
Securing video calls with QKD

Frederik Wedel-Heinen

Chief Cryptologist, Dencrypt

Agenda



Company and product
presentation



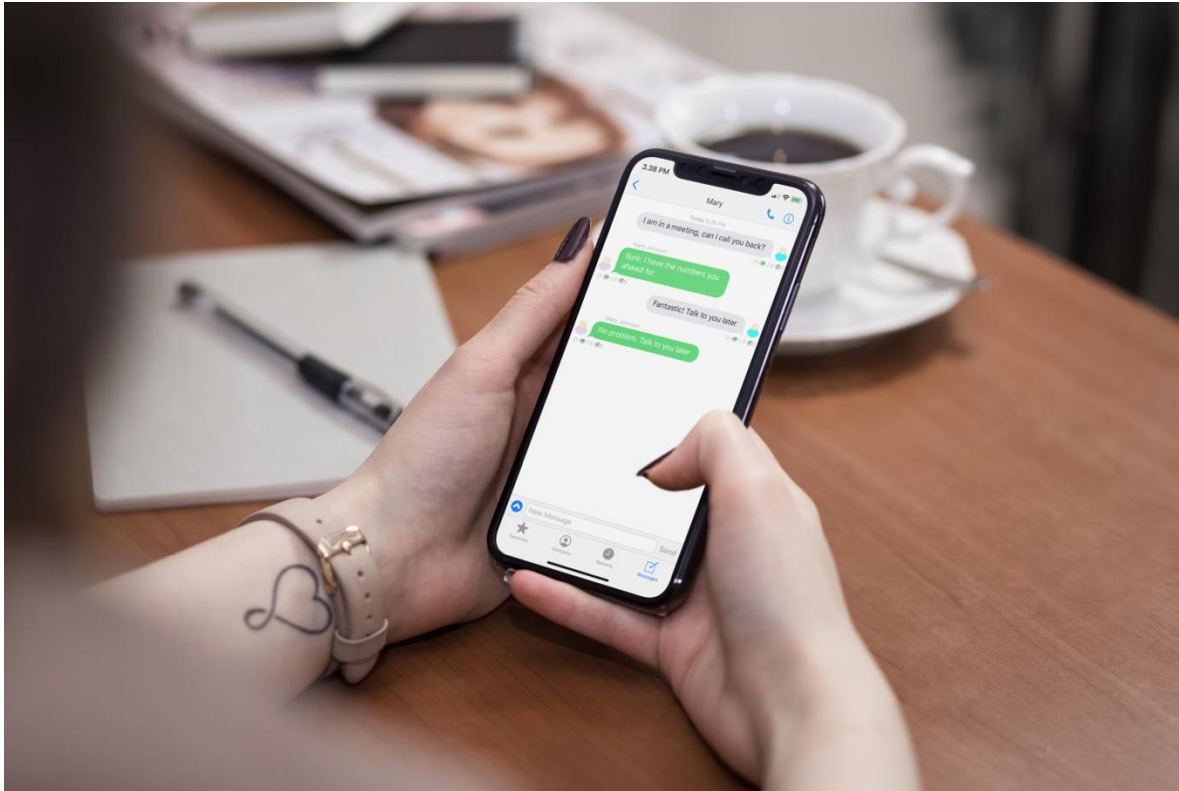
The CyberQ project

Dencrypt

- Founded in 2014
- Co-founder Lars Knudsen
- Dynamic Encryption
- 25 employees



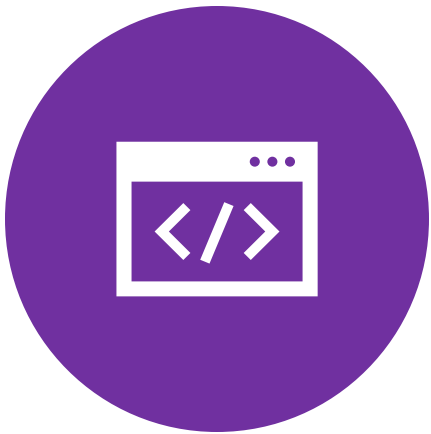
Product



Dencrypt Communication Solution:

