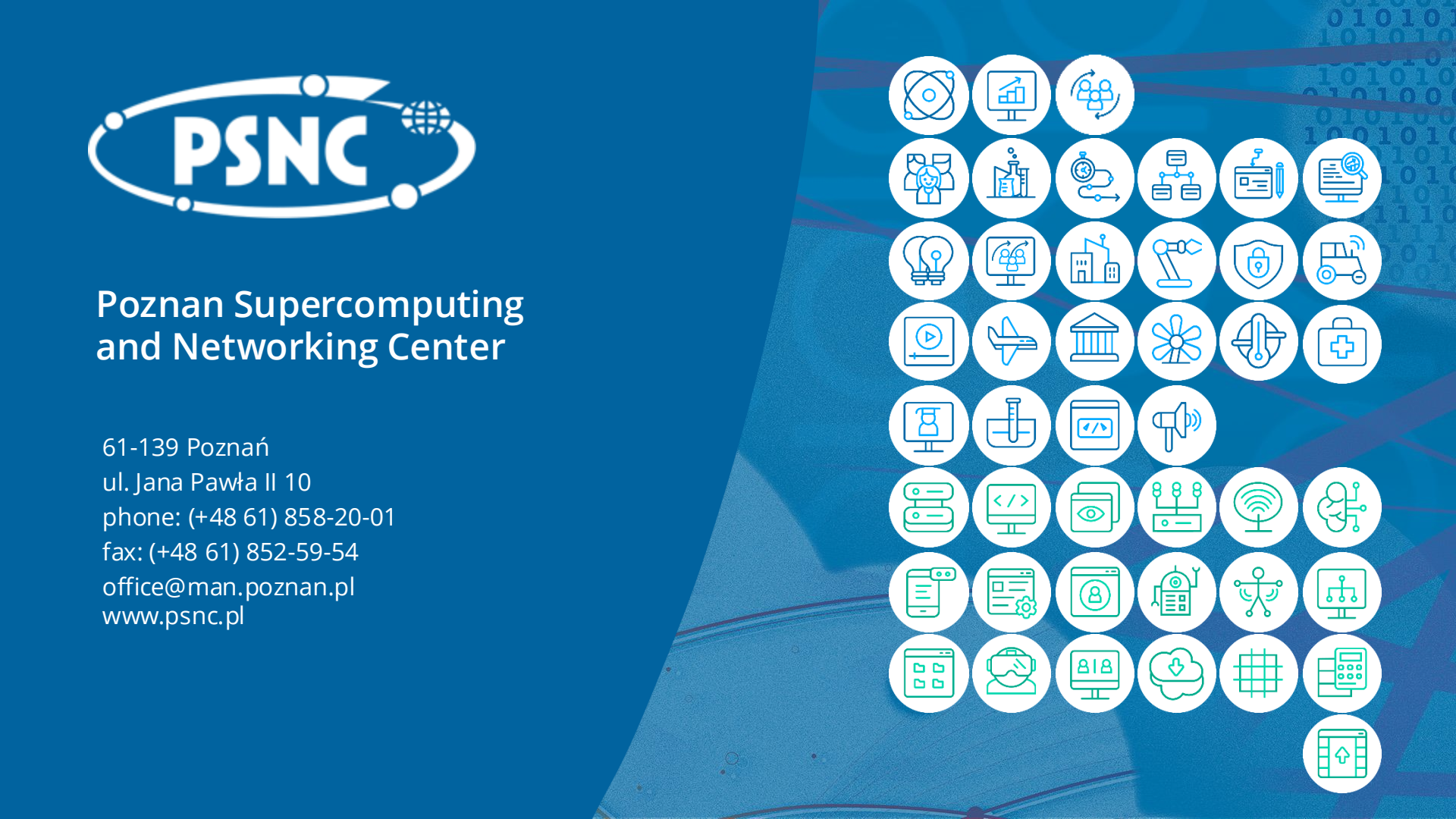


Poznan Supercomputing and Networking Center

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl

Piotr Rydlichowski

Key Management System for Quantum Key Distribution Network - concepts and integration with network services

QKD and KMS

- Quantum Key Distribution (QKD) protocols and infrastructure allows for implementation of the point-to-point links to exchange random numbers (keys) over quantum communication links which are also Information-Theoretically-Secure

- Key Management System (KMS) is a crucial element that allows to build larger, scalable Quantum Key Distribution Networks

