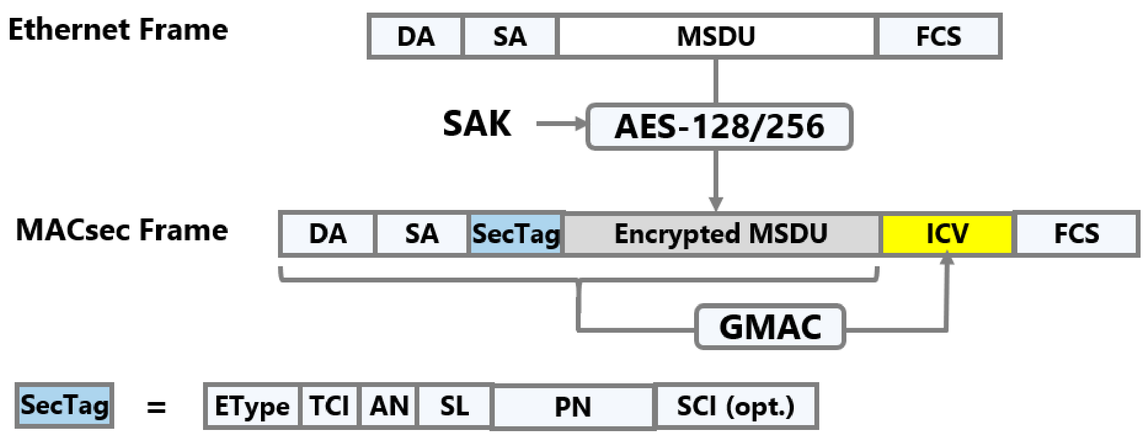
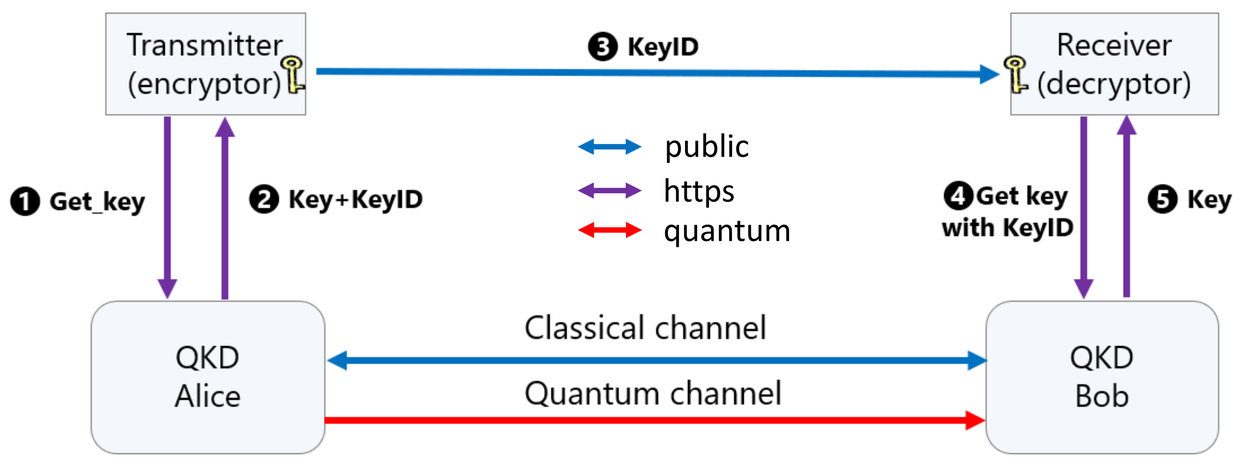
Using QKD in MACsec for Secure Ethernet Networks

Joo Yeon Cho and Andrew Sergeev, ADVA Optical Networking (jcho@adva.com. asergeev@adva.com)

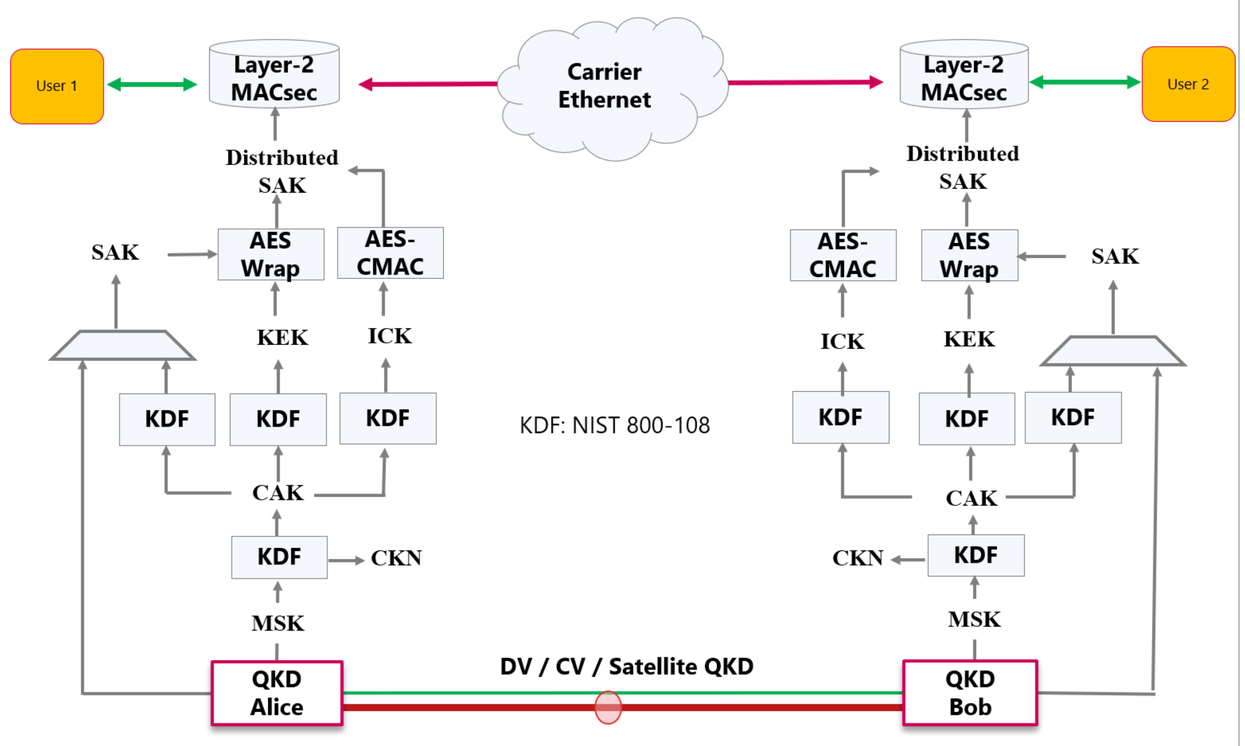
IEEE 802.1AE MACsec encryption and integrity check



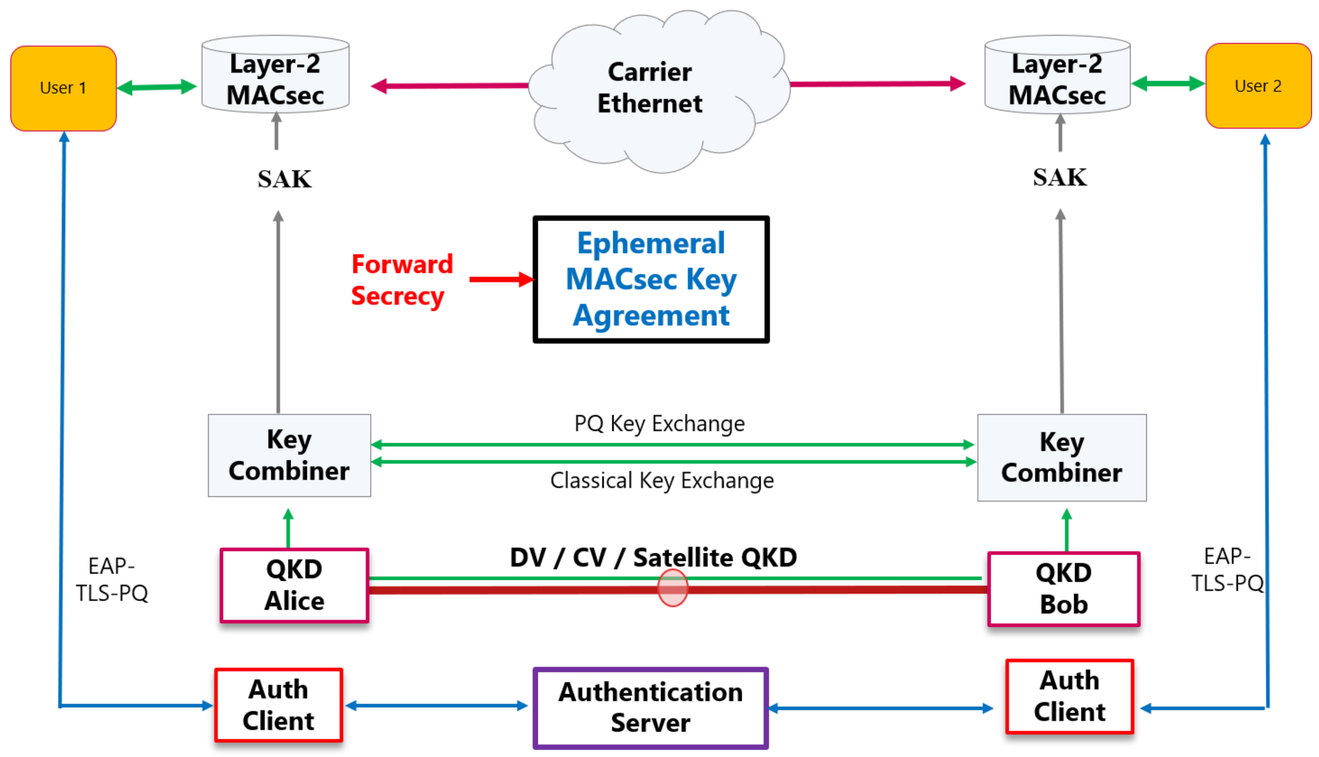
QKD key delivery interface based on REST API: ETSI GS 014



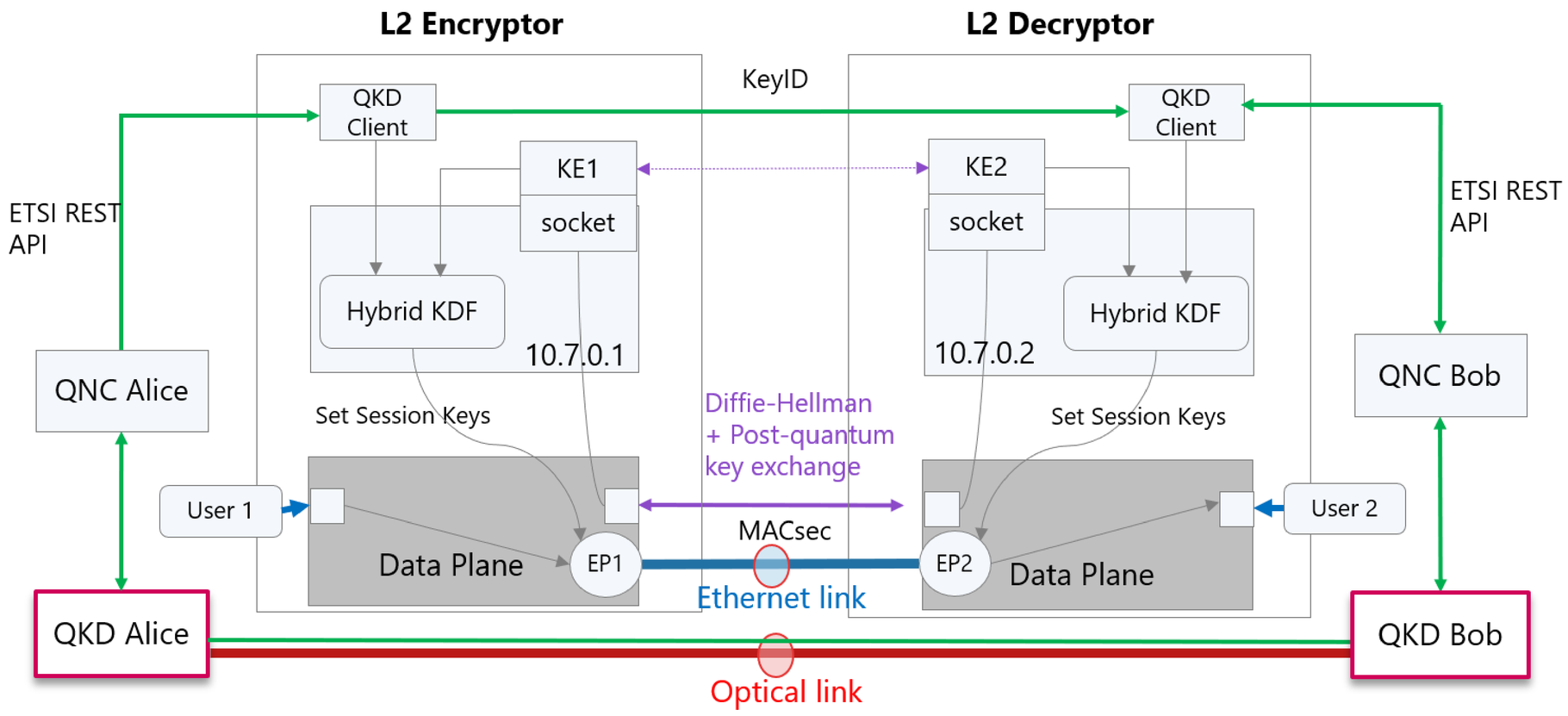
S1. Hierarchical derivation of MACsec keys using QKD



S2. Hybrid ephemeral MACsec keys using QKD



Test Platform: P2P MACsec using QKD + PQC + DH key exchange



Conclusion and References

- We propose a QKD-based session key exchange protocol for MACsec: hierarchical and ephemeral.
- A hybrid key exchange provides a robust solution for quantum-safe key exchange.
- We verified by experiments that the proposed protocol can be performed with a reasonable speed and latency.

Acknowledgement

This research is co-funded by OpenQKD project under the Horizon 2020 Framework Program of the European Union (Grant agreement No 857156).