- Instant messaging
- Audio and video calls
- Interoperability with third party systems (e.g. Pexip)
- Central administered phonebook
- Closed system (invite only)

Technologies



WEBSERVER (HTTPS)



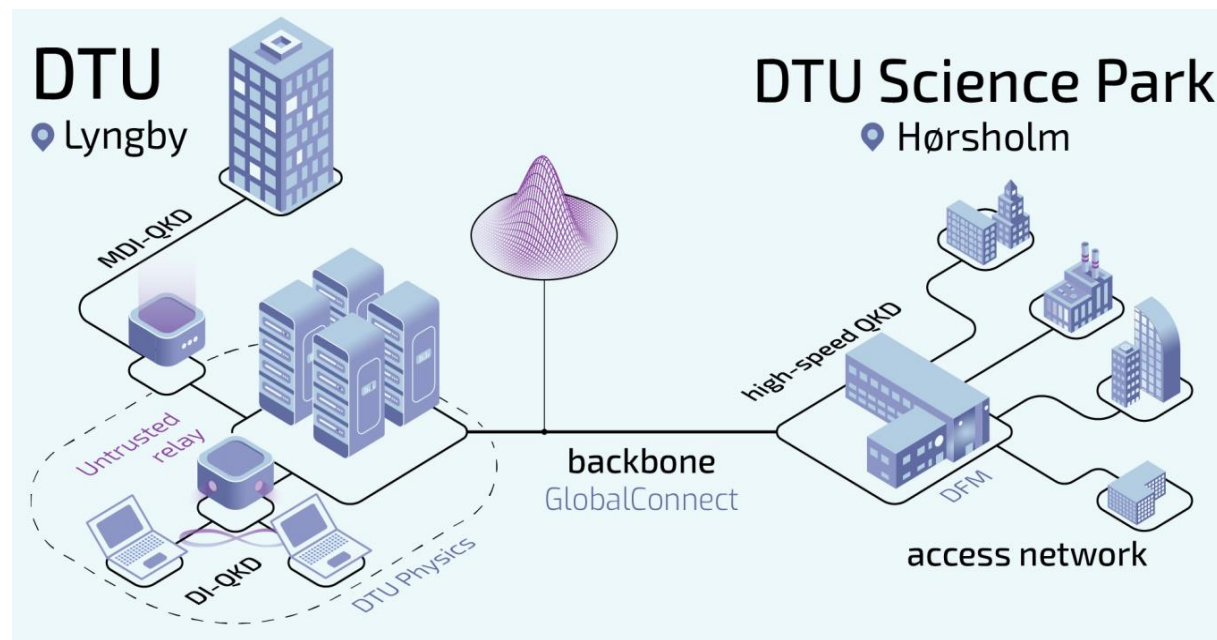
INSTANT MESSAGING
(X3DH, DOUBLE RATCHET)



AUDIO AND VIDEO CALLS
(DTLS-SRTP, SRTP)

