# Basque open and standard-compliant KMS for quantum-safe networks by EHU

Eire Salegi Zulaika, University of the Basque Country (EHU)
Ane Sanz Rekalde, EHU/RedIRIS
eire.salegi@ehu.eus
ane.sanz@ehu.eus

Infoshare: Community-Built Quantum Communication Tools
03 December 2025

# Agenda

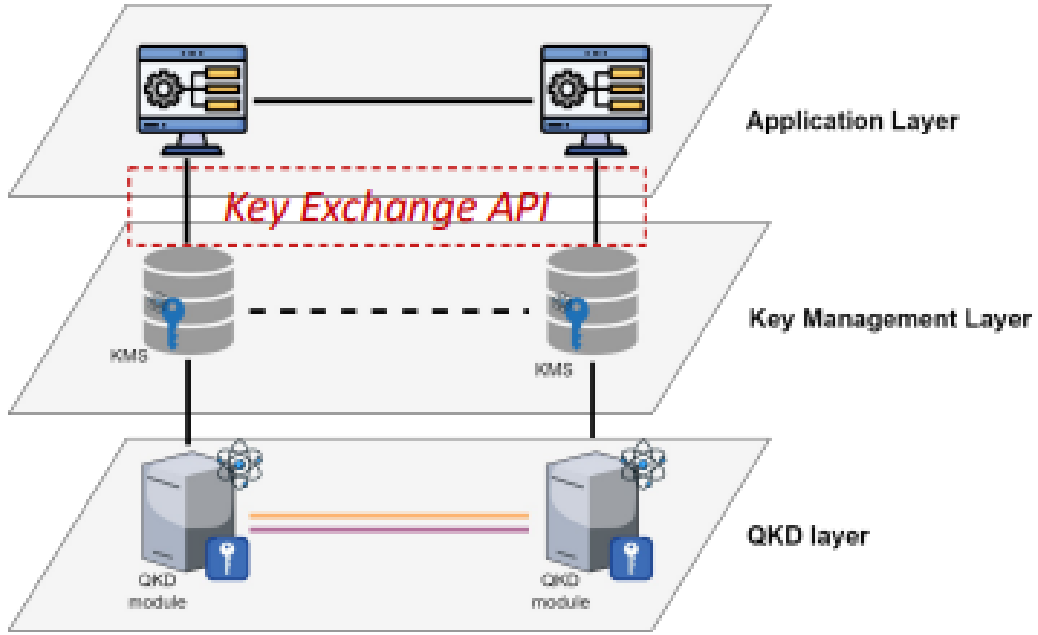
- Introduction
- Adaptive Security Framework
- Implementation
- Conclusions

# Introduction

# Introduction

QKD presents various challenges when integrating in real-world networks:

- Physical constrains (links max. ~100km).
- Inherently point-to-point topology.
- Unfeasibility of a fully quantum network.

