EuroQCI

REPUBLIKA HRVATSKA
Ministarstvo znanosti, obrazovanja i mladih

Funded by the European Union

CROQCI

MBT 2026
Quantum-safe Networking

Duje Gašperov
Advanced IT Technologies and Software Development Senior Specialist Coordinator

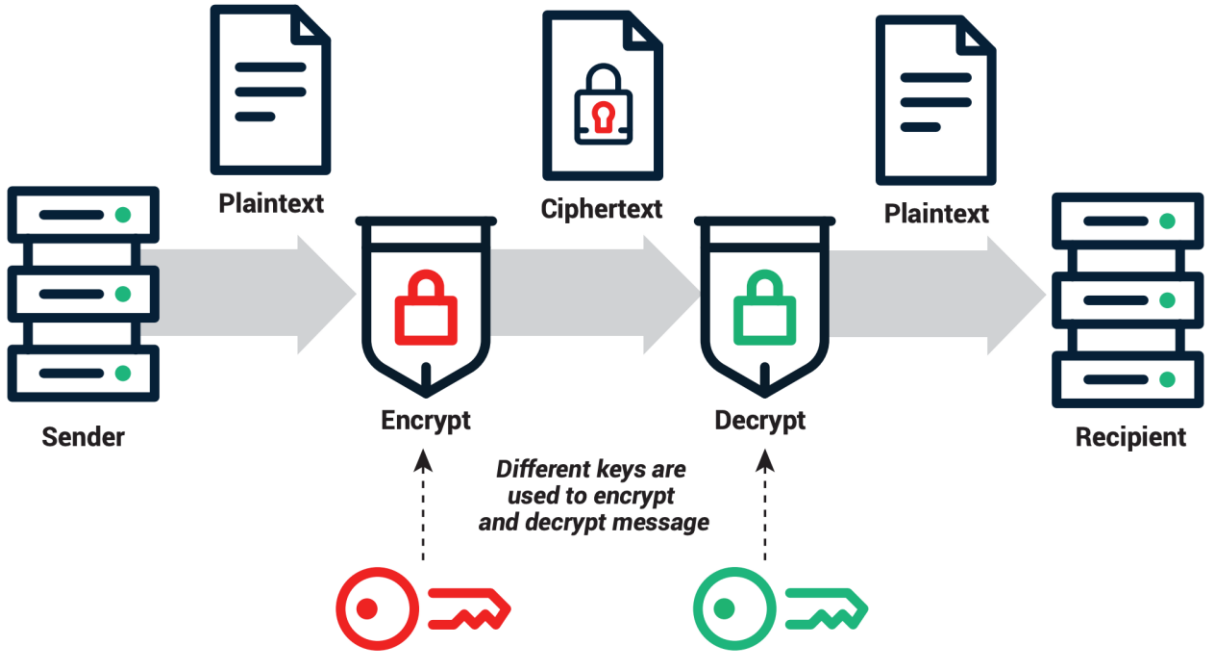
OIV Digital signals and networks

Introduction

- Croatian Quantum Communication Infrastructure(*CroQCI*)
- Part of European Quantum Communication Infrastructure(*EuroQCI*) initiative
- Quantum computing advances threaten the core mathematical foundations of global internet security (RSA, ECC, ECDH).
- Quantum Key Distribution (QKD)

