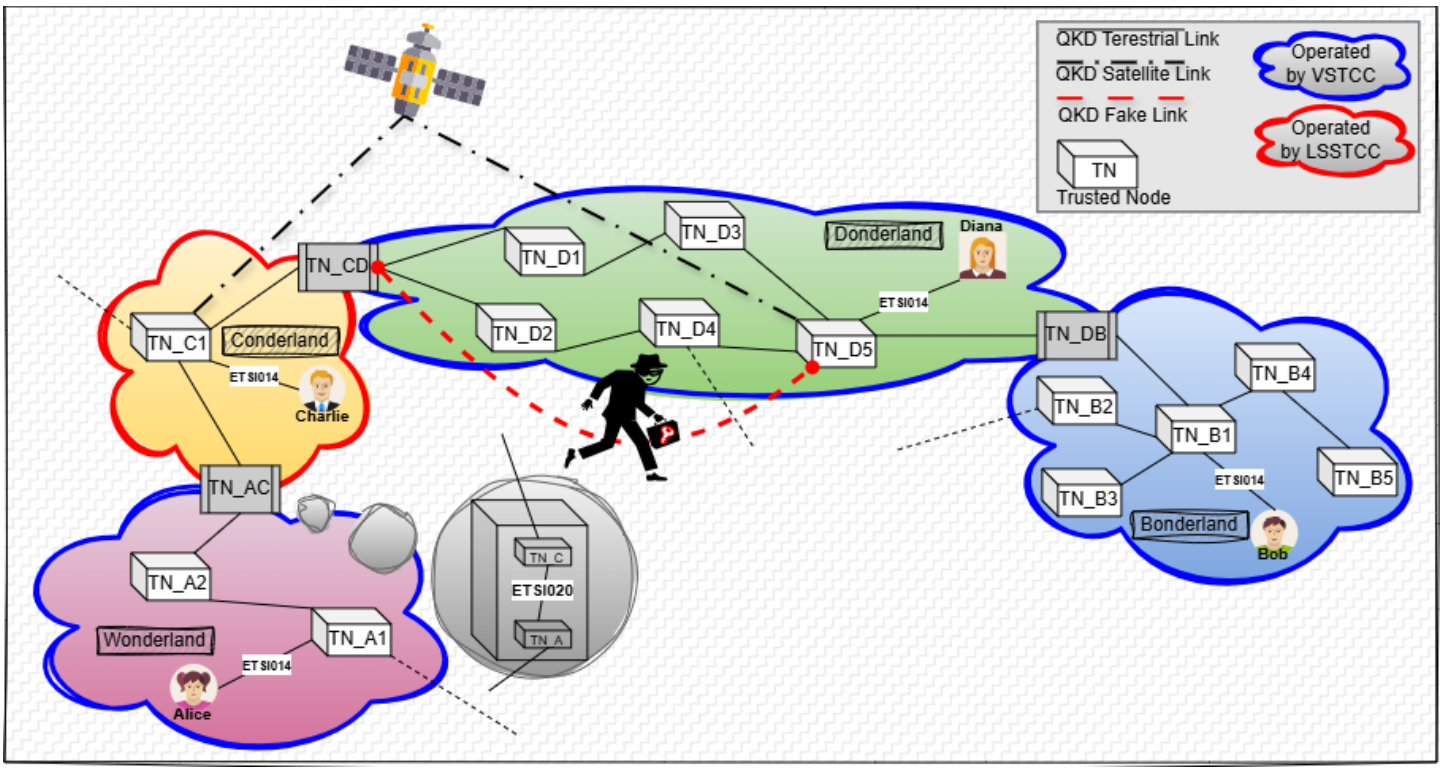
Towards the EuroQCI Proof of Concept: Label Your Keys, or At Least Preserve Labels and Pass On



Current state of affairs

Among EU member states, public authorities, EC & HaDEA, researchers and beneficiaries, SES and vendors, the **unanimous goal within EuroQCI is to create at least a pan-European QKD proof of concept**.

EuroQCI consortia are preparing cross-consortium integration and adopting interfaces such as the recently launched ETSI GS QKD 020, with **the number of cross-border connections being one of the most valued KPI of the second phase of EuroQCI**. Each project will therefore need to develop or procure software components for inter-domain key exchange and orchestration. Additionally, **as per the recommendation of EC/HaDEA and disseminated by PETRUS to all EuroQCI CEF consortia** based on the **policy** *"Preparing for the CEF Call: Assessing a major financial risk due to the impossibility of scaling the European QKD Network"* released in March 2025 [1], **all applicant projects have provisioned a task, a group of tasks, or even a dedicated work package towards cross-consortium operational collaboration**, tasks which are now started or preparing to start.

Now, let us consider the image above with 4 actors in 4 different interconnected domains (countries): Alice in Wonderland, Bob in Bonderland, Charlie in Conderland, and Diana in Donderland, in order to highlight several concerning aspects.

A blocker towards proof of concept

The **most significant issue**, is the following. Suppose Donderland i**s not able to ensure connection or availability of nodes TN_D1 up to TN_D4**, for a variety of reasons:

- Perhaps Donderland has not provisioned national budget for the rental or maintenance of the fiber optic cables connecting the nodes. With the funding for national networks already used, **they are not able to maintain node connections up** (as is the case for some countries in EuroQCI).
- Maybe the infrastructure in Donderland was planned as described in the picture, but **is still under development and is not yet operational** (as is the case for other countries in EuroQCI).
- Perhaps there is a service outage, with **one or more links offline due to their inherent sensitivity** (as is generally the case with most QKD systems).