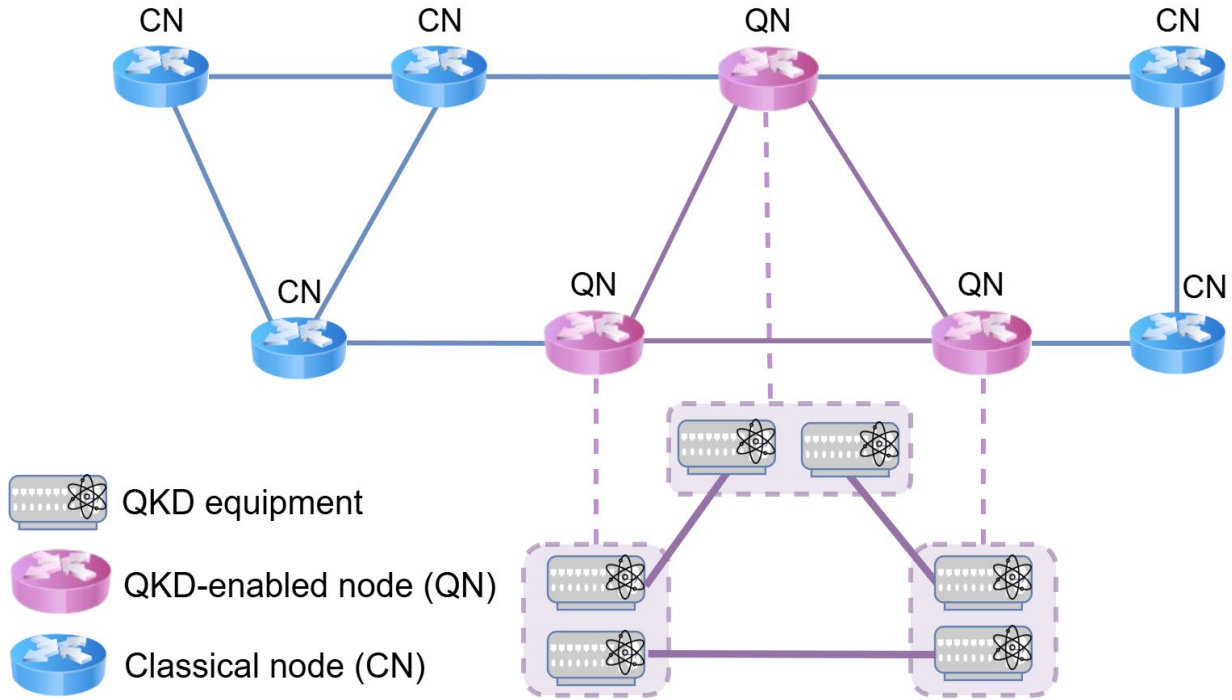


# Adaptive Security Framework

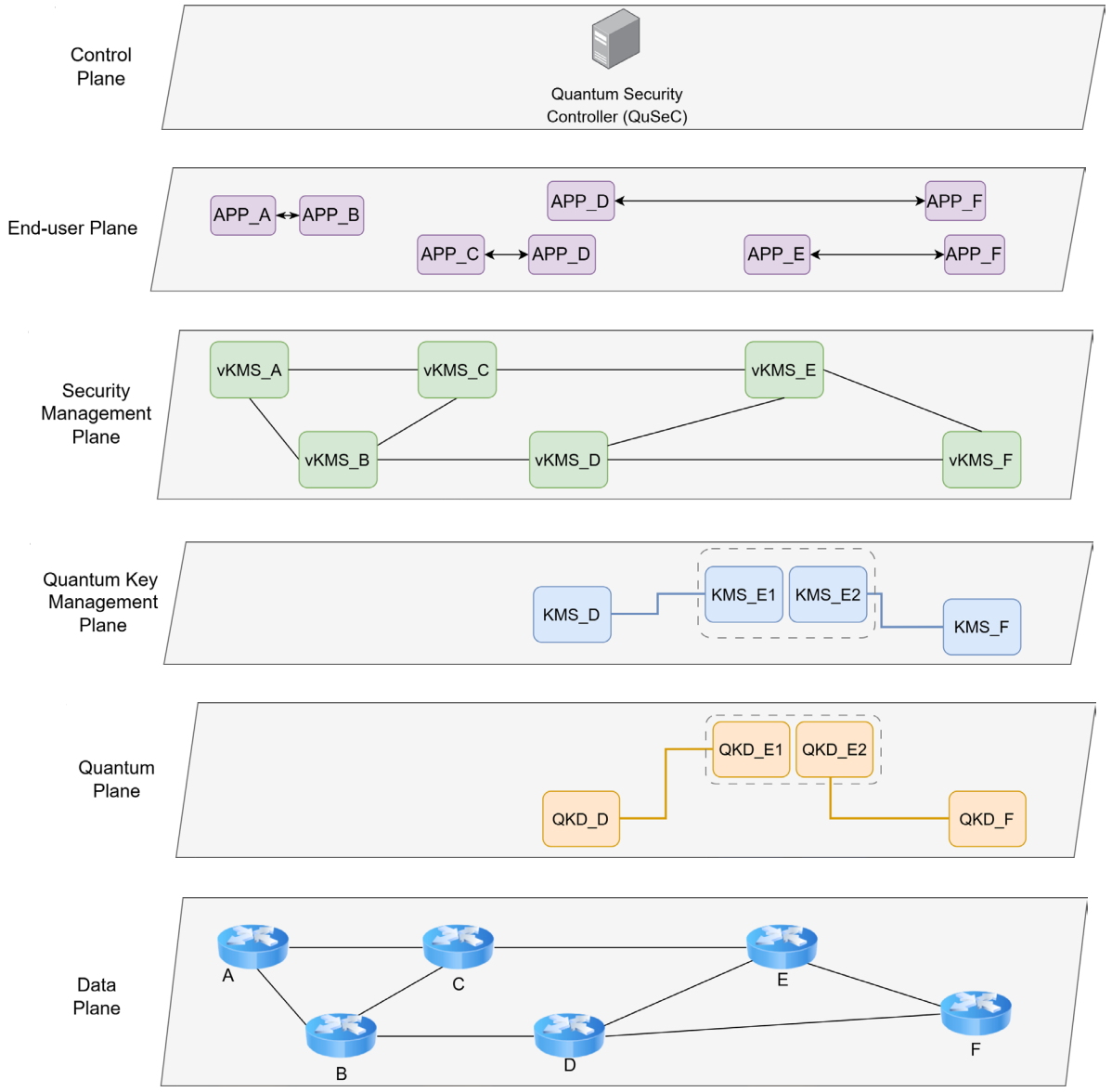
GN5-2

# Adaptive security framework

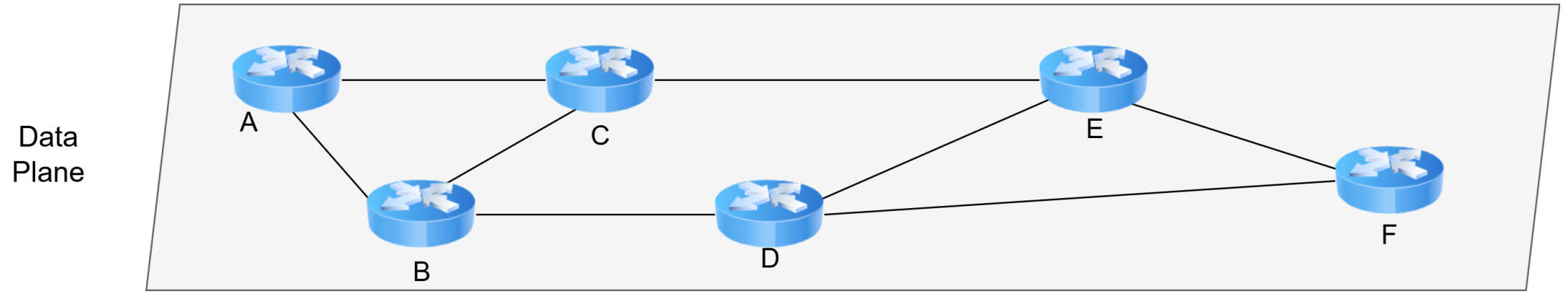
- SDN-based centralised controller.
- Heterogeneous networks.
- Adaptive security.
- Hybridisation PQC/QKD.



# Architecture of the framework

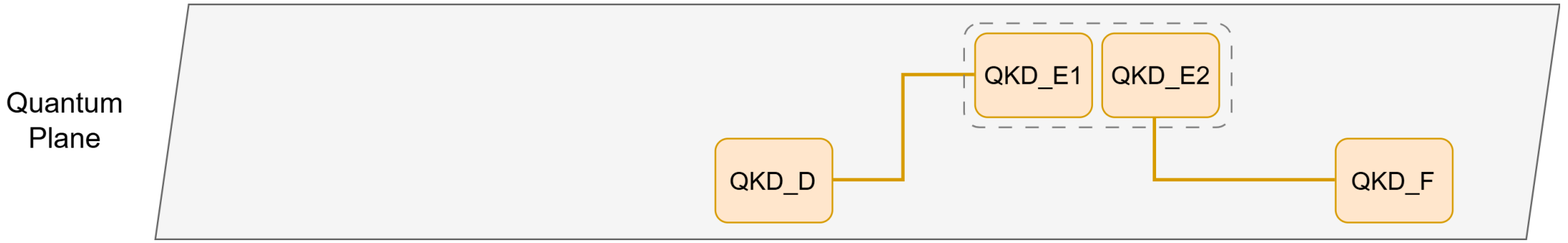


# Data Plane



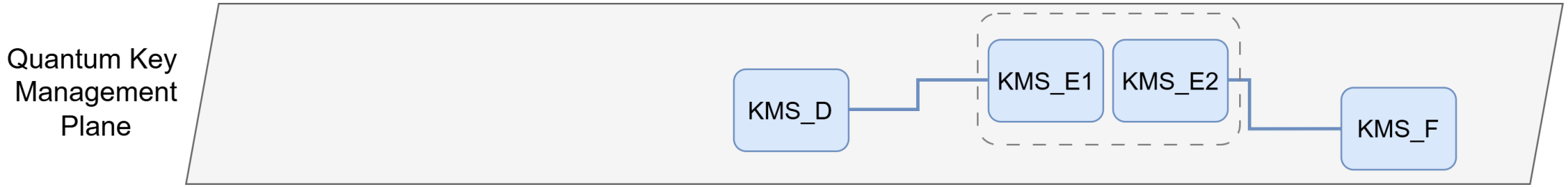

- Infrastructure and equipment for user traffic transmission.

