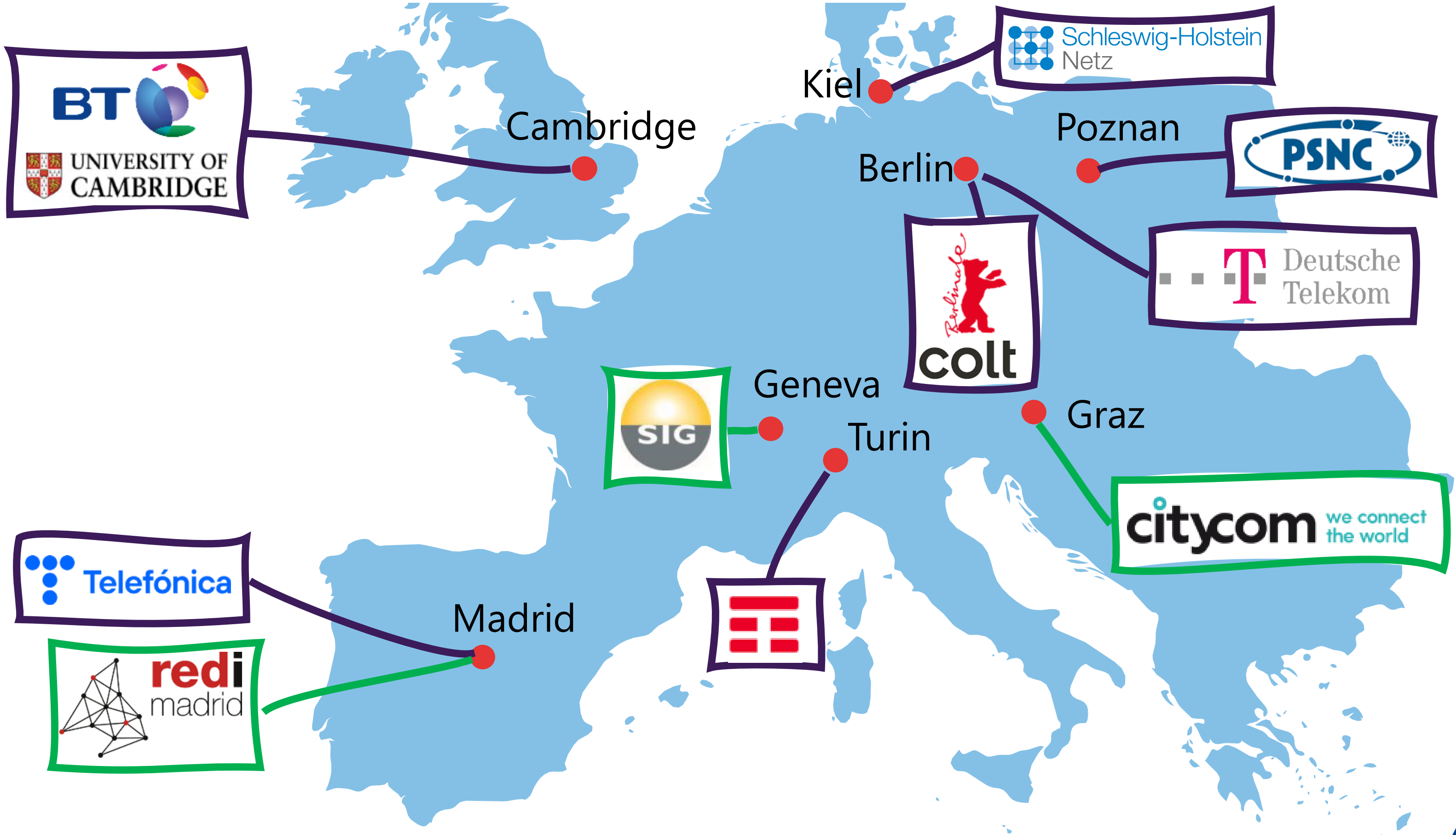
Practical deployment considerations for QKD systems

Jörg-Peter Elbers, ADVA

ECOC 2021 WS "Optical comms beyond 2020: Are we ready for the quantum age?", Bordeaux, 13 Sept 2021