- KMS is also interface for QKD infrastructure to other network services and infrastructures

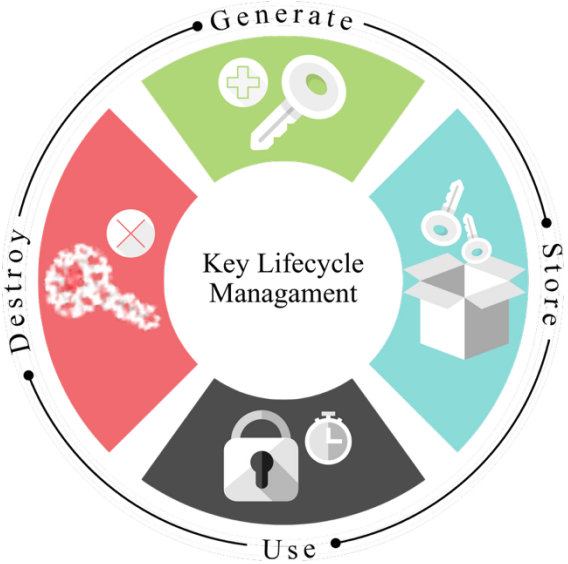
- Quantum Key Distribution Networks can be viewed as potential separate layer in existing communication network

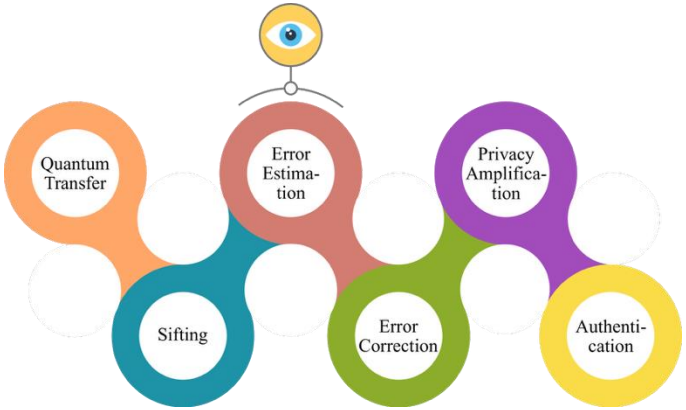
KMS

KMS system has several crucial functionalities:

- Retrieving the QKD keys from different QKD devices
- Provides the keys to applications
- Stores keys
- Need to be reliable on operational environment – high availability and backup services
- Implements optionally SDN interfaces and principles
- For interoperability purposes needs to be compliant with different standards and draft standards for interfaces and architecture
- Allows to build logical topologies of QKD networks and services
- Can be integrated with PKI and HSM infrastructure

