SAGA 1G - preparing for EuroQCI

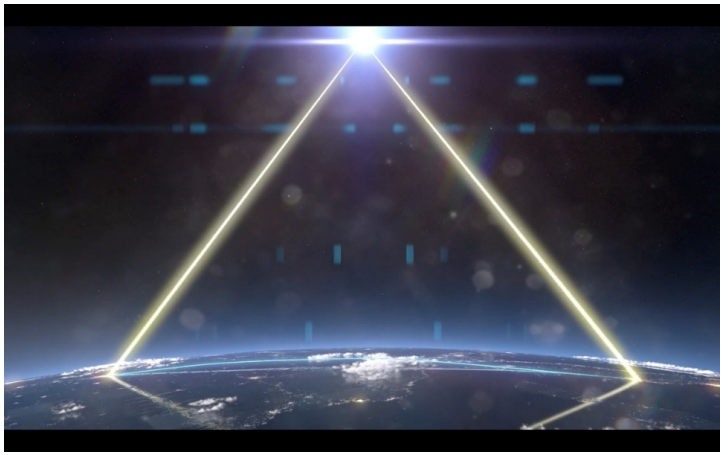
LASER World of Photonics - Quantum Communication - 29.06.2023

N. Lindman – SAGA Implementation Manager

SAGA 1G – Context

ESA's **S**ecurity **A**nd crypto**GrA**phic Mission - SAGA

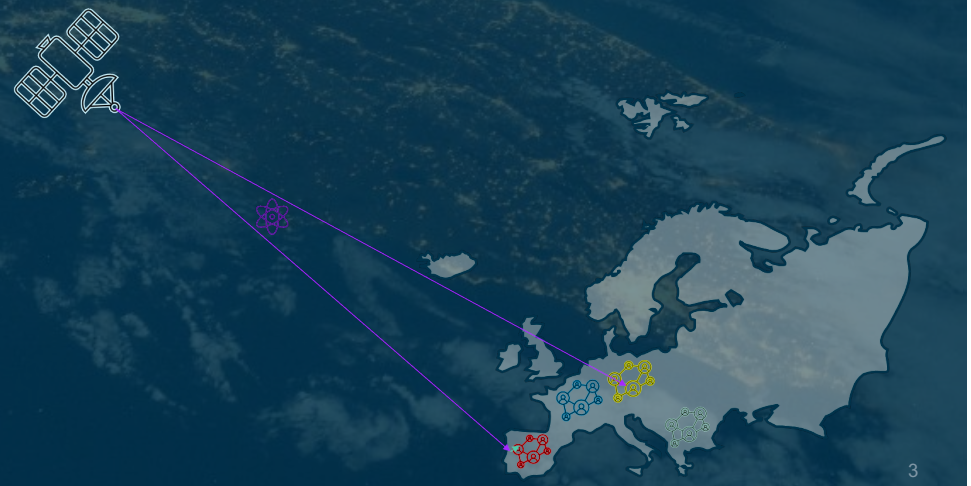
- SAGA (created 2019) is the ESA project and **space element of EuroQCI**, part of the EC Secure Connectivity initiative.
- SAGA will design, develop & validate the EuroQCI space segment and shall provide global Quantum Key Distribution **classified services** for European Users (**governments**).
- SAGA 1st Generation system, based on LEO implementation providing **Prepare and Measure** QKD (unclassified services);
- Future generation system, targeting the implementation of a **full operational** service based on a mixture of QKD protocols and orbits.



SAGA 1G Scope

Applicable requirement documents:

- EuroQCI User Requirements Document – EC document
- EuroQCI Concept of Operations – EC document
- SAGA 1G EC-ESA Working Assumptions – EC-ESA joint document
- SAGA Program Security Instructions (PSI) – ESA document