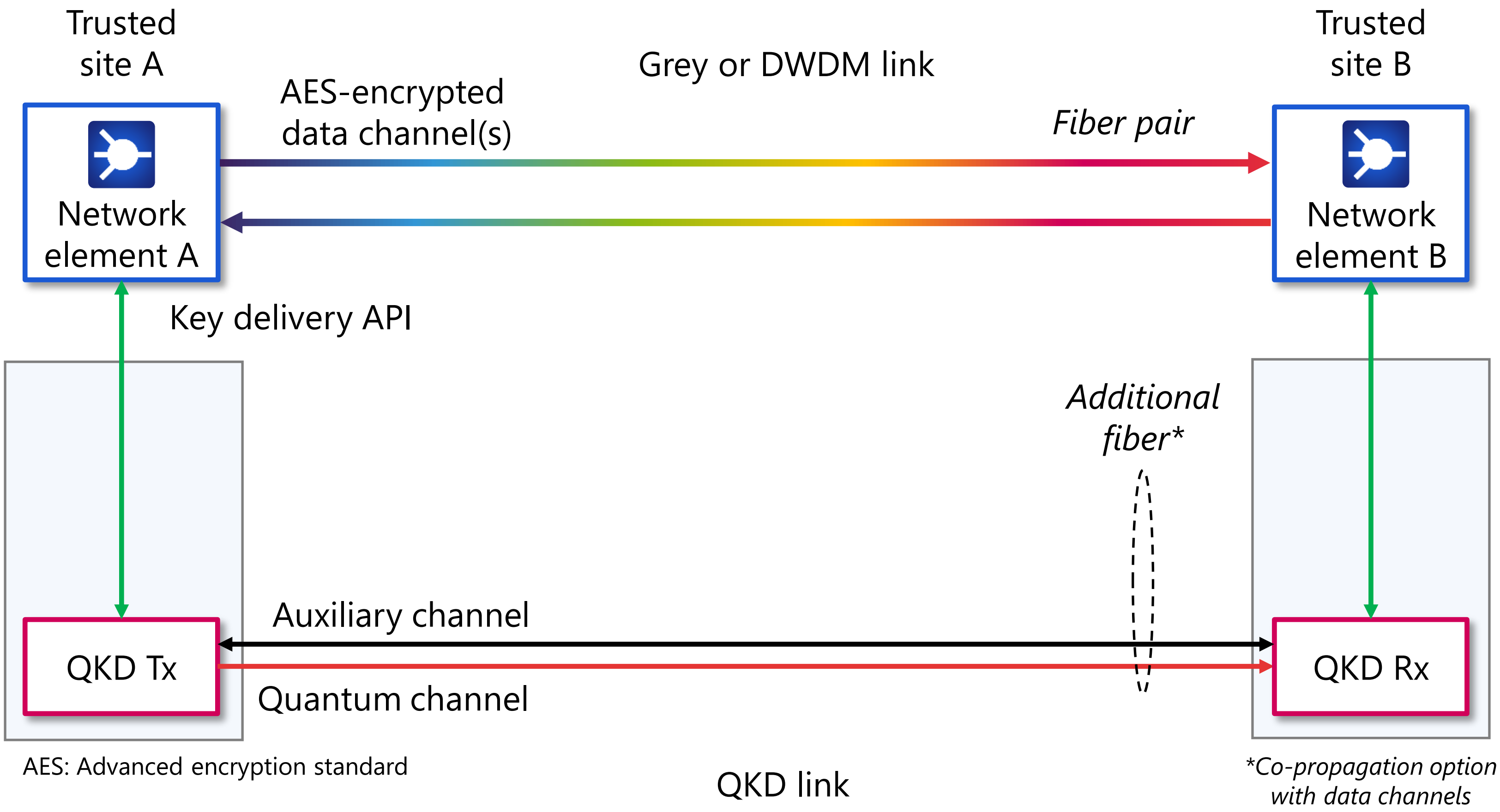
ADVA: Enabling QKD deployments

OPEN QKD



ADVA™

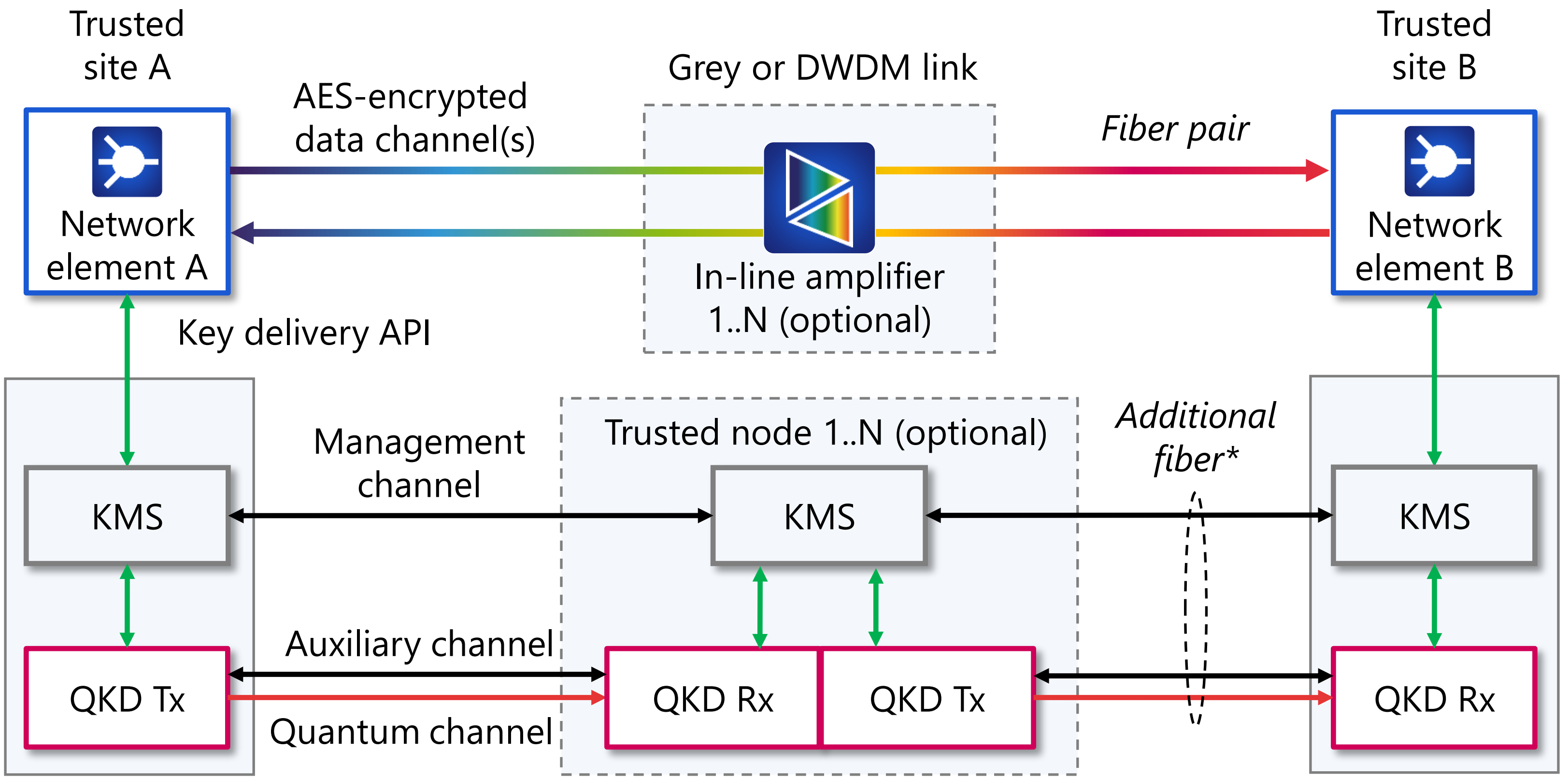
QKD is part of a larger network encryption solution …



AES: Advanced encryption standard

Co-propagation option with data channels

… and creates dependencies important to understand



AES: Advanced encryption standard
KMS: Key management system

QKD link

Co-propagation option with data channels

Deployment considerations & lessons learnt

- Record key rates are not needed. A few kb/s of secure key rate are enough[1]
- Compatibility with deployed fiber infrastructure is critical (patch panels, amplifier spacings, …)
- QKD link budget is often scarce. 25dB would be good to have
- Separate fiber for QKD is recommended. Bidi-WDM is easier than QKD co-propagation
- Stable, carrier-class operation and low-touch provisioning is (much) needed
- QKD complements PQC[2] and needs to be priced accordingly (expect <10k€ per TX/RX pair)
- Standardisation & security certification is required for wider market adoption
- Is there a market for a „QKD dark fiber" and/or a „quantum key distribution" service?

[1] Key refresh every 3Tbit for 2^{-60} attack success probability (A. Luykx and K. Paterson, 2016)

[2] Post-quantum cryptography, offering key exchange algorithms resistant to quantum computer attacks

Thank you

jelbers@adva.com

IMPORTANT NOTICE

ADVA is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.
The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.