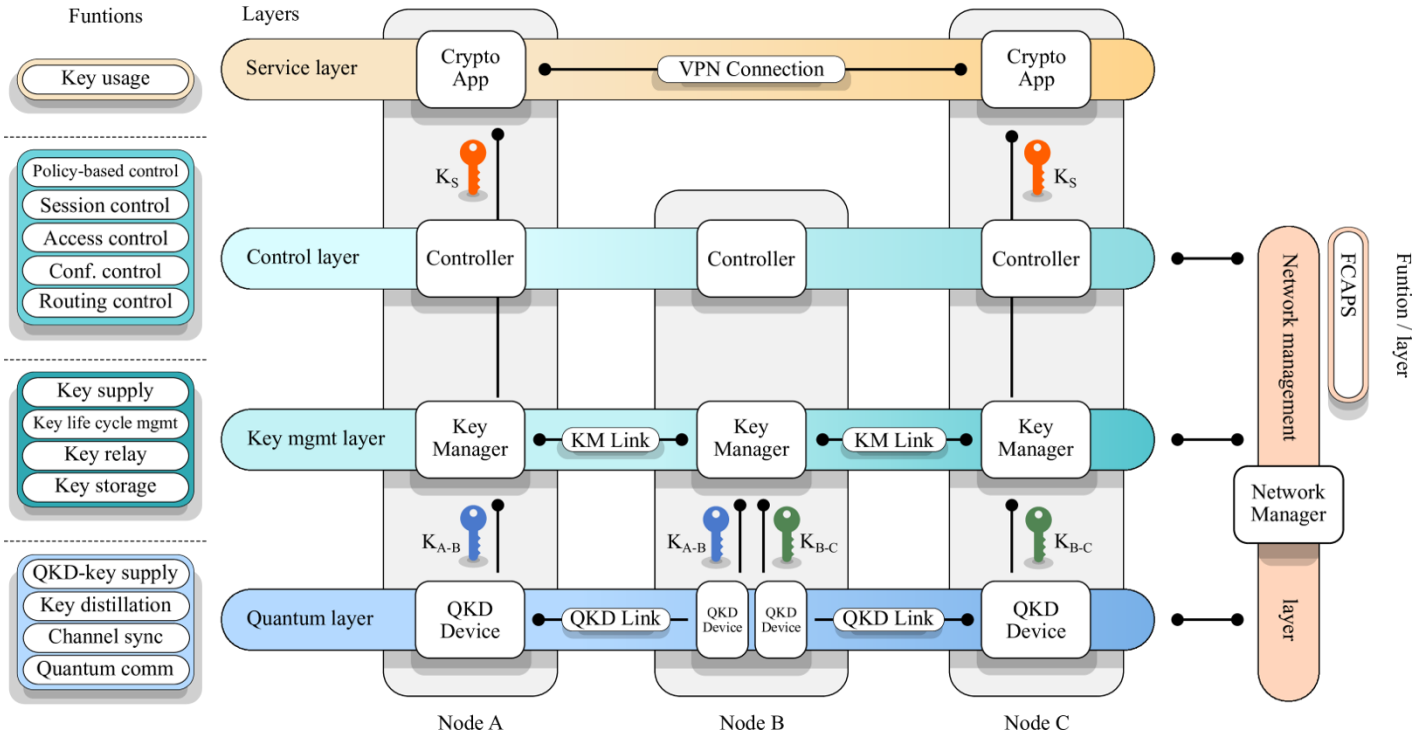
Key Management Concept and QKD proces steps





https://arxiv.org/html/2408.04580v1

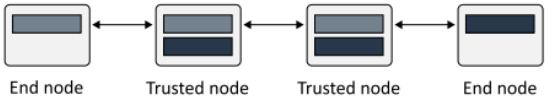
Architecture of QKD Network



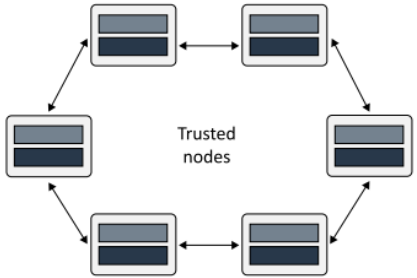
https://arxiv.org/html/2408.04580v1

Architecture of QKD Network

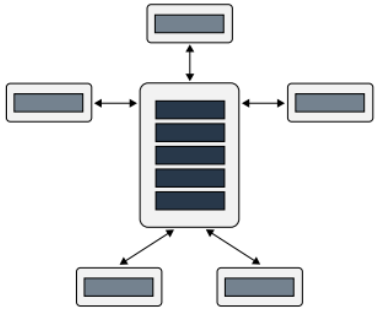
Point-to-point (with relay for long distance)