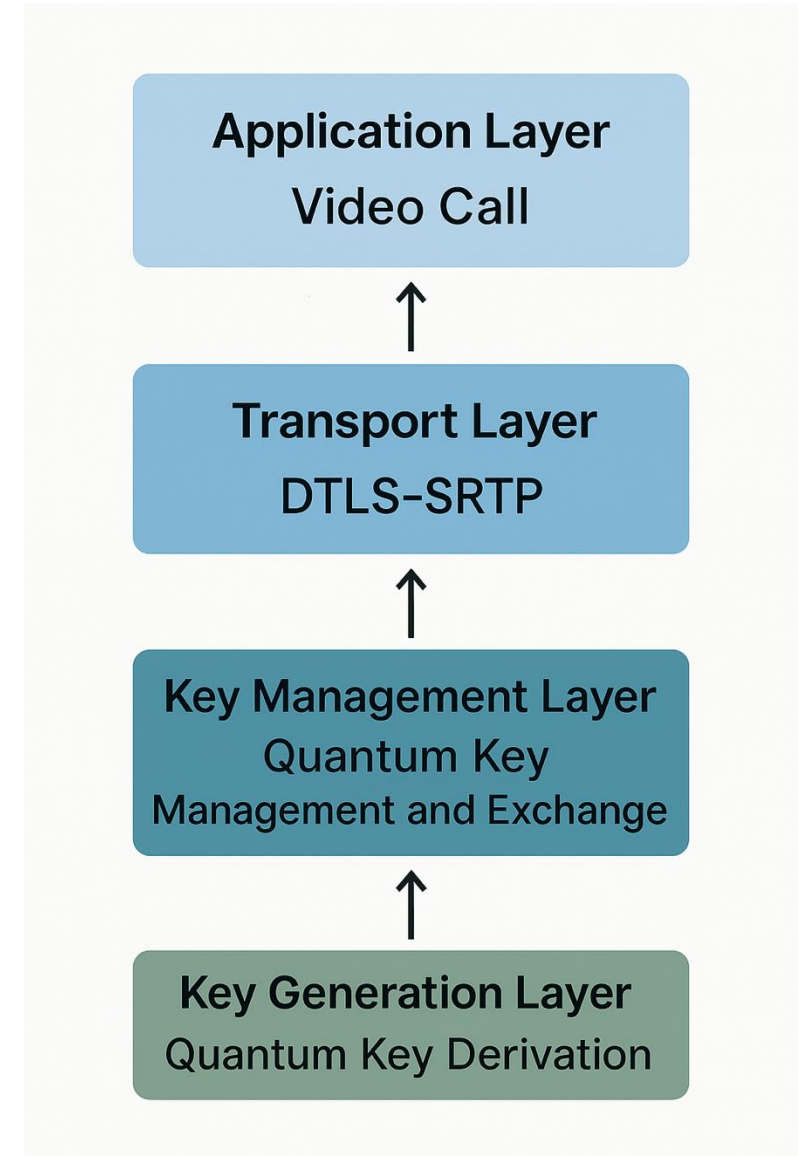
CyberQ research project

- Advancing squeezed light QKD
- Standardisation of calibration and verification of squeezed light QKD
- Establishing a network between two DTU sites
- Encrypted video call using QKD keys

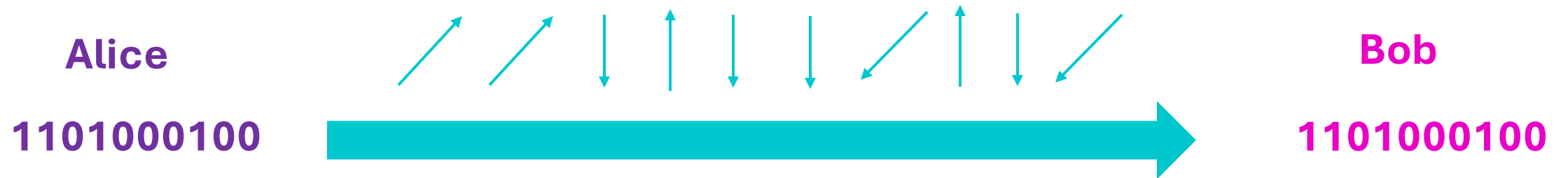


Partners: Dencrypt – GlobalConnect – Technical University of Denmark – Danish Fundamental Metrology – Ghent university – SiPhotonIC

