How to efficiently Test & Qualify QKD Solutions

Gert Grammel
ggrammel@juniper.net

JUNIPER NETWORKS | Driven by Experience™

What is it that we need to Validate?

Starting point: Eavesdropping Detection in BB84 Quantum Key Distribution Protocols

The nature of quantum mechanics provides us with an opportunity to statistically detect eavesdropping in quantum key distribution (QKD) protocols, which is unimaginable in classical digital communications. By utilizing Hoeffding's inequality, this study analyzes the upper bounds of the false-positive ratio (FPR) and false-negative ratio (FNR) of eavesdropping detection in the Bennett–Brassard-84 (BB84) QKD protocol, where eavesdropping is detected if the measured quantum bit error rate (QBER) is equal to or higher than a threshold.

Black Link Model

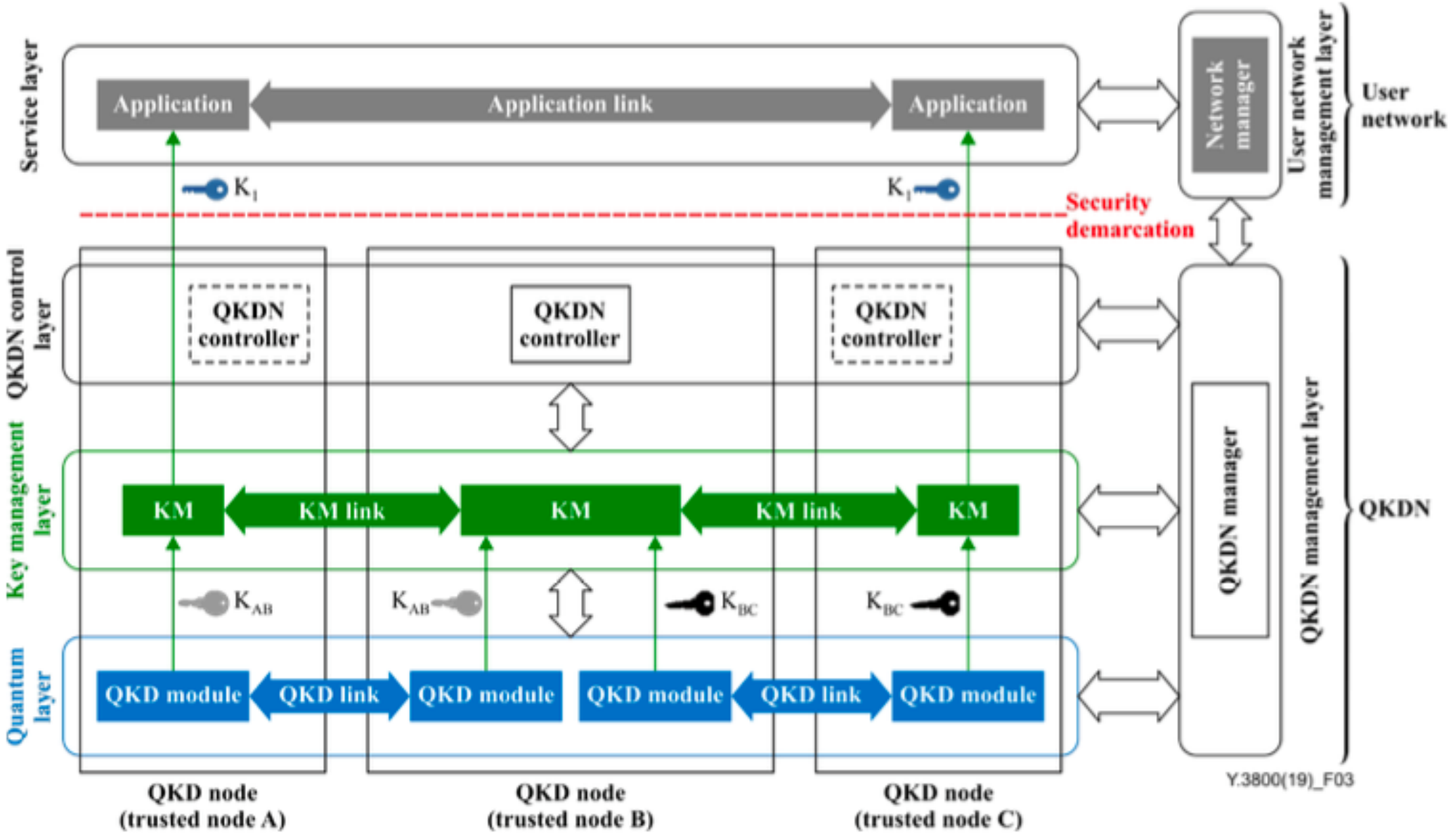
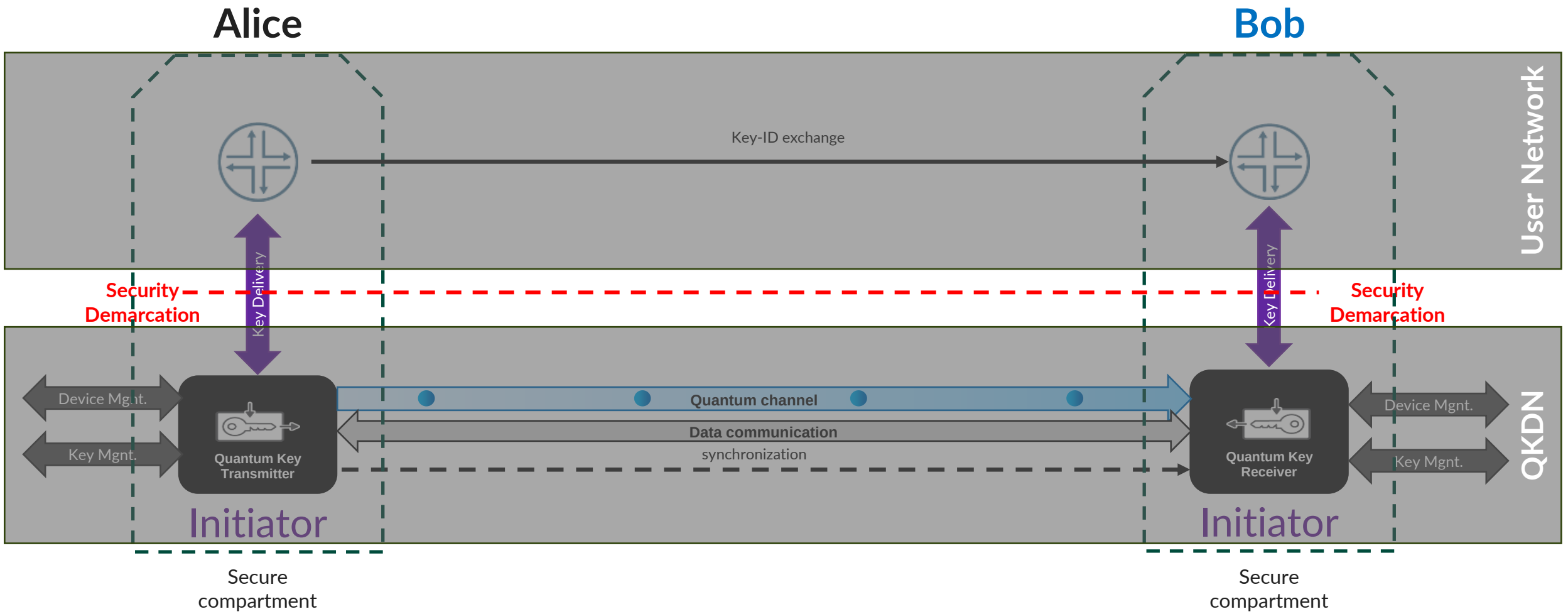


Figure 2: Conceptual structure of a QKDN as in ITU-T Y.3800 [1].

Y3800 “Black-Link” Model



Y.3800 Black-Link Model

- ITU-T Y.3800 is based on logical entities and identifies a single security demarcation
- ITU-T Y.3800 shows QKD/KME related entities without security demarcations despite the interfaces are accessible outside secure compartments
- ITU-T Y.3800 describes that a QKD link consists of the following channels but doesn't detail the security impact:
  - A quantum channel for the quantum communication stage and
  - a classical channel for the post-processing stage.
  - an additional synchronisation channel is used to synchronise and reference the quantum signals in the quantum channel between QKD-Tx and QKD-Rx.
- The service Layer is outside the QKD/KME architecture but implementation issues of key-ID communication *may* expose valuable data to an attacker too.

A Black Link Model hides Implementation details and does NOT allow to efficiently validate whether the implementation is secure.

Black Box Model

- 1 2 Key Exchange Interface
- 3 4 QKD production Interface
- 5 6 Key Management Interface
- 7 8 Device Mgnt Interface
- 9 10 VPN Service Interface

