Key Management System for a QKD network

Supervisor: Armando Pinto (anp@ua.pt)
Collaborator: Diogo Matos (dftm@ua.pt)
Keywords: Quantum technologies, Key management system
Number of team elements: 4 to 6

Context:
Quantum Key Distribution (QKD) enables the negotiation of cryptographic keys in a secure manner without relying on computational complexity to achieve its security. In QKD Network (QKDN), keys are first generated by the physical layer, then are managed by a Key Management System (KMS) that, ultimately, will provide key material to secure applications. For such a system to correctly operate, a KMS and other components attached to it need to be employed in order to correctly retrieve, synchronize, store, manage and distribute quantum symmetric and oblivious keys in a secure and efficient manner.

Proposed objectives:

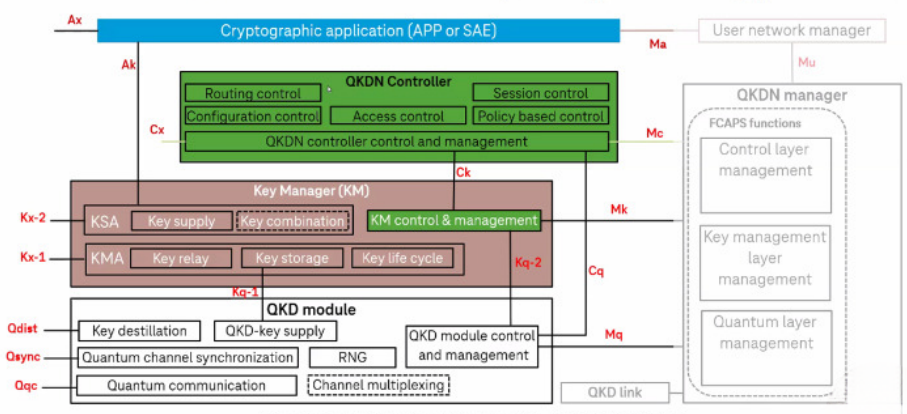

Fig 1 - QKDN interfaces defined in ITU-T Y.3802

This proposal aims at contributing actively to the development of a quantum key management system. The system will follow international and EU standards specified by institutions such as ETSI[1] and ITU-T[2]. The work done in this project will complement the work that is being done by IT in the scope of the Discretion[3] and PTQCI[4] projects.

[1] https://www.etsi.org/
[2] https://www.itu.int/
[3] https://discretion-eu.com/
[4] https://ptqci.av.it.pt/

We expect the group to work on these major topics:

- Study the main standards, directives and work done previously on the topic of QKDNs and quantum/classical KMSs
- Develop an integral part of a quantum key management system;
- Integrate and validate the developed solution into a QKDN;

Milestones / Months[5]

- Very basic KMS (ITU-T Y.3803 / DISCRETION-D3.1) - beg. December
- Interface to the applications (ETSI QKD GS 004/14) - end February
- Interface to the Quantum Layer (ETSI QKD GS 004) - end March
- KMS 1.0 (all vital functionalities) - end April
- KMS 2.0 - end May
- Final report - June

[5] To be further described to the selected group. Months subject to change in order to better suit UC'S calendar.