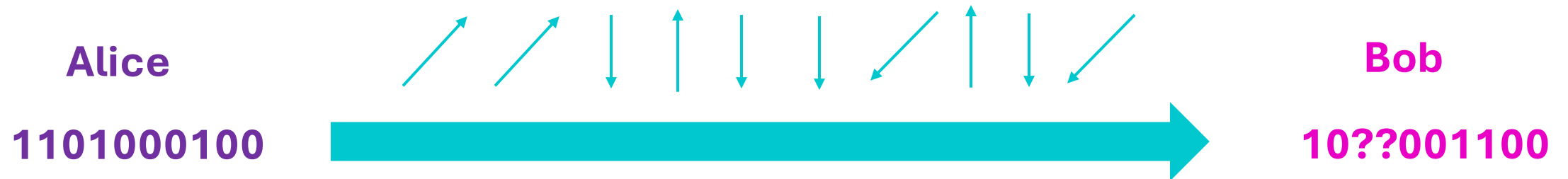
Encrypted videos



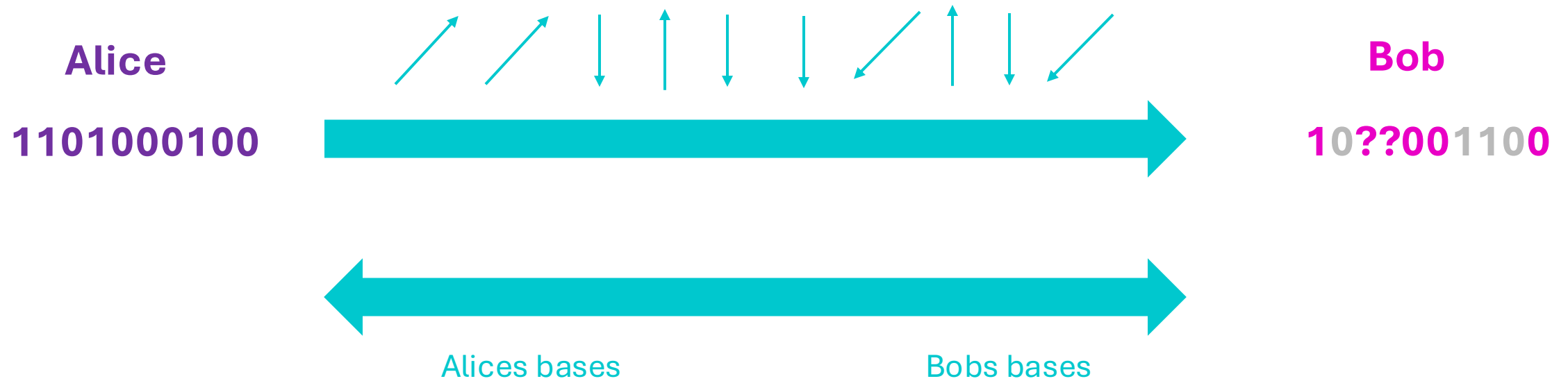
Quantum key derivation



Quantum key derivation



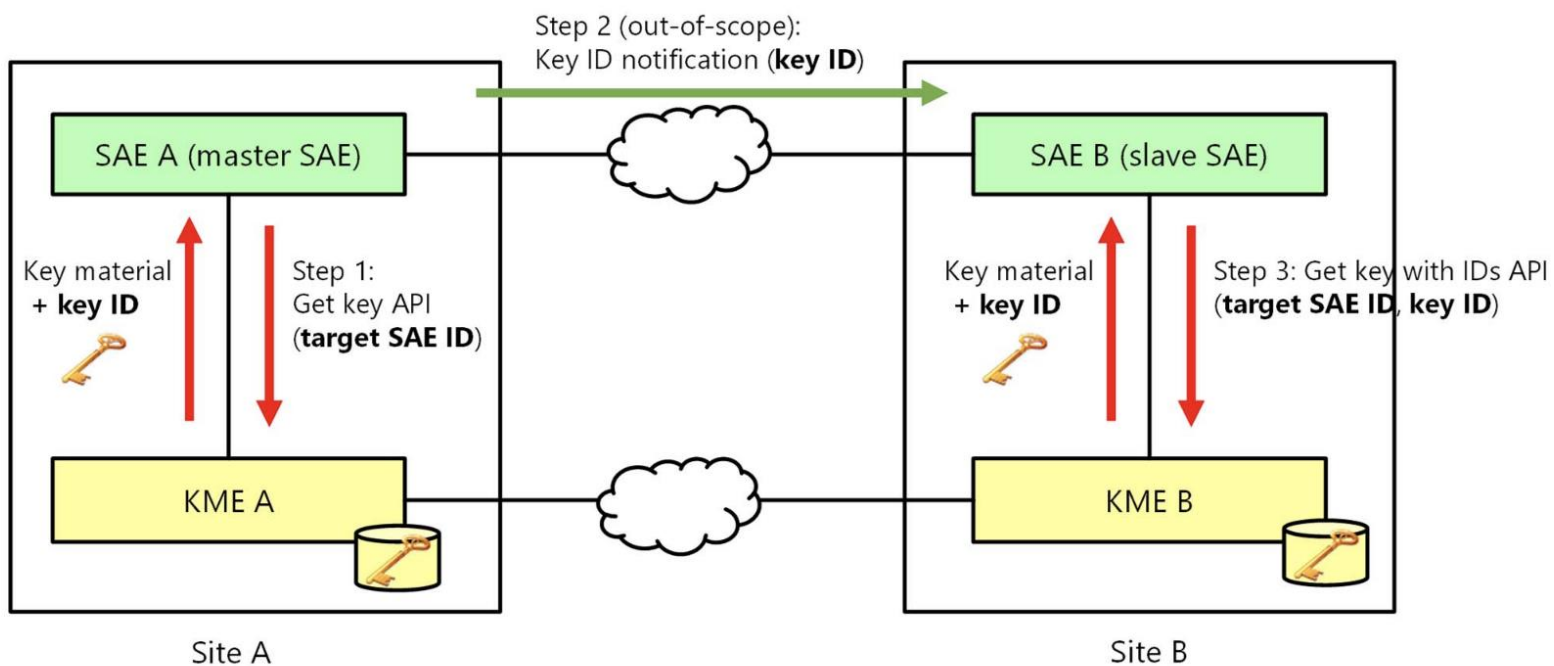
Quantum key derivation



Quantum Key Management and Exchange (QKME)



Quantum Key Management and Exchange (QKME)



Source: ETSI QKD GS 014

Quantum Key Management and Exchange (QKME)



Get key

https://{hostname}/api/v1/keys/{sae_id}/enc_keys