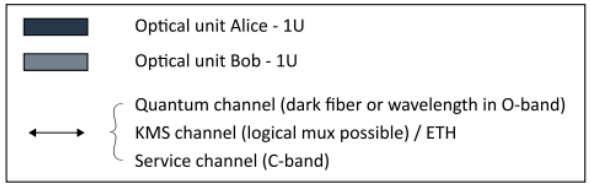


Ring network



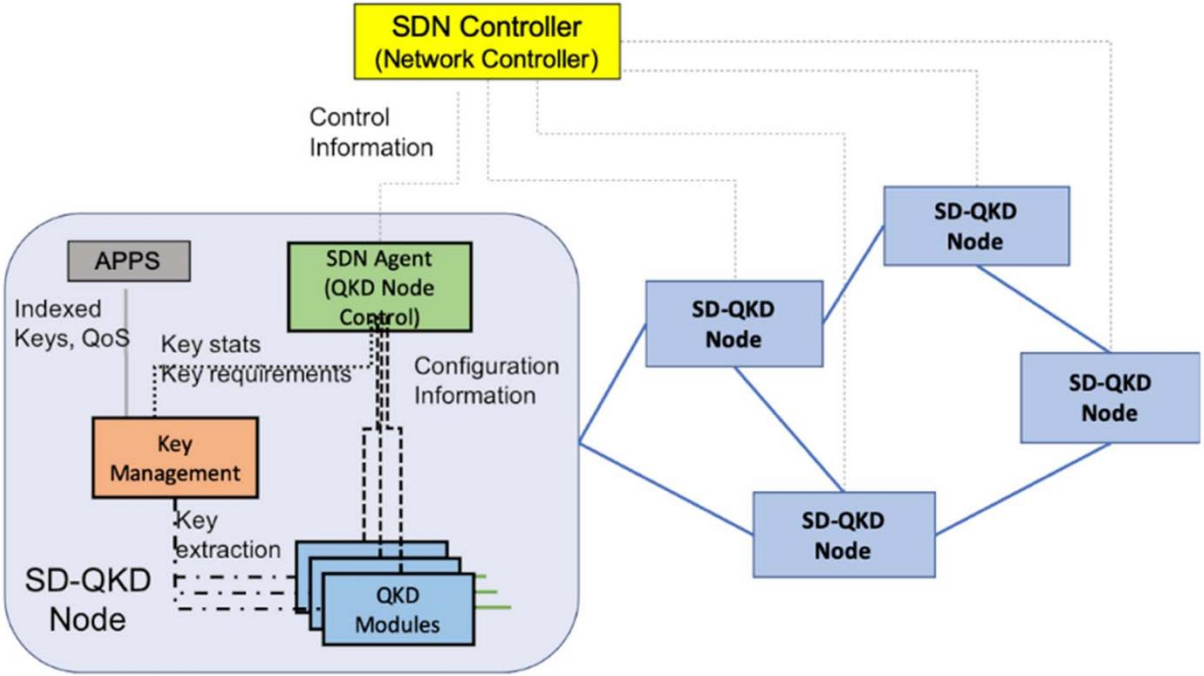
Star





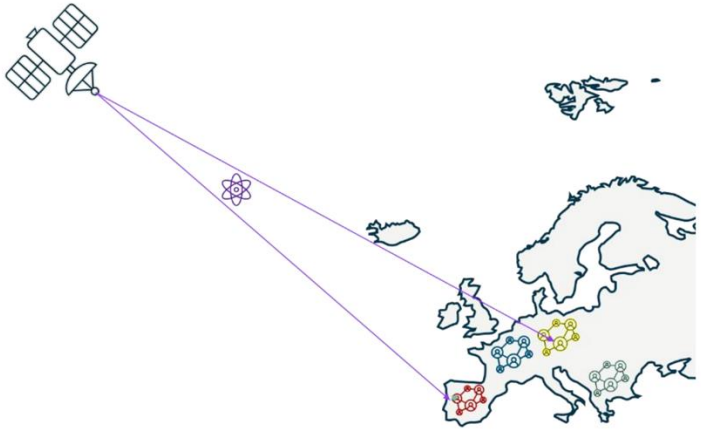
https://www.ilasersg.com/cerberis-xg-qkd-system/