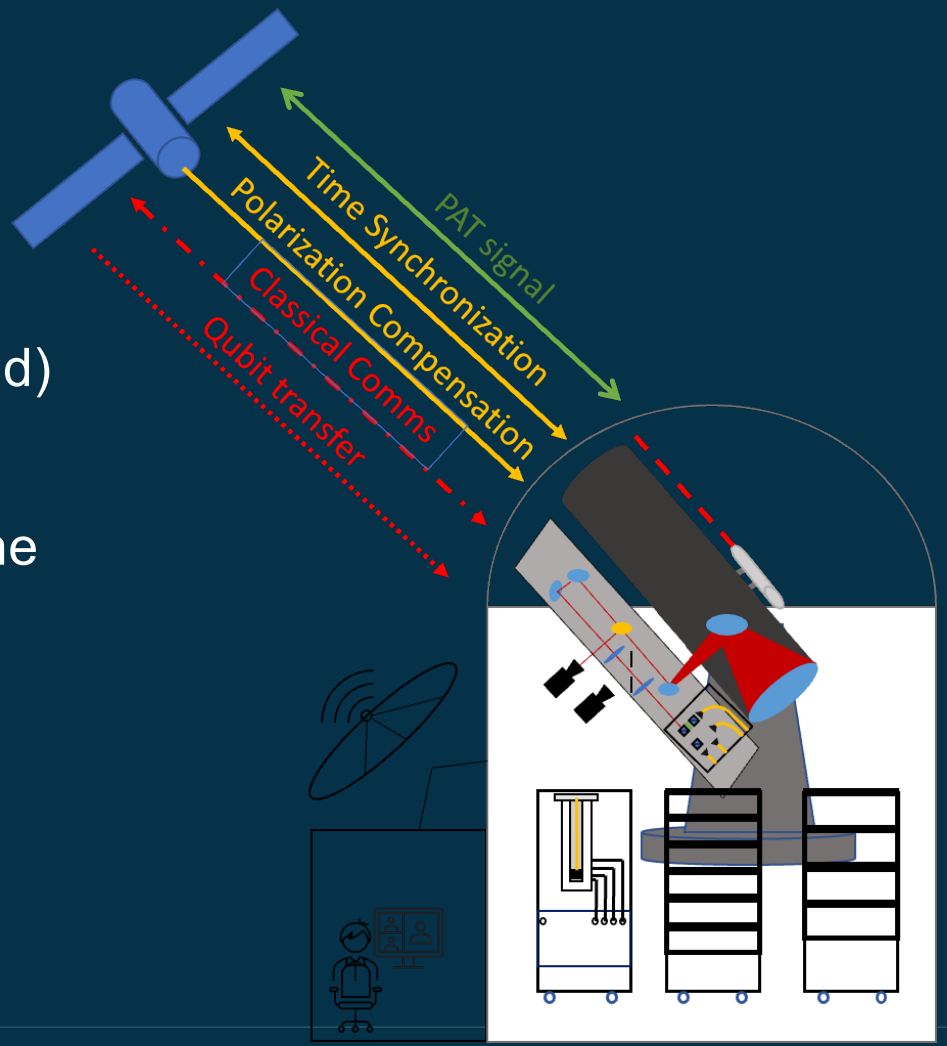
SAGA 1G Objectives

Readiness **for EuroQCI QKD service** developments:

- Definition of the EuroQCI QKD protocol
- Prepare for QKD security proof
- QKD technology maturation
- Prepare for QKD components security certification
  - Component identification
  - Protection profiles
- Perform in-orbit validation
  - QKD performance profiling
  - System verification (pen-test) and qualification
  - Service validation
- European supply chain readiness

QKD Protocol Definition – Basic Properties

- Discrete-variable P&M type protocol
- C-Band for the QKD downlink (1550nm band)
- Polarization encoded quantum states
- Optical links for the classical channel and the time synchronization channel



QKD Protocol Definition – detailed parameters

An (incomplete) list of parameters is:

Wavelengths, spectral widths, pulse frequencies, pulse properties of the specific QKD protocol, QKD pulse indistinguishability, jitter requirements, polarization requirements (incl. tracking), transmission patterns (frames, sifting blocks, etc…)

Authentication, sifting block sizes, error correction codes, confirmation hash functions, error estimations, privacy amplification hashing (incl. seed exchange), epsilon security parameter, link interruption routines

Exchange of meta data, classical data protocol parameters for data transfer, classical crypto for securing the classical channel

The final version will have >100 different parameters

QKD Protocol Definition - Security

Security assessments of the protocol to protect the confidentiality, integrity and availability of the SAGA service with special emphasis on:

- Preventing the exploitation of side channels
- Preventing “quantum hacking” attacks
- Preventing classical cybersecurity threats on the classical channels
- Assuring that the QKD protocol is executed within the parameters assumed by the QKD security proof

The current QKD protocol definition IRD is ESA RESTRICTED, parts of the content may have different classification levels in future iterations.

QKD Protocol Definition - Challenges

The intrinsic properties of QKD lead to the following challenges:

- Highly interconnected relations between (nearly) all channels and their properties: changing one parameter may have an influence on many others
- Strong relationships between performance, security and specific design implementations: QKD is a hardware based system, impossible to define the protocol without taking many design decisions
- No clear line between protocol and implementation leads to conservative classification.

Development in close coordination with EC and the NSAs to prepare for certification.

SAGA project status

- SAGA Phase A (feasibility) 3 parallel contracts completed July 2022
- SAGA Phase B1 (requirements definition) 2 parallel contracts kicked-off in January 2023 with ADS and OHB
  - Delta PRRs – closed out beg April 2023
  - SRRs – September 2023
- SAGA QKD Technology Preparation (up to PDR) to be added to the scope of the Phase B1s:
  - QKD technology maturation is on the critical path
  - To ensure project continuity

Outlook

- Start the SAGA Technology Preparation activities as extensions to the on-going Phase B1 (System Definition) activities.
- Consolidate the funding approach together with EC and ESA Participating States.
- Prepare and start SAGA 1G implementation contract(s) (B2/C/D/E1) by mid 2024.