# Quantum Plane




- QKD modules and links.
- Responsible for generating keys and forwarding them to the plane above.

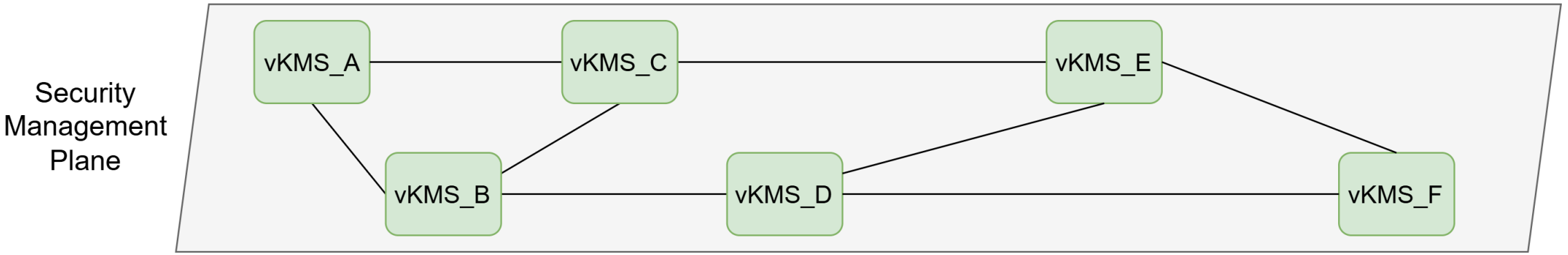
# Quantum Key Management Plane




Local KMS:

- Deployed only in QNs.
- Store the keys handed by the QKD.
- Implement ETSI 014 standard for the plane above.
- Receive controller's network instructions.
- Other functionalities related to relaying keys (including ETSI 020).

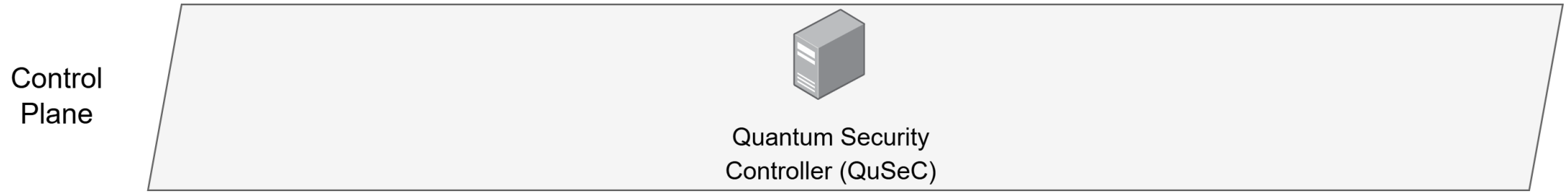
# Security Management Plane




Virtual KMS (vKMS):

- Deployed in both QN and CN.
- Allows CN to establish quantum-safe keys.
- Receives requests from the end-user applications, leveraging ETSI 014.
- Under the instructions of the controller, executes operations related to QKD, PQC or hybridisation to deliver quantum-safe keys.

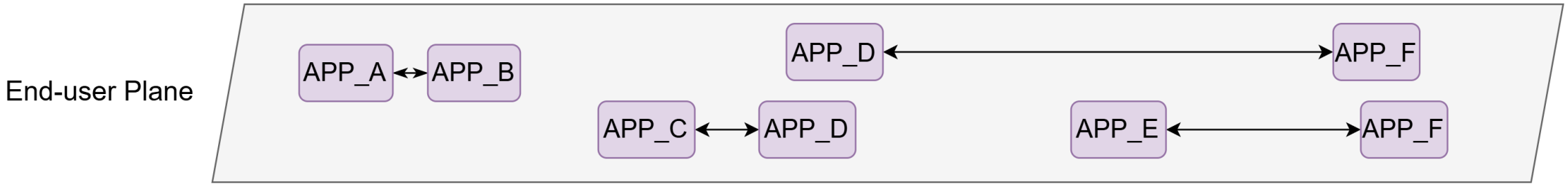
# Control Plane




Quantum Security Controller (QuSeC):

- Maintains a global view of the network topology.
- Path computation functions.
- Assigns a Security Level for each application pair.
- Path installations in Local KMS.
- Cryptographic indications on vKMS.