To satisfy cross-domain demands, domain **Donderland integrates a fake QKD link between TN_CD and TN_D5, by transporting keys via an unsecured mechanism (e.g. email, an unsecured API, even a manually carried external hard-drive, PQC, etc.)**, while still provisioning them using established QKD standards. Without any further information, particularly a clear, authenticated forwarding & operational key history, no party involved in the interconnection can guarantee that QKD was even used in other intermediary domains. Thus, **the resulting infrastructure does not work even as a proof of concept, as fake international keys may be provided without involving any QKD at all.**

Label your keys with metadata!

The solution is to **implement a simple system of key labels and request metadata**, fully compatible with existing standards. Besides **enabling EuroQCI as a proof of concept**, key & request metadata would have the added benefit

Authored by **Dr. Alin-Bogdan Popa** and **Prof. Pantelimon George Popescu**
Reviewed and discussed with **Acad. Sandor Imre** and **Dr. Laszlo Bacsardi**

of **significantly improve the functional and operational performance of EuroQCI** by solving several other current issues, listed below and further explained in detail in [2].

Concerns (with examples)

Many aspects regarding operational interconnection and future commercial adoption are left unresolved:

1. **Lack of fresh keys.** In Conderland, **an older vault key was provided between TN_C1 and TN_CD** instead of a fresh QKD key generated within seconds of its consumption, leading to a compromised military use-case between Alice and Diana.
2. **Impossibility of request constraints.** Due to political reasons, Bob requires keys to **avoid specifically the region of node TN_D2**. However, it is **not possible to relay such requests** programmatically, so the network will never satisfy Bonderland's political and operational constraints.
3. **Expensive satellite keys.** Charlie and Diana motivate the significant national expense on OGSs and space-segment connection A) by promising the satellite keys which bypass potentially compromised terrestrial trusted nodes will be used in particular governmental use-cases, and B) by committing politically to a fair allocation of satellite keys to domains Wonderland and Bonderland, which lack OGS capabilities. However, with **satellite and terrestrial keys being part of the same pools and forwarded all the same**, **they become indistinguishable** and the space-segment expense is considered a waste of money.
4. **Security breaches.** Following a public **announcement of a security breach on node TN_D2**, Alice and Bob want to **assess the extent and severity of the damage, as well as identify the potentially compromised communication**, for example by identifying which of their keys were forwarded along TN_CD→TN_D2→TN_D4→TN_D5 and which along TN_CD→TN_D1→RN_D3→TN_D5 (or perhaps even via satellite connection bypassing most Donderland nodes altogether). However, with **no way to bind route and composition techniques to a key**, they must deprecate their entire secure communication during the affected period as well as for the subsequent period for a duration equal to the time a key is usually stored in a vault.
5. **Incompatibility with QKD as a service.** In future QKD-as-a-Service (QKDaaS) models, the natural development when adoption of QKD reaches higher levels, **a QKD service provider requires machine-readable information on beneficiary, custody, reservation, SLA class, and billing**, in order to delegate capacity through third party providers or tenants (for example, when the network of Conderland is operated by a different company). But without a way to do this, the business model is doomed to fail, and QKD networks will not reach widespread adoption for critical commercial infrastructure.

Recommendation for a simple viable solution

Our recommendation is for all EuroQCI CEF projects to take advantage of the opportunity given by available work in cross-domain software-level interconnection to label their keys with as much relevant metadata as possible, which is fully possible and compatible with already established standard such as via ETSI GS QKD 020/014 mandatory & optional extension mechanism. A standardized common metadata profile for QKD networks should cover: *common semantics, binding to keys & requests, transport through existing interfaces or complementary mechanisms, authentication, integrity, selective topology disclosure, access control, rules for enforcement, governance, and versioning*. Pending the adoption of a complete standard at European level or maybe in case of lack of implementation capacity, the recommendation is to **ensure external key and request metadata information is at least preserved and passed on at node and domain boundaries**.

This opportunity must be **seized now**, as **retrofitting such mechanisms later may be impractical and expensive** due to lack of budgeted effort and acquisition planning, and all the key material that has been generated in the meantime will have already been consumed and **will remain untrackable forever**.

Alignment with CEF Digital EuroQCI objectives

The approach is strongly aligned with declared objectives of the present call:

- The call aims for "*securing their communications and data, especially those that cross national borders and serve more than one Member State*" – see section **"A blocker towards proof of concept"**
- "*The management of encryption keys (Key Management System) between all elements of the EuroQCI in an end-to-end manner should also be considered. This would include managing the keys efficiently and securely, ensuring their transmission to recipients, optimal routing and monitoring of system performance, and solutions for the control layer, i.e. software-defined network (SDN)*" – see **concerns 1, 2, 5**
- As a priority, "*Addressing the coexistence of QKD with conventional communications technology is encouraged, together with interoperability at the orchestration level of the network. Solutions should rely on state-of-the-art interoperability methods and standards, and address scalability, upgradability and end-to-end security.*" – see **concern 4**
- As a priority, *"Interconnection with the EuroQCI's space segment"* – see **concern 3**

[1] https://quantum.upb.ro/qpolicies.html
[2] Popa AB, Popescu PG. "In QKD, Key Metadata is Key." *arXiv preprint arxiv: 2608.11502* (2026)

Authored by **Dr. Alin-Bogdan Popa** and **Prof. Pantelimon George Popescu**
Reviewed and discussed with **Acad. Sandor Imre** and **Dr. Laszlo Bacsardi**