Get key with key ids

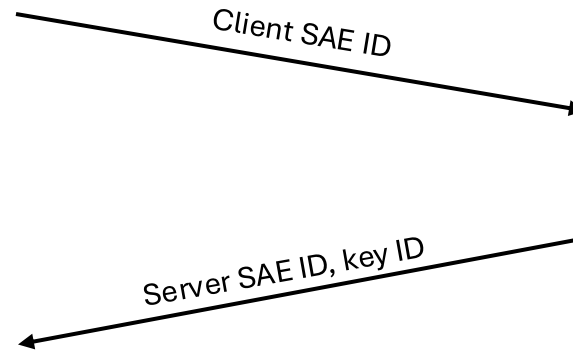
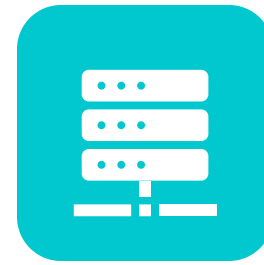
https://{hostname}/api/v1/keys/{sae_id}/dec_keys



Get status

https://{hostname}/api/v1/keys/{sae_id}/status

Integration with TLS/DTLS (KEM)



Integration with OpenSSL through providers

Provide local KME
configuration
(hostname, port, etc)

Check for missing
provider functionality

Performance/robustness
implications

Questions?