# End-user plane

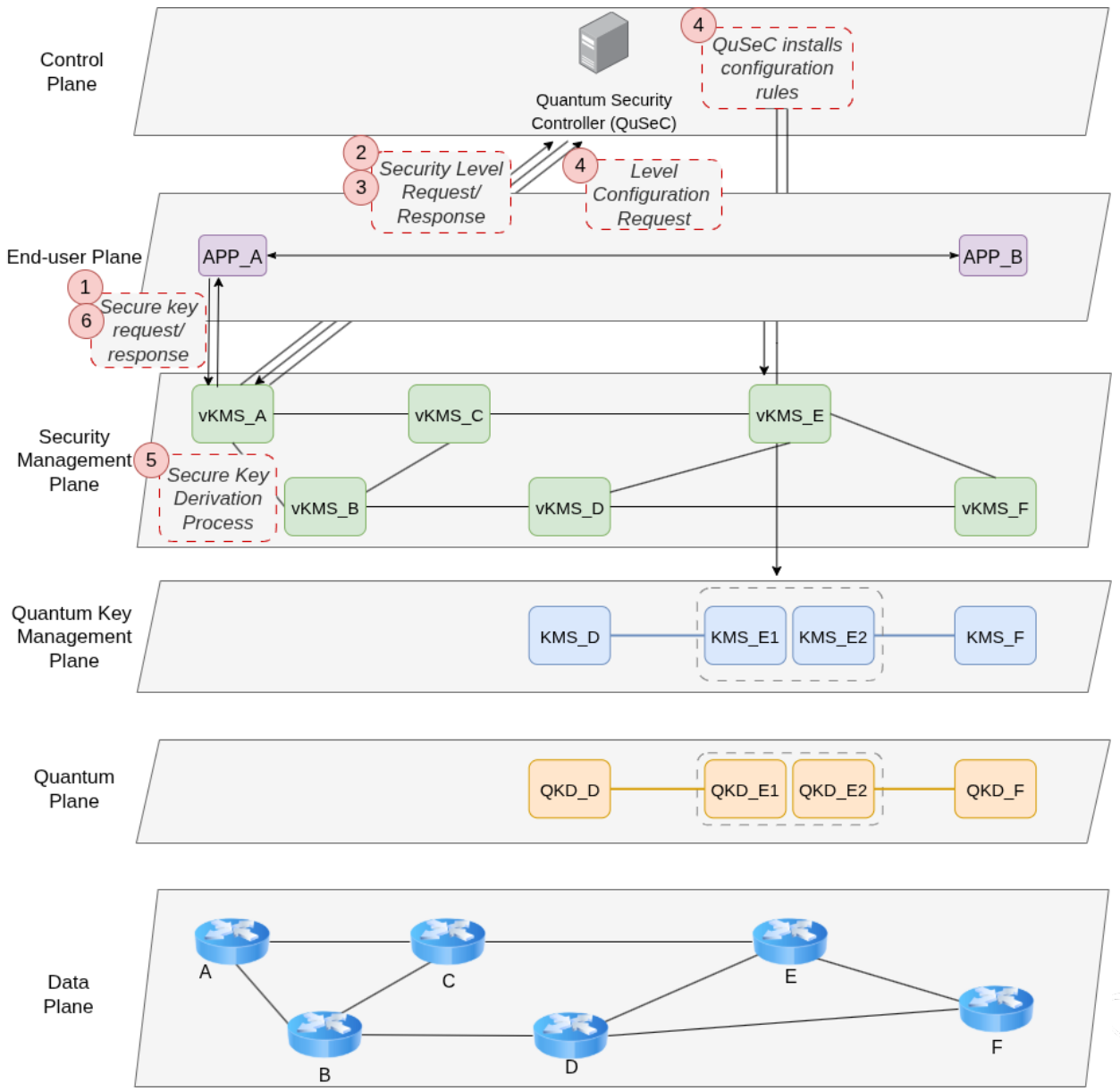



- The applications that request symmetric keys without knowledge of the underlying infrastructure.

# E2E key establishment

## Initiating application side:

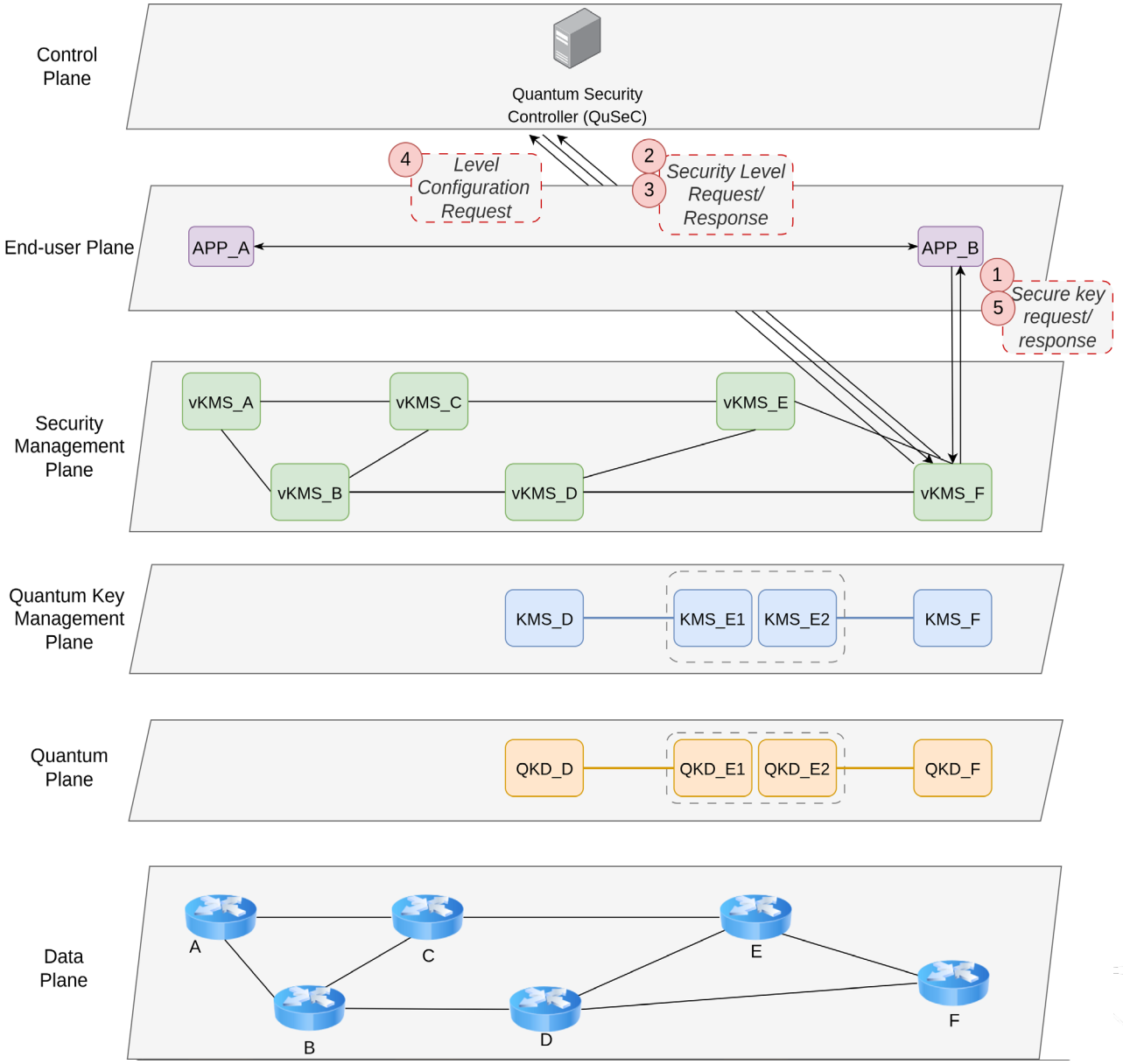
1. Initiating application requests a key to its vKMS.
2. vKMS queries the QuSeC for the Security Level.
3. The QuSeC assigns a Security Level.
4. vKMS requests a level-specific configuration and QuSeC realises the required installations.
5. vKMS starts the corresponding Secure Key Derivation proccess.
6. vKMS delivers the key container to the initiating application.



# E2E key establishment

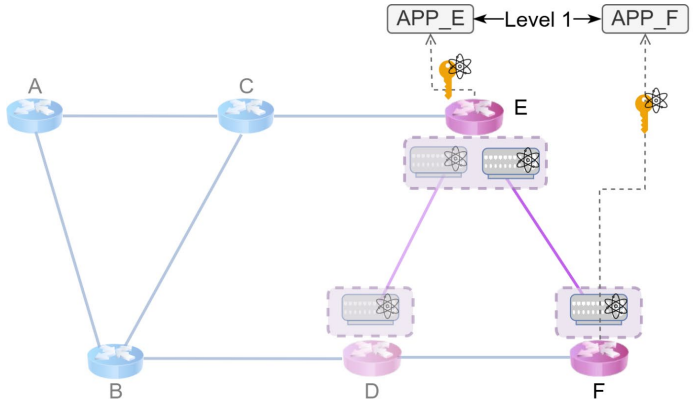
## Target application side:

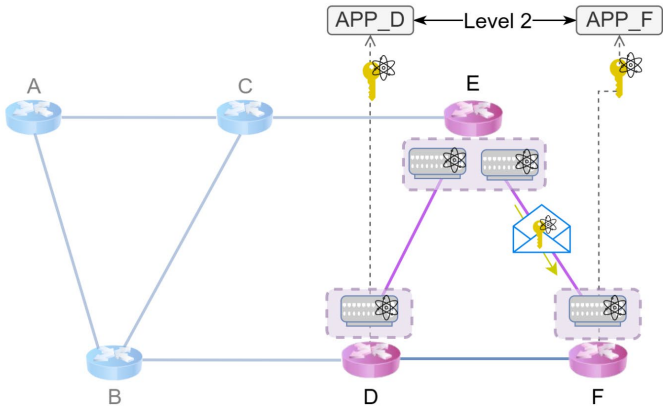
1. Target application requests a key to its vKMS specifying the key ID.
2. vKMS queries the QuSeC for the Security Level.
3. The QuSeC assigns a Security Level.
4. vKMS requests a level-specific configuration and QuSeC checks state and responds that the key is ready to be delivered.
5. vKMS retrieves and delivers the key container to the target application.

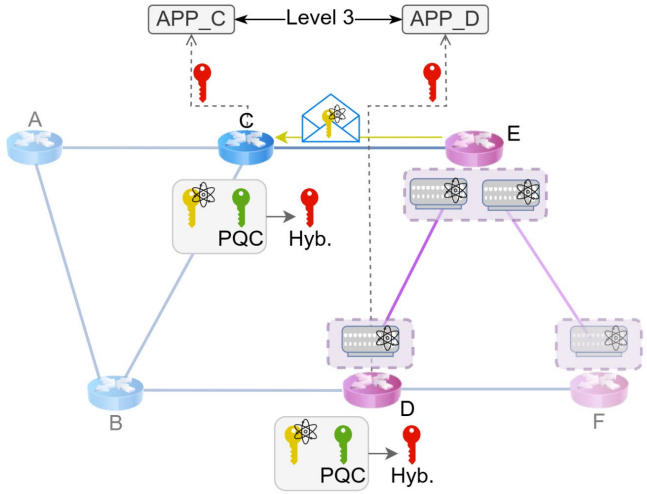


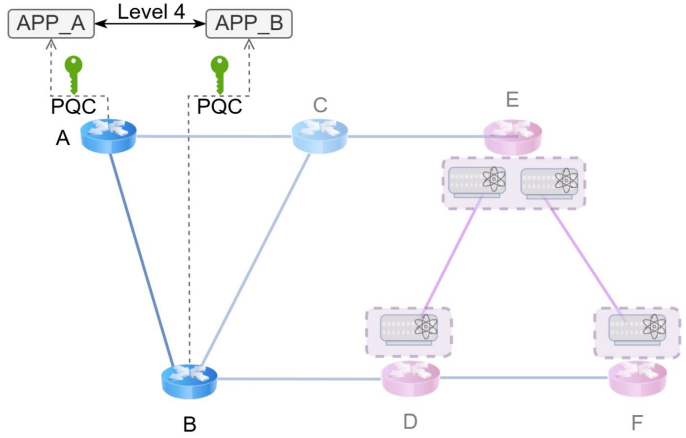
# Security Assignment

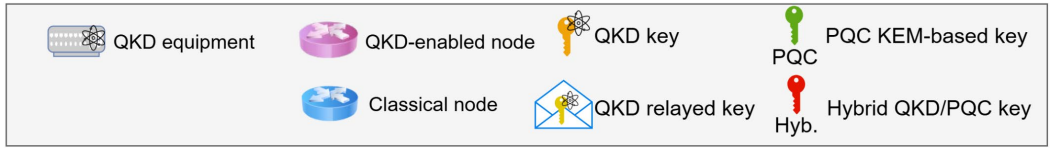
- Depends on the quantum capabilities and the path of the key requesting nodes.
- The QuSeC assigns a Security Level for each application pair:
  - Level 1
  - Level 2
  - Level 3
  - Level 4