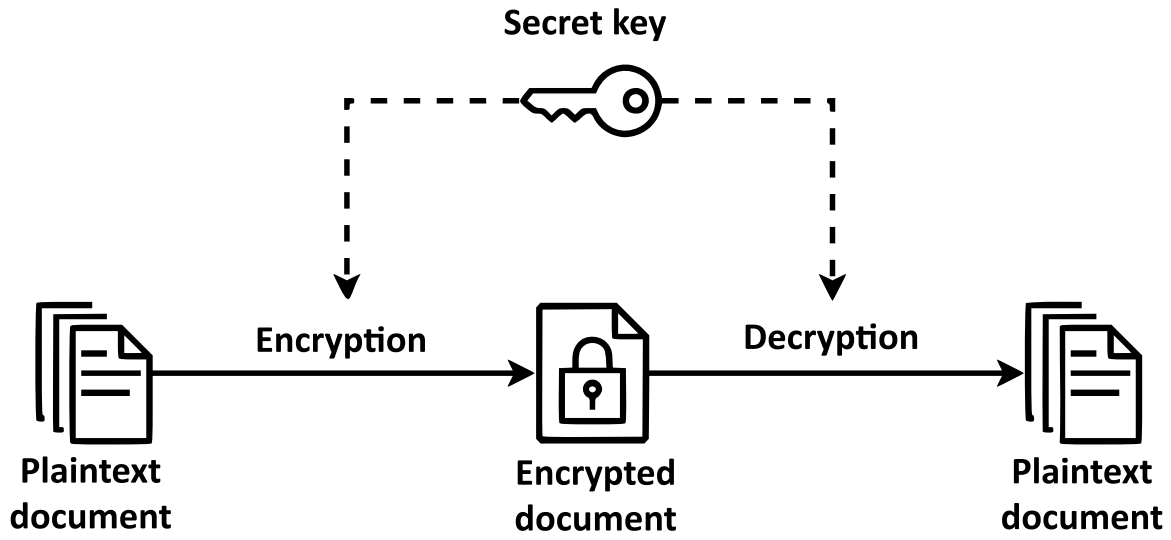
Asymmetric cryptography

- Known as Public Key Infrastructure(PKI)
- Asymmetric algorithms: RSA, ECC, DH, ECDH
- Based on complex mathematical problems that computers cannot easily solve 'backwards' (e.g., factoring enormous numbers into prime factors)

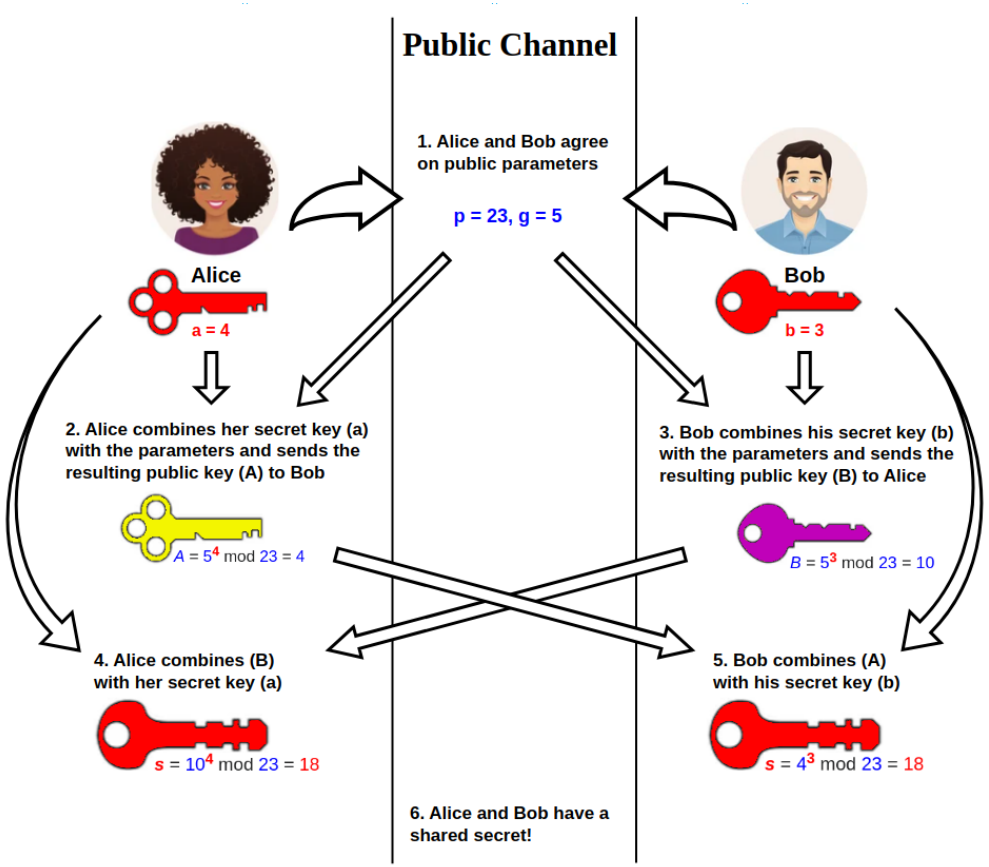


Symmetric cryptography

- Uses the same key for both encryption and decryption of data
- Symmetric algorithms: DES, 3DES, ***AES***, OTP…
- AES-256 accepted as a quantum-safe algorithm
- **Drawback:** Secure key distribution is difficult, as both parties must have the key before secure communication begins