With quantum computers network security is at risk

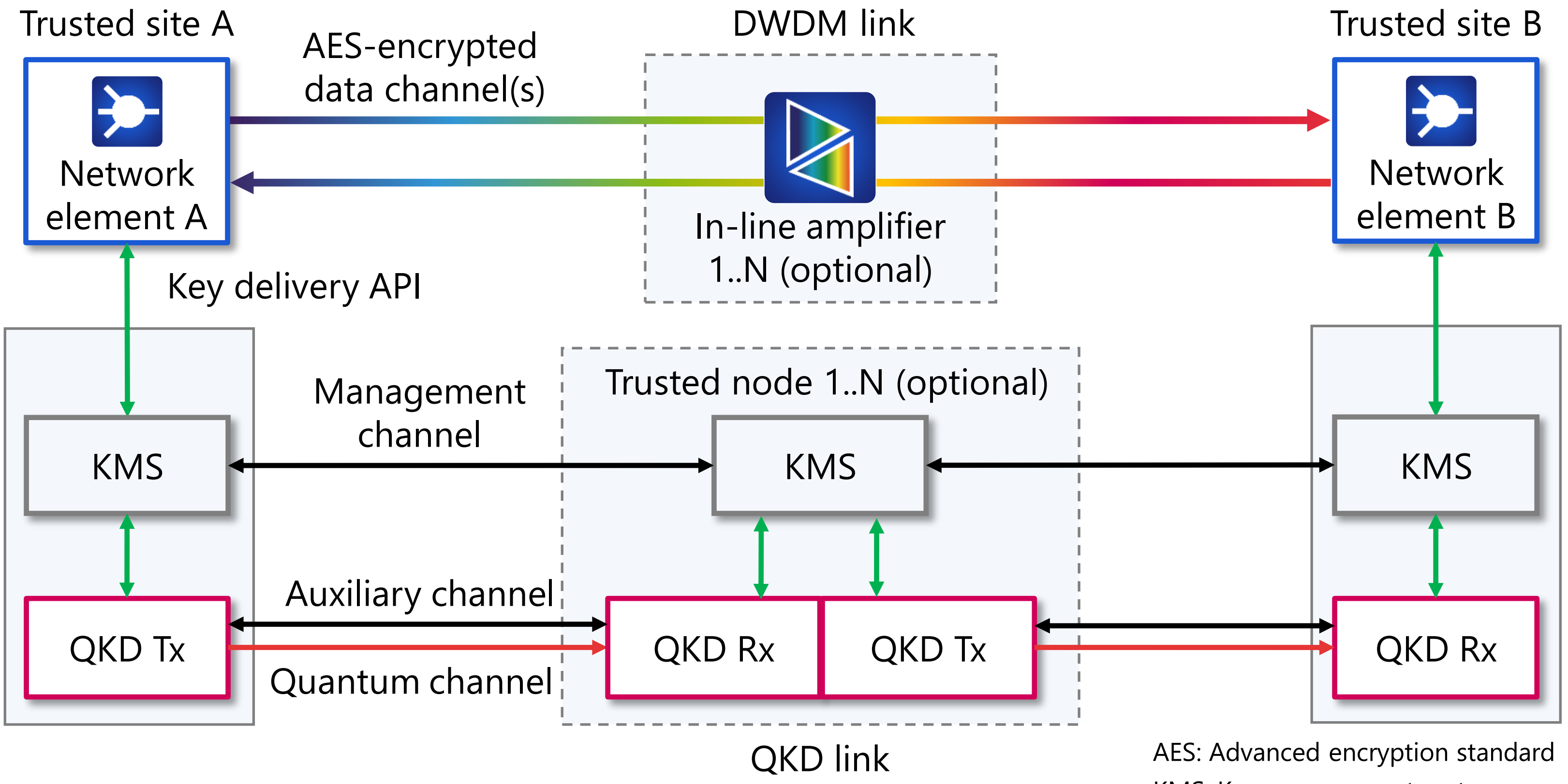
Key exchange is the weak link – options for quantum resistance:

Post-quantum cryptography (PQC)	Quantum key distribution (QKD)
Is based on hardened algorithms	Is based on laws of quantum physics
Works with any communication channel	Needs optical fiber or free-space media
Requires endpoint access on protocol level	Requires access to physical infrastructure
Is independent of optical link parameters	Depends on optical link parameters

First line of defense

Additional protection

Simplified setup



AES: Advanced encryption standard
KMS: Key management system