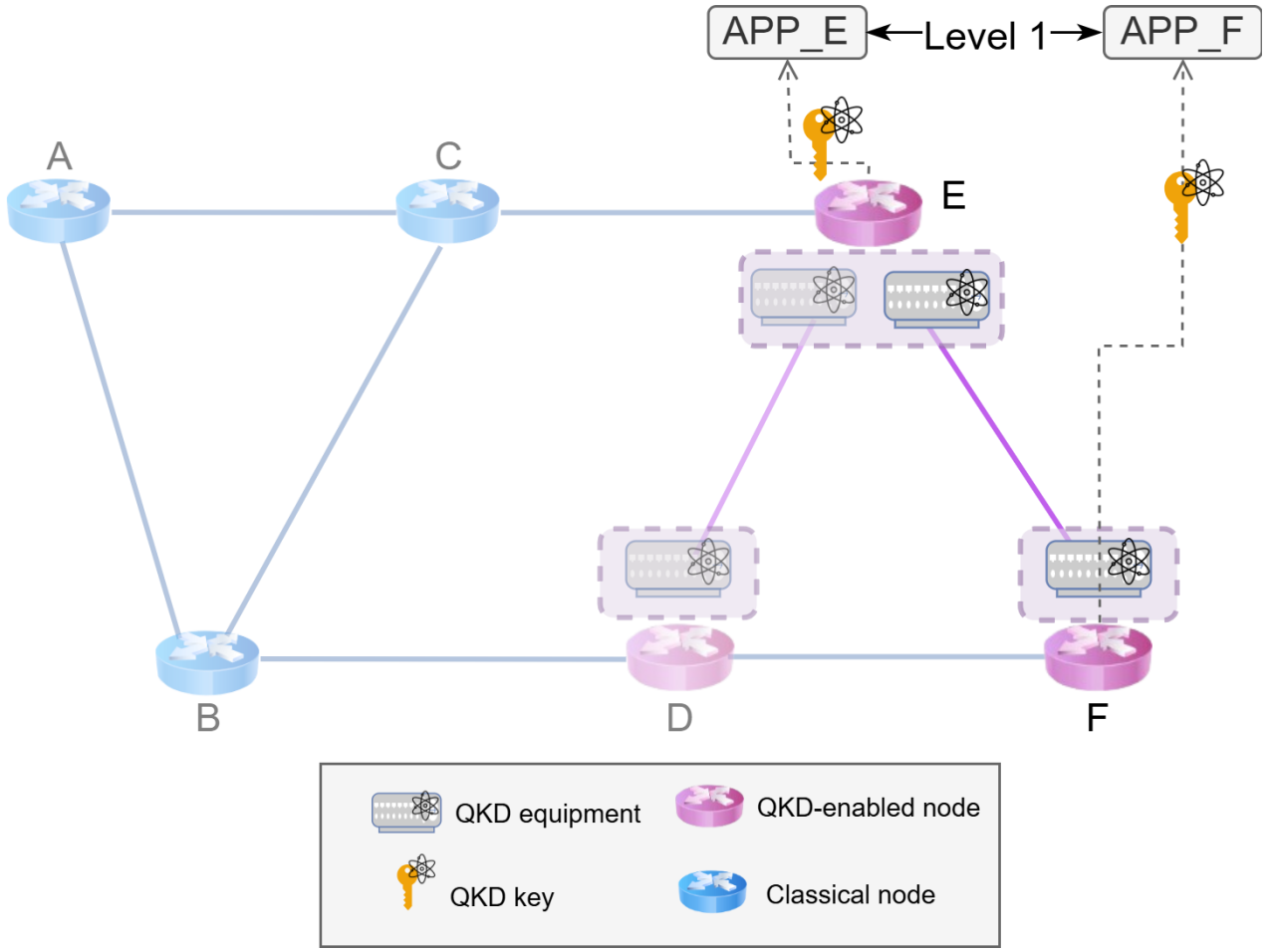



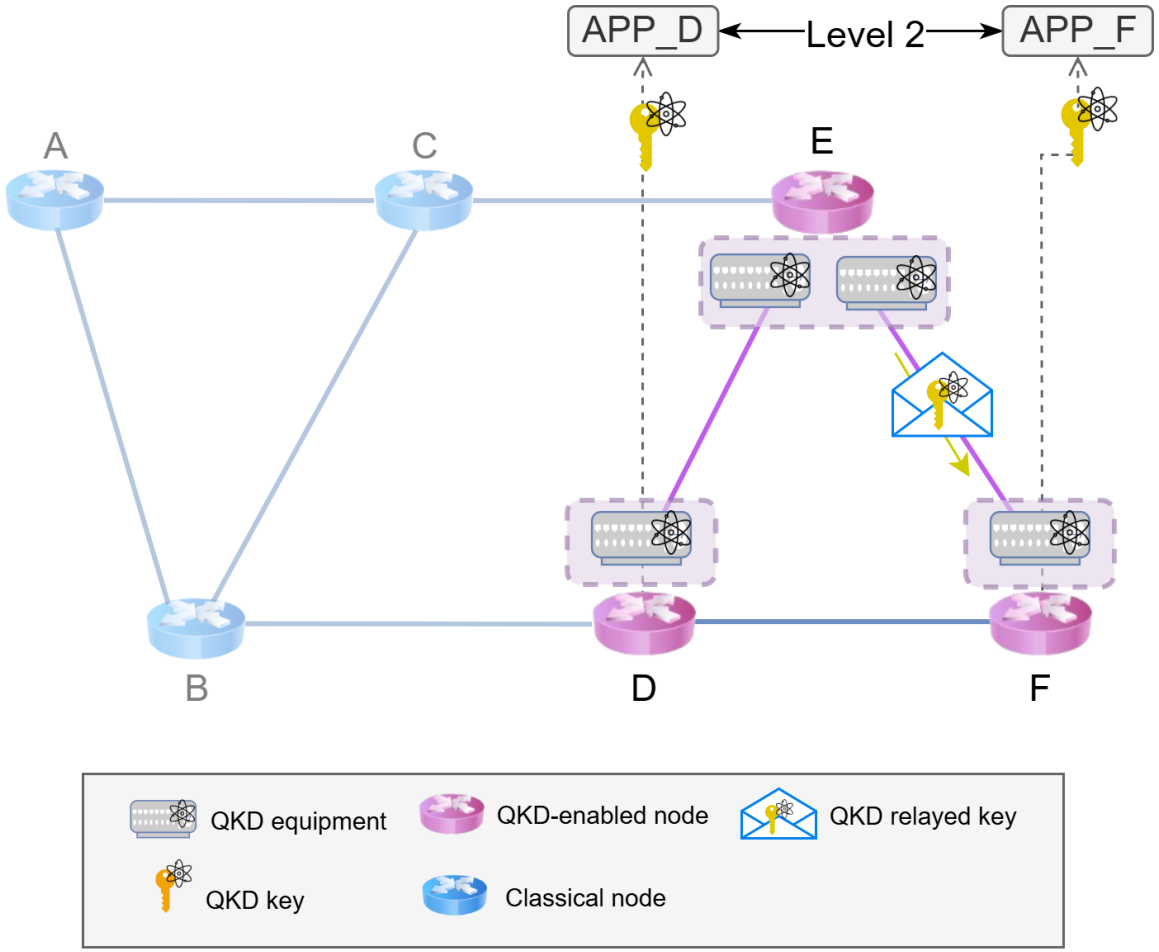
# Level 1

- Direct QN-to-QN
- Direct QKD link
- Final key is directly the QKD key



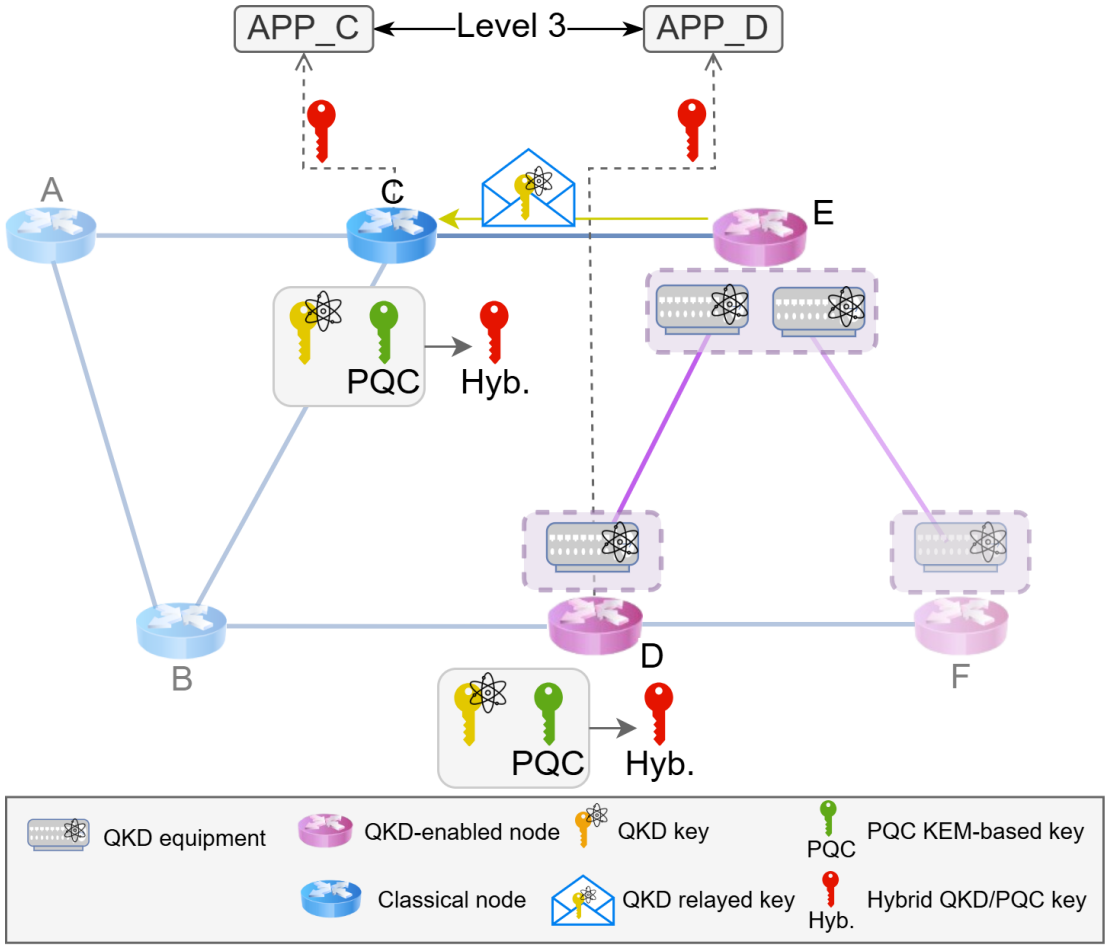
# Level 2

- Multi-hop QN-to-QN
- No direct QKD link, need for trusted relays
- QKD key relay with OTP protection



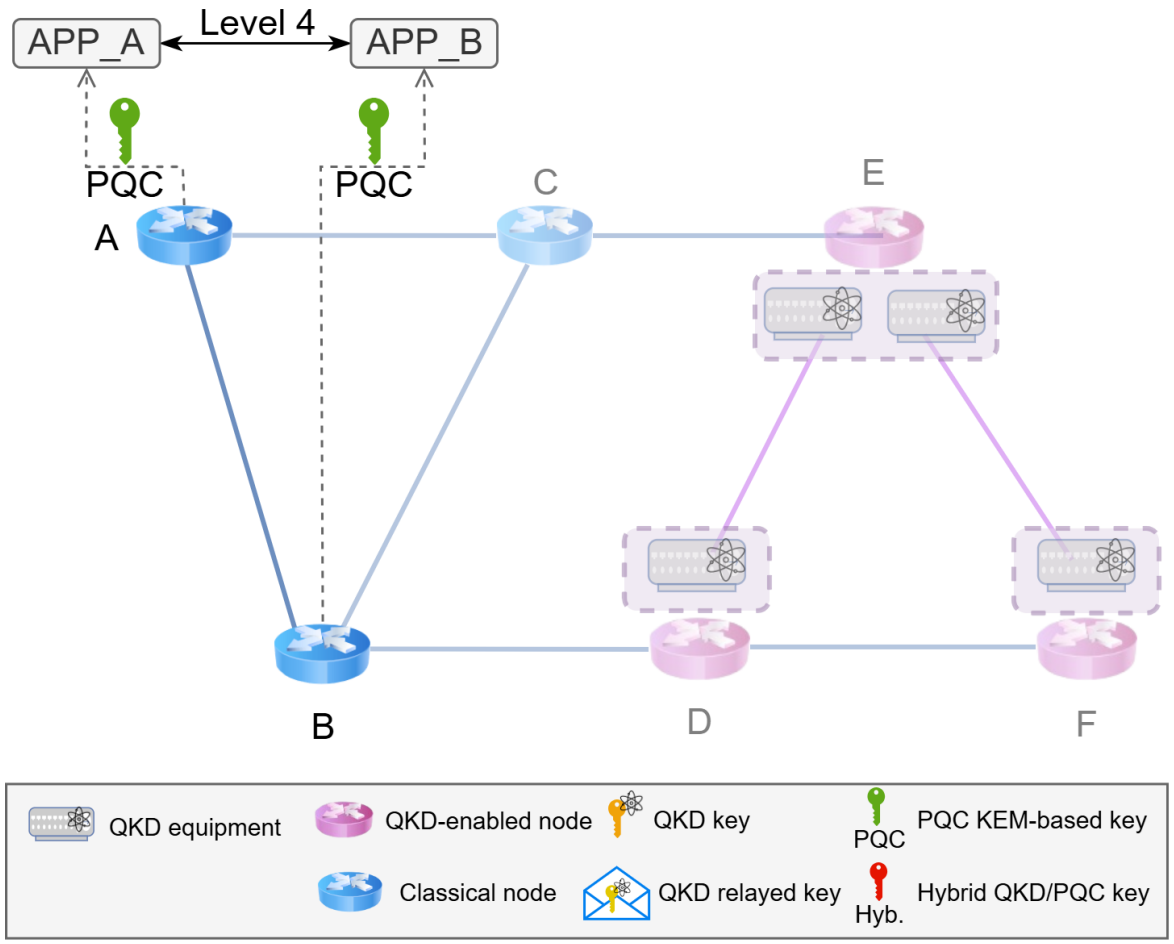
# Level 3

- CN-to-QN
- Relay QKD key to CN
- Hybridisation of QKD and PQC keys



# Level 4

- CN-to-CN
- Purely PQC key establishment



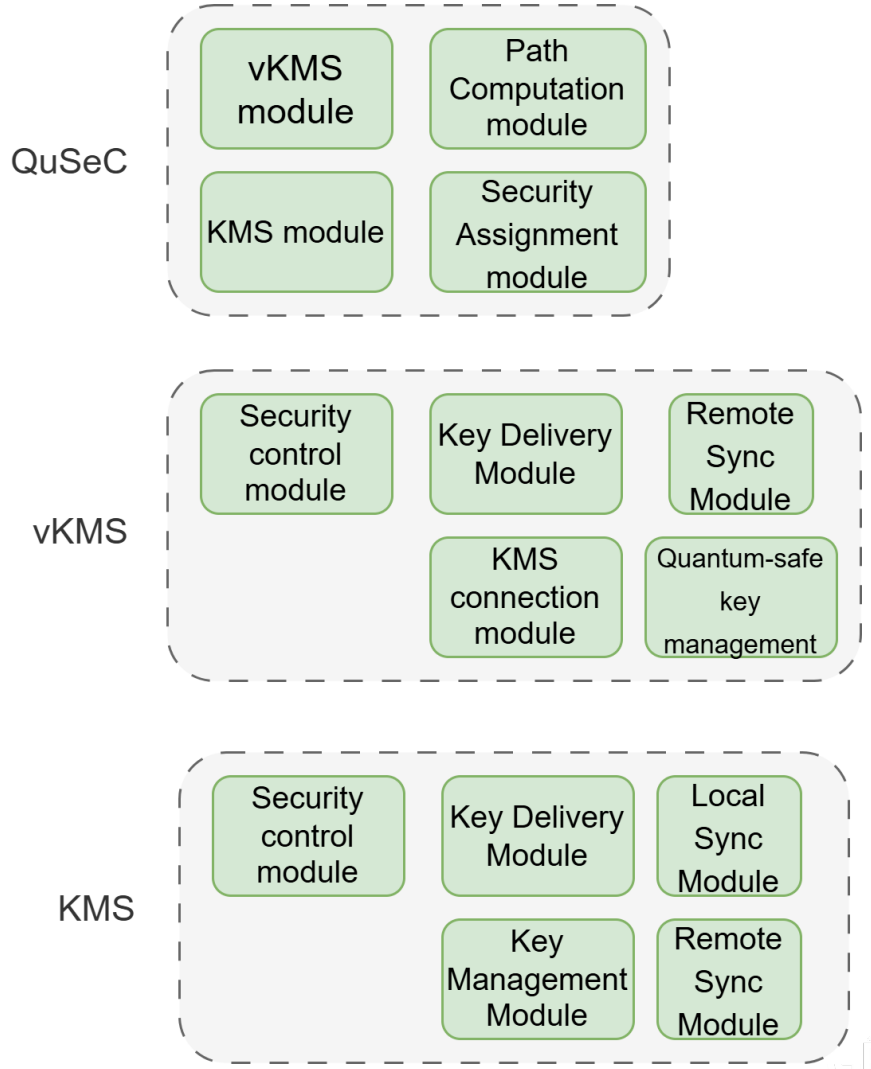
# Summary Table

| Security Level | Established Key |
|---|---|
| Level 1 | QKD |
| Level 2 | QKD |
| Level 3 | Hybrid PQC/QKD |
| Level 4 | PQC |

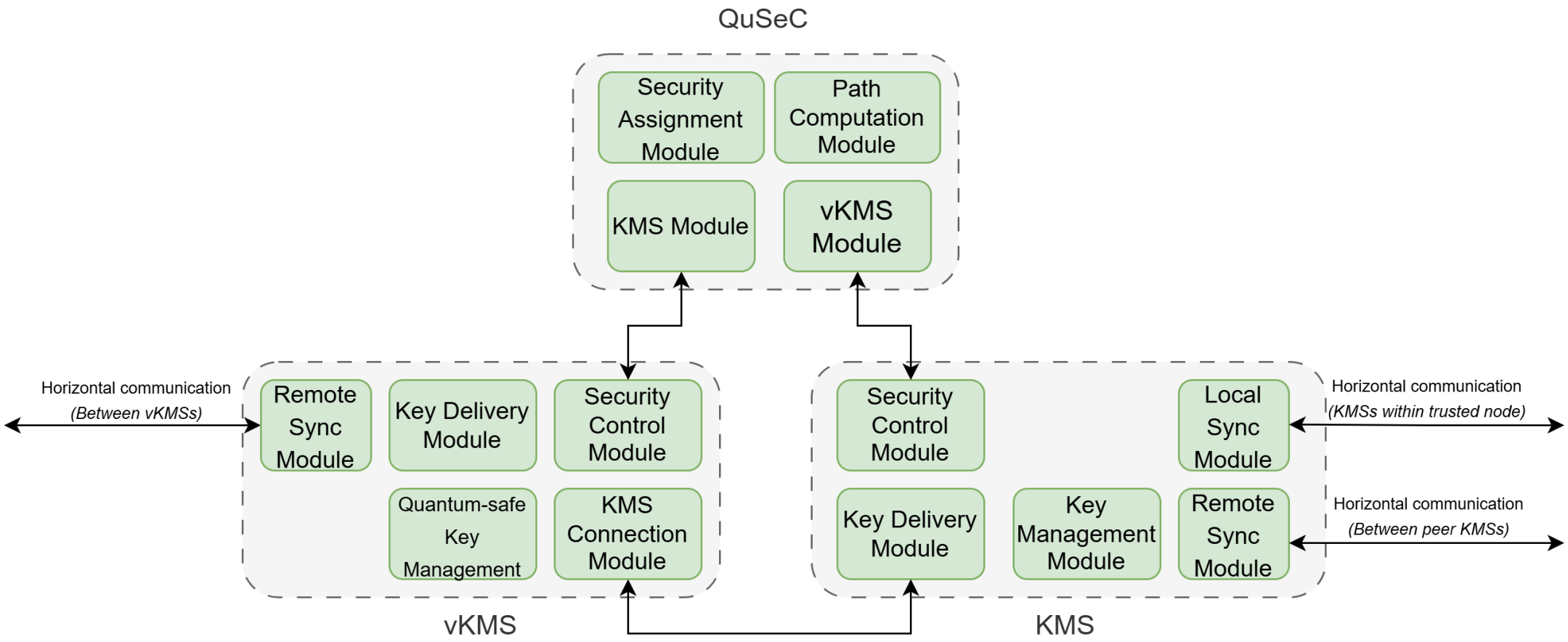
# Implementation

# Modular implementation of QuSeC, vKMS, KMS

- Enables independent development, testing, and integration of individual modules.
- Enhances resilience and maintenance.
- Allows scalability and extensibility, as new capabilities can be integrated seamlessly.
- Improves interoperability.



# Modular implementation of QuSeC, vKMS, KMS



# Conclusions

# Conclusions

1

## Validation

The framework has been validated in a virtualised testbed.

2

## Use case

It has been integrated on a 5G network testbed with different commercial QKD equipment.

3

## Open Source

Currently the source code is not available, but we plan to publish it open source.

https://arxiv.org/abs/2511.22416

# Thank You

Eire Salegi Zulaika, University of the Basque Country (EHU)
Ane Sanz Rekalde, EHU/RedIRIS
eire.salegi@ehu.eus
ane.sanz@ehu.eus

www.geant.org

Co-funded by
the European Union