spin-off, *id Quantique*. With this

Downtown Geneva



Cerberis QKD Solution

For more information
http://www.idquantique.com/
olivier.pfeiffer@idquantique.com