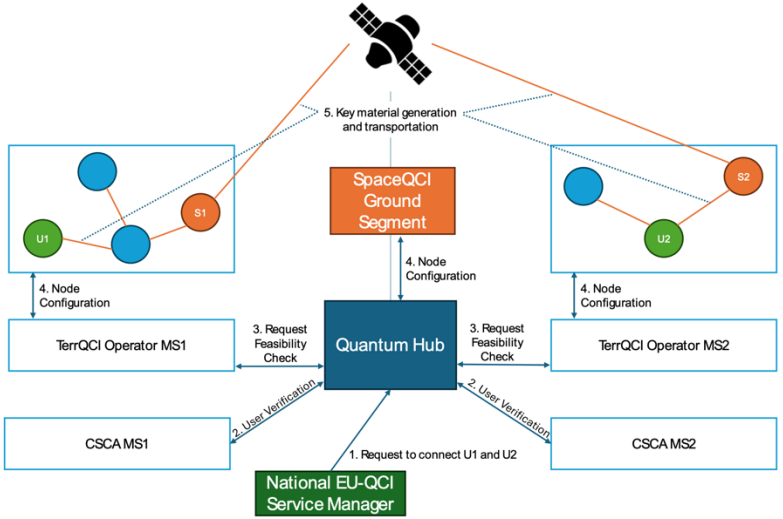
Architecture of SD-QKD Network



https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf

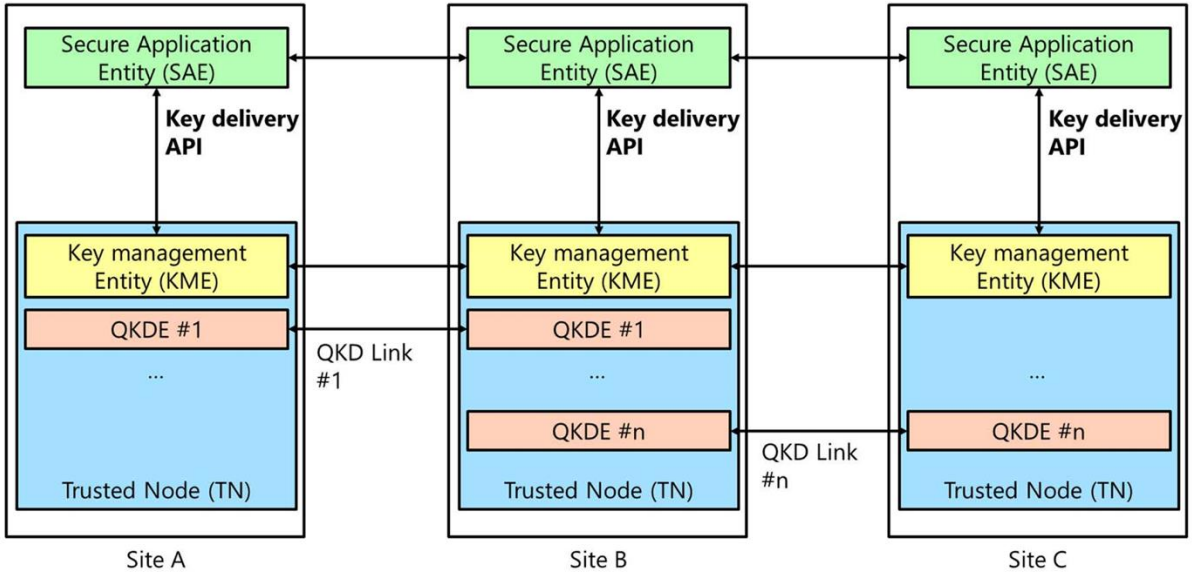
Architecture of EuroQCI





https://digital-strategy.ec.europa.eu/en/miscellaneous/euroqci-conops-concept-operations

ETSI QKD 014



https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

ETSI QKD 014

```
{
    "source_KME_ID": "AAAABBBBCCCCDDDD",
    "target_KME_ID": "EEEEFFFFGGGGHHHH",
    "master_SAE_ID": "IIIIJJJJKKKKLLLL",
    "slave_SAE_ID": "MMMMNNNNOOOOPPPP",
    "key_size": 352,
    "stored_key_count": 25000,
    "max_key_count": 100000,
    "max_key_per_request": 128,
    "max_key_size": 1024,
    "min_key_size": 64,
    "max_SAE_ID_count": 0
}
```

```
{
    "keys": [
        {
            "key_ID": "bc490419-7d60-487f-adc1-4ddcc177c139",
            "key": "wHHVxRwDJs3/bXd38GHP3oe4svTuRpZSOyCC7x4Ly+s="
        },
        {
            "key_ID": "0a782fb5-3434-48fe-aa4d-14f41d46cf92",
            "key": "OeGMPxh1+2RpJpNCYixWHFLYRubpOKCw94FcCI7VdJA="
        },
        {
            "key_ID": "64a7e9a2-269c-4b2c-832c-5351f3ac5adb",
            "key": "479G1OsfljpmfA5vn24tdzE5zqv5CafkGxYrLCk8384="
        },
        {
            "key_ID": "550e8400-e29b-41d4-a716-446655440000",
            "key": "csEMV9KkmjgOPF90uc54+hykhg6iI5GTPH1P9PjgLVU="
        }
    ]
}
```

```
{
    "number": 3,
    "size": 1024
}
```

```
{
    "number": 1,
    "size": 4096,
    "additional_slave_SAE_IDs": [
        "ABCDEFG",
        "HIJKLMN"
    ]
}
```

```
{
    "number": 20,
    "size": 512,
    "extension_mandatory": [
        {
            "abc_route_type": "direct"
        },
        {
            "abc_transfer_method": "qkd"
        }
    ],
    "extension_optional": [
        {
            "abc_max_age": 30000
        }
    ]
}
```

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

Poznan Supercomputing and Networking Center

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl