The QuSat project:
Towards commercial key distribution from space

Bruno Huttner & José Achache
ID Quantique & ALTYN

February 2017

Why QuSat? Why now?

- Threat of the Quantum Computer
- Need for **Quantum-Safe security**
- Re-tool all our cybersecurity infrastructure

- New tools:
  - **Quantum-Resistant Algorithms (QRAs)**
  - **Quantum Key Distribution**

Quantum-Safe = QRA + QKD

- QDK in space removes the distance limitation of ground QKD

PROPRIETARY

QuSat: Value proposition

- QKD is Quantum-Safe

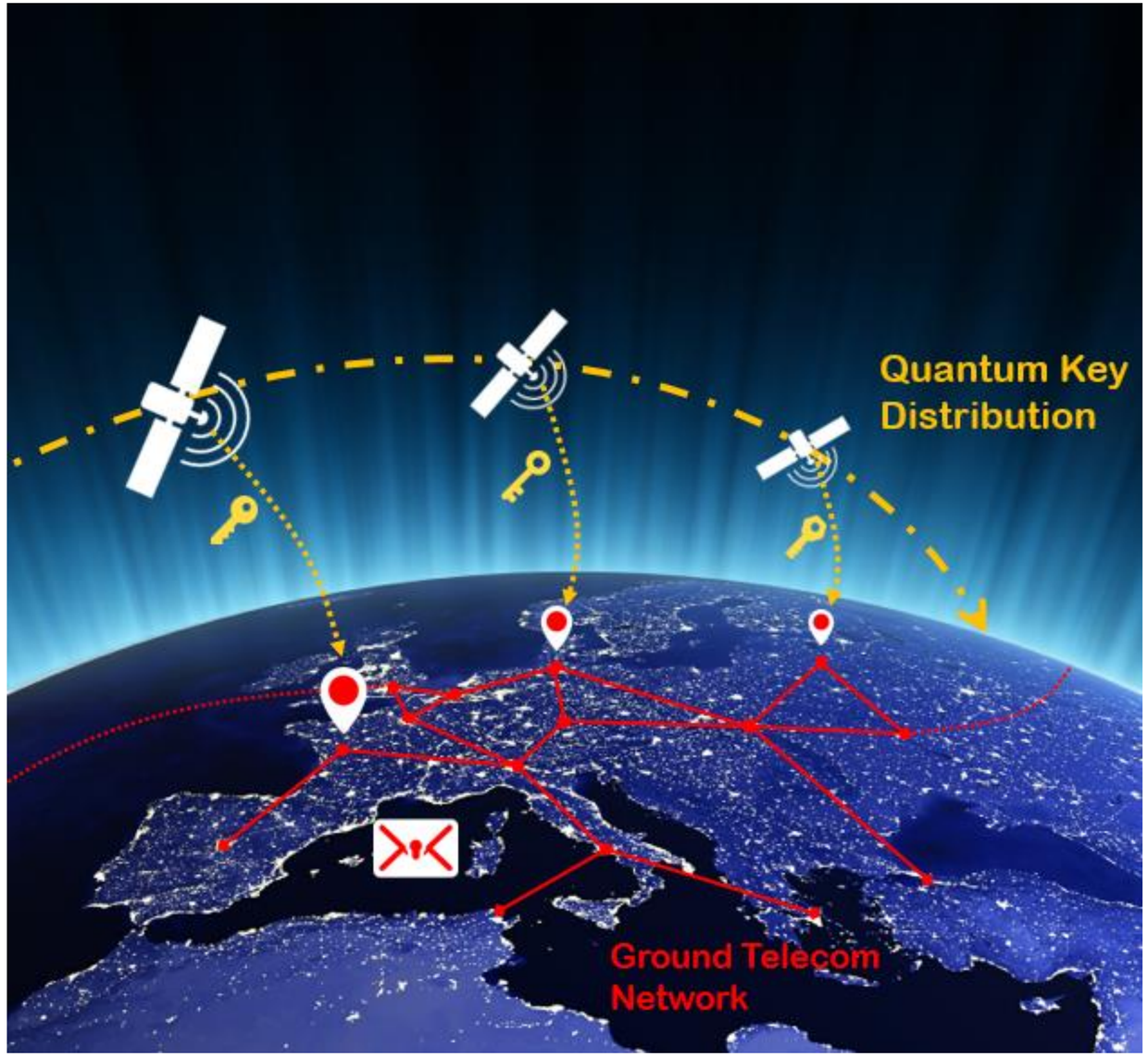
  But need quantum-safe signature (e.g. Hash-based schemes)

- QKD **adds** a layer of security (not exclusive!)

- Main advantage with respect to QRAs for key distribution
  - Real-time eavesdropping only
  - Long term security

PROPRIETARY

QuSat : Current Status



Partnership:

IDQ FROM VISION TO TECHNOLOGY & ALTYN

Funded by Swiss Space Office (SSO)

- Phase 0 (preliminary): done
- Phase A (feasibility): starting March 2017
- Phase A study will last 12 months

PROPRIETARY

QuSat: program for phase A

- Technical feasibility

- Market analysis

PROPRIETARY

QuSat driving ideas

- Low cost

- Keep the space segment simple

- Low cost User Terminals

PROPRIETARY

QuSat: the team

- Management:
  - Project manager: ALTYN
  - Quantum payload manager: ID Quantique

- Team
  - 8 to 10-person team…

- Partners
  - TBD…

PROPRIETARY

QuSat: Initial requirements

SWISS QUANTUM

Laser Communication Terminal

- Weight: < 30 kg
- Power consumption: < 60 W
- Data rate: 1 Gbit/s
- Link length: 1’000 km
- Diameter of the telescope: 10 -15 cm
- Pointing accuracy: 10-20 μrad

Ground User Terminals:

- Diameter of the telescope: 20- 50 cm
- Pointing accuracy: 10-20 μrad
- Single user or optical hub
- Low cost per user

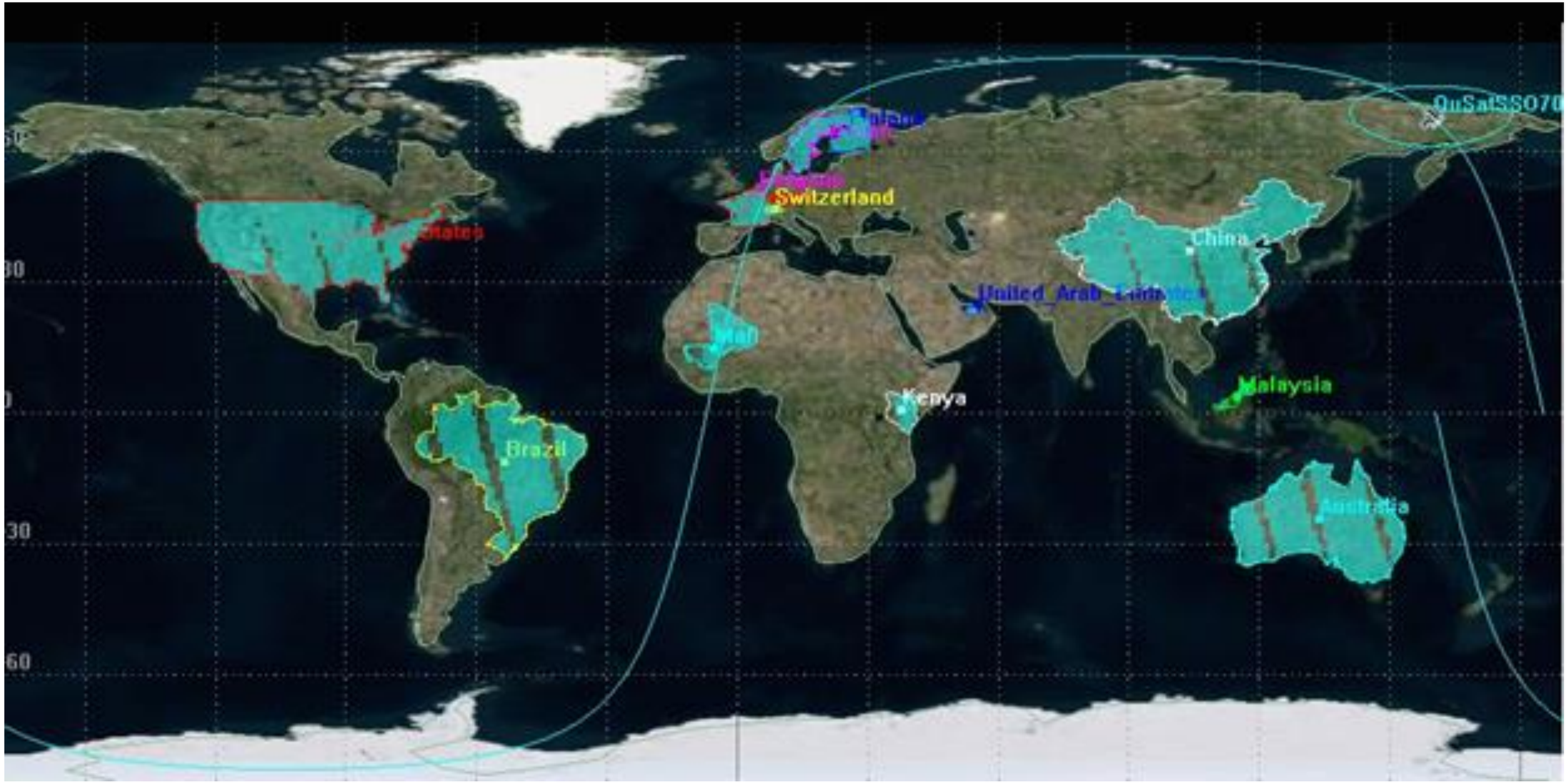
Spacecraft:

- Overall mass: 150 kg
- Power 160 W

PROPRIETARY

IDQ ALTYN

Simulation of QuSat coverage over selected countries



PROPRIETARY

Conclusion

- QKD can add a layer of security different from QRAs
- Satellite QKD solves one of the big issues of QKD: distance
- Work still needed to convince the cyber security community…

Contacts: bruno.huttner@idquantique.com
jose.achache@altyn.ch

PROPRIETARY