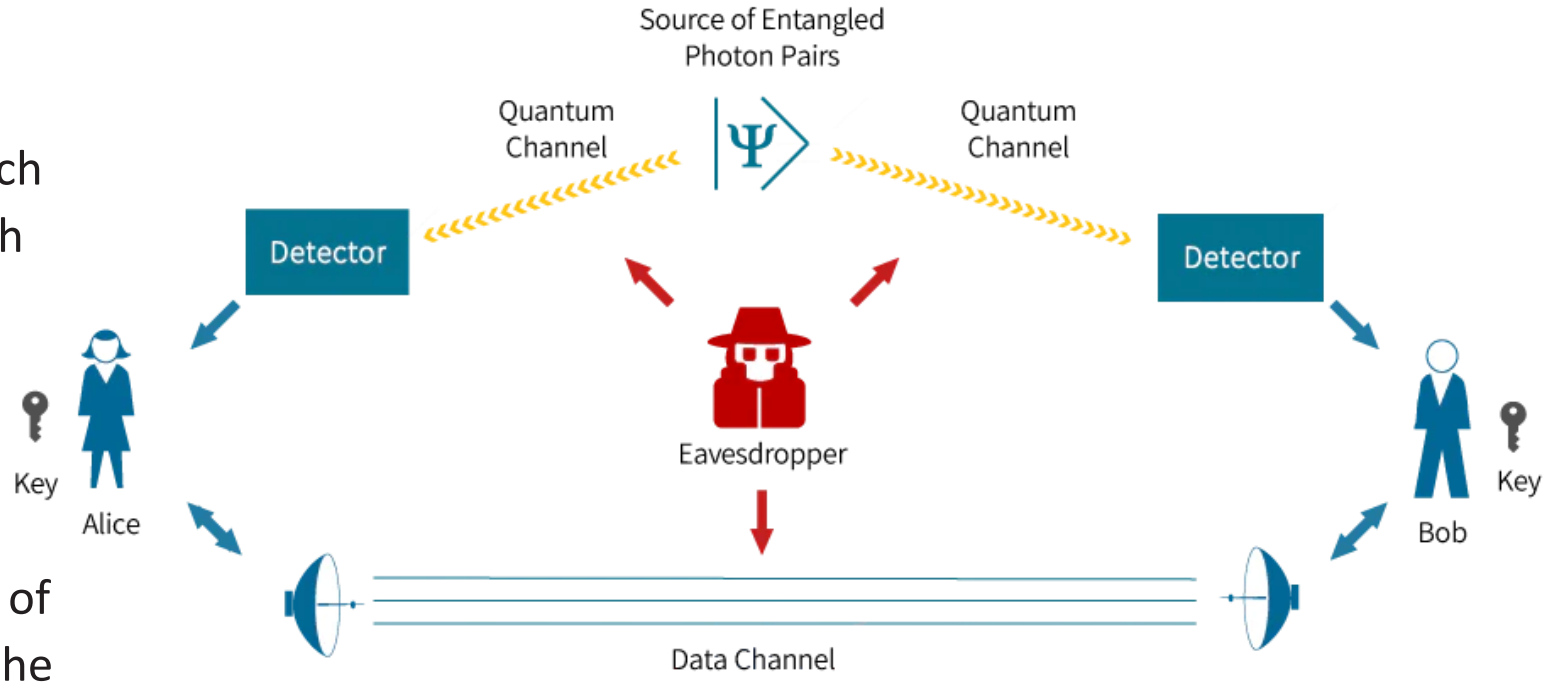
ECDH (Elliptic Curve Diffie-Hellman)



- **Key Agreement Protocol** that allows two parties, each having an elliptic-curve *public-private key pair*, to establish a shared secret over an insecure channel
- **Objective**: To securely? derive a cryptographic key without ever transmitting the key itself over the network.
- **Main Vulnerability**: Susceptible to Shor's Algorithm on future large-scale quantum computers (Quantum Threat)
- **Usage:** HTTPS/TLS 1.3, Signal, Whatsapp, iMessage …

Entanglement based QKD

- Pairs of photons are generated in such a way that the quantum state of each photon cannot be described independently of the state of the other
- Measuring one particle instantaneously influences the state of its entangled partner, regardless of the distance between them



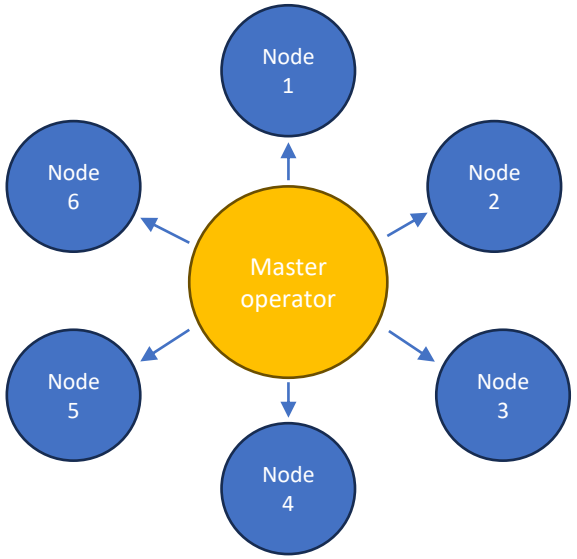
ECDH vs Entanglement based QKD

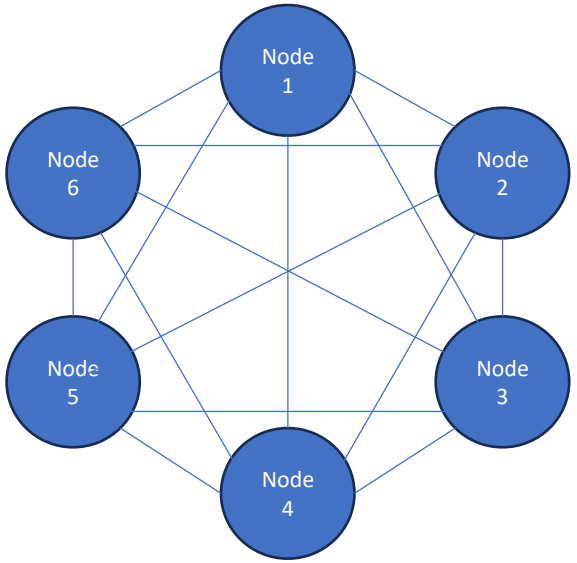
Feature	ECDH (Classical)	QKD (Entangled Photons)
Security Basis	Mathematical complexity (Elliptic Curves)	Laws of Quantum Physics
Quantum Resistance	**Vulnerable** (Broken by Shor's Algorithm)	**Immune** (Information-theoretic security)
Infrastructure	Standard Internet / Software-based	Specialized Fiber Optics / Satellites
Current Usage	Ubiquitous (HTTPS, Signal, VPNs)	Specialized (Military, Banking, Research)

CroQCI

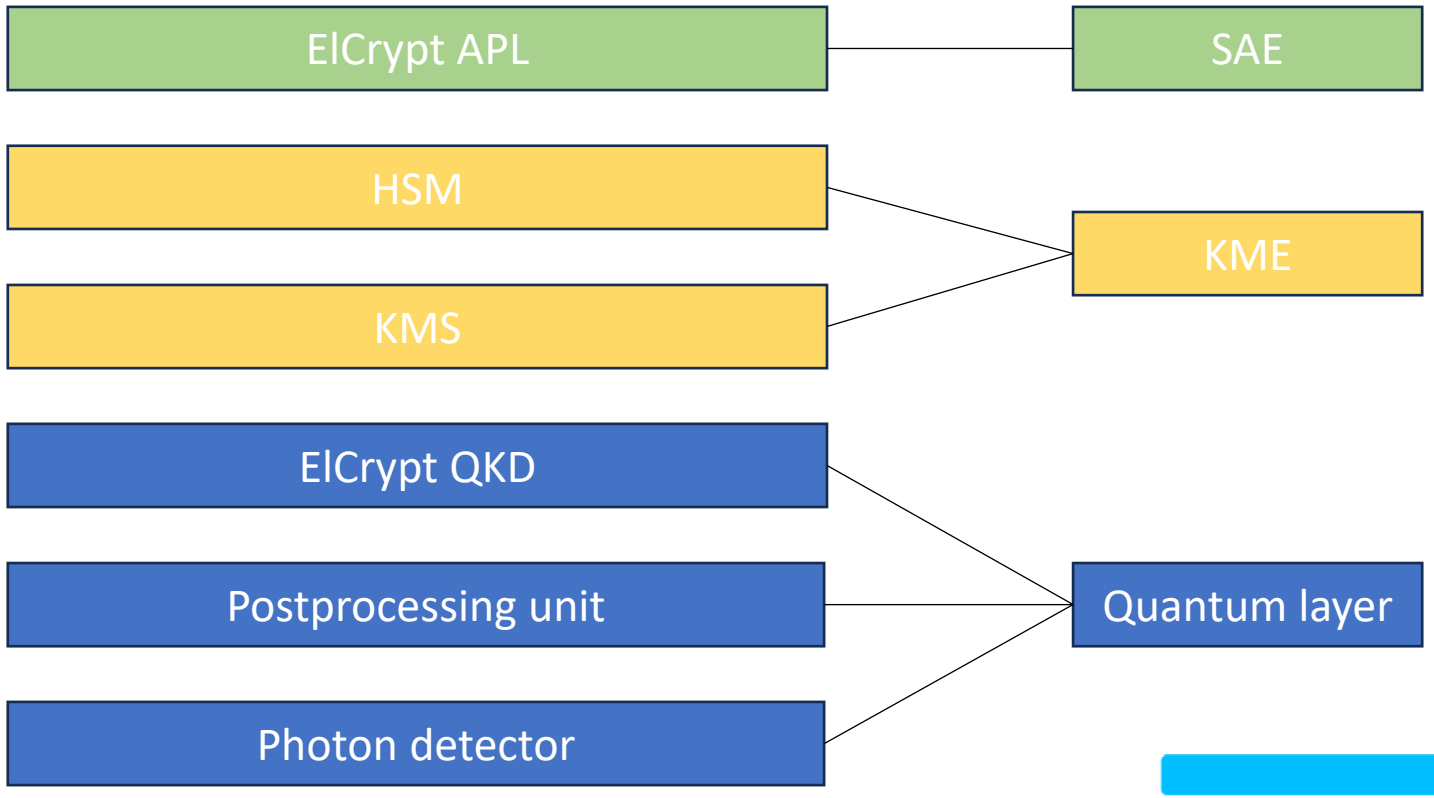
Experimental infrastructure:

- Six client nodes and master operator
- All users can generate keys for all combinations of pairs





CroQCI


ElCrypt APL
SAE
HSM
KME
KMS
ElCrypt QKD
Postprocessing unit
Quantum layer
Photon detector

Encryptors in CroQCI network

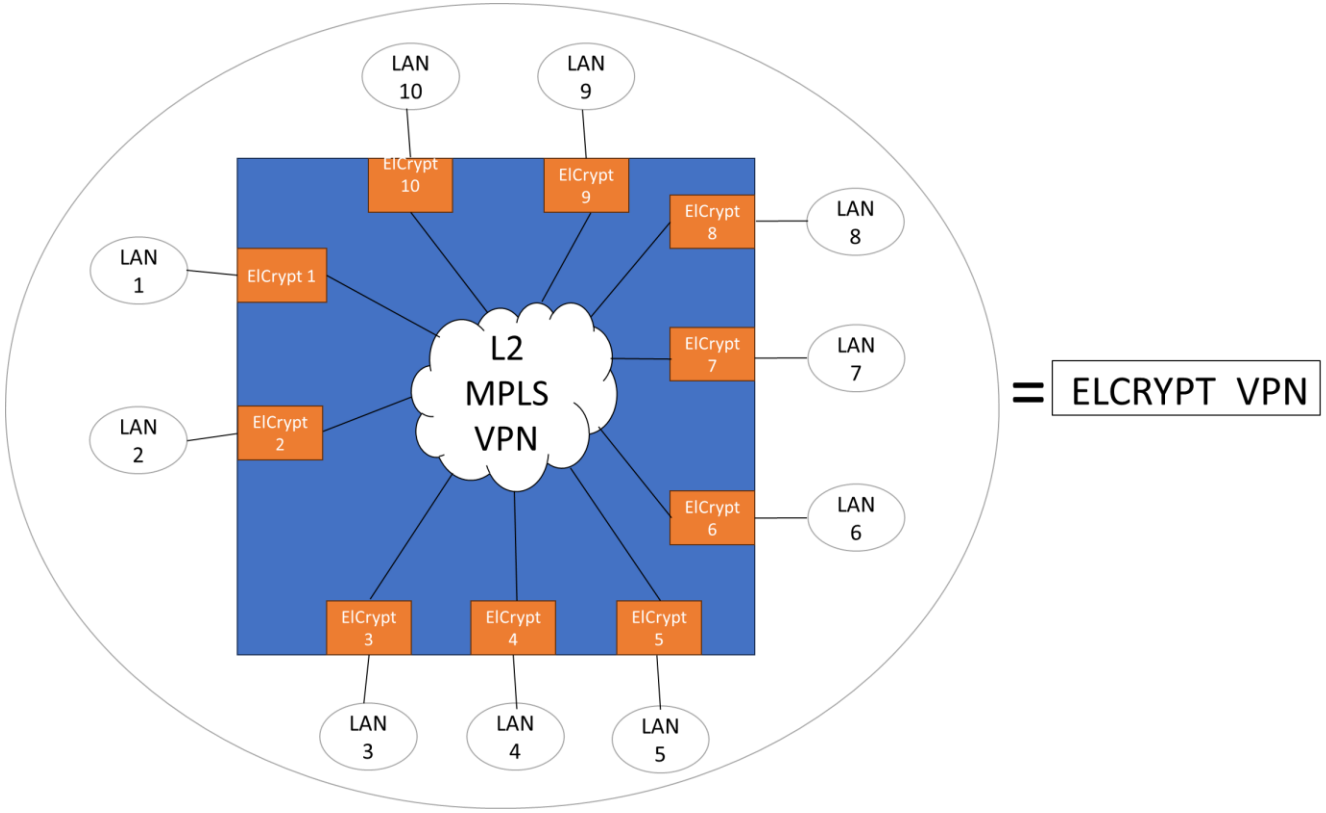
Usage:

- Real-time data encryption
- VPNs
- Quantum key distribution - QKD

Specifications:

- OSI L2 real-time data encryption in MESH network topology up to 20 links
- Hardware accelerated ***AES-256-GCM*** crypto algorithm
- Authentication based on GCM tags for every frame sent
- ETSI GS QKD 014
- Ethernet speed up to 10Gbps
- SFP+ interfaces

Encryptors in CroQCI network



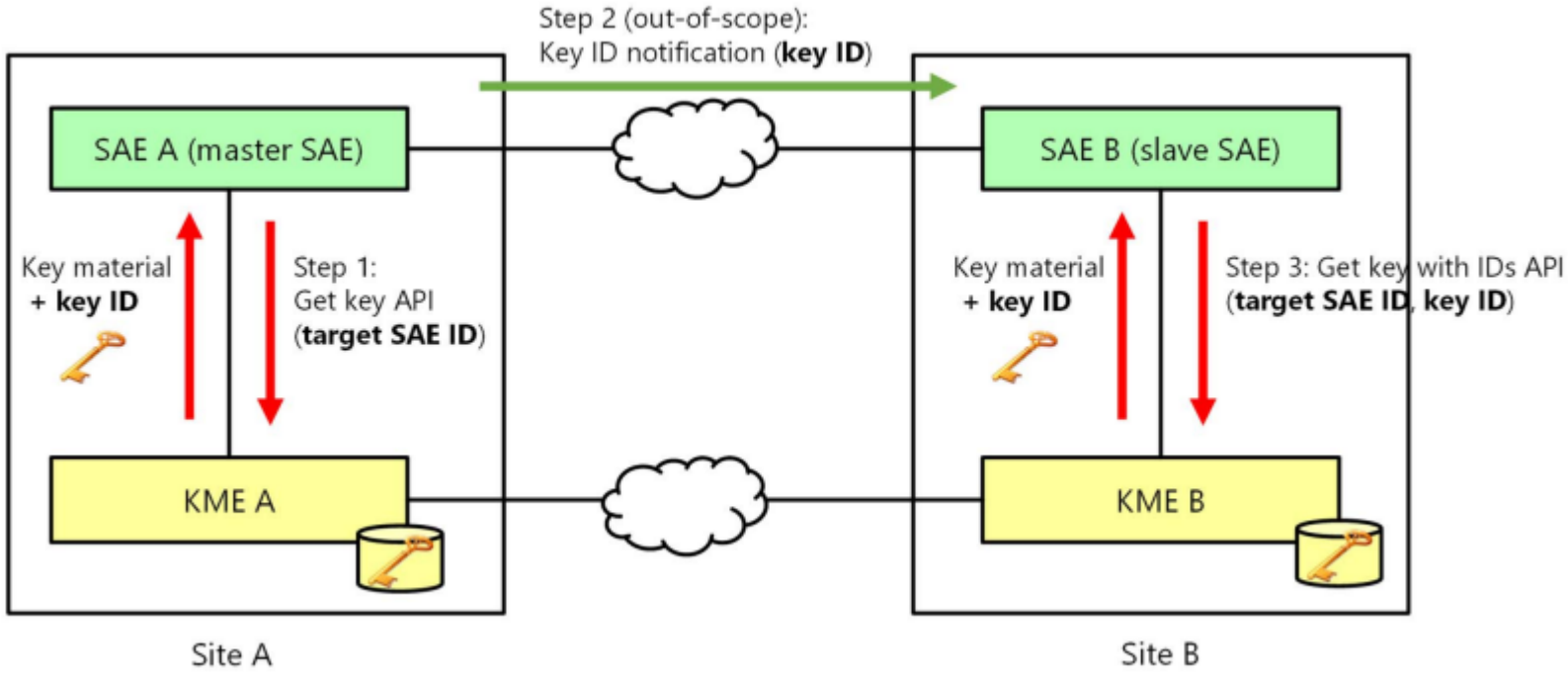
Example of application:

Hosts in LAN 1 and LAN 7 communicate with each other as if they belong to the same local area network

ETSI GS QKD 014

- **Industry Standard**: Developed by the European Telecommunications Standards Institute (ETSI)
- **Core Function**: Defines a standardized Key Delivery API
- **The Bridge**: Connects secure applications (SAE) with Quantum Key Management Systems (KMS)
- **Main Benefit**: Enables multi-vendor interoperability across quantum networks

ETSI GS QKD 014



Conclusion

- **The Vulnerability**
  - Modern public-key cryptography (RSA, ECC) will be broken by future quantum computers running Shor's algorithm.
- **The Immediate Risk: „Harvest Now, Decrypt Later”**
  - Adversaries are intercepting and storing encrypted data today, waiting to decrypt it once quantum hardware matures.
- **The Dual Defense Strategy**
  - **Post-Quantum Cryptography (PQC)**: Software upgrade replacing math problems with quantum-resistant algorithms (e.g., ML-KEM).
  - **Quantum Key Distribution (QKD)**: Hardware solution using the laws of physics to share unbreakable encryption keys

EuroQCI

REPUBLIKA HRVATSKA
Ministarstvo znanosti, obrazovanja i mladih

Funded by the European Union

CROQCI

Thank you for your attention!
Questions?

Duje Gašperov
Advanced IT Technologies and Software Development Senior Specialist Coordinator

OIV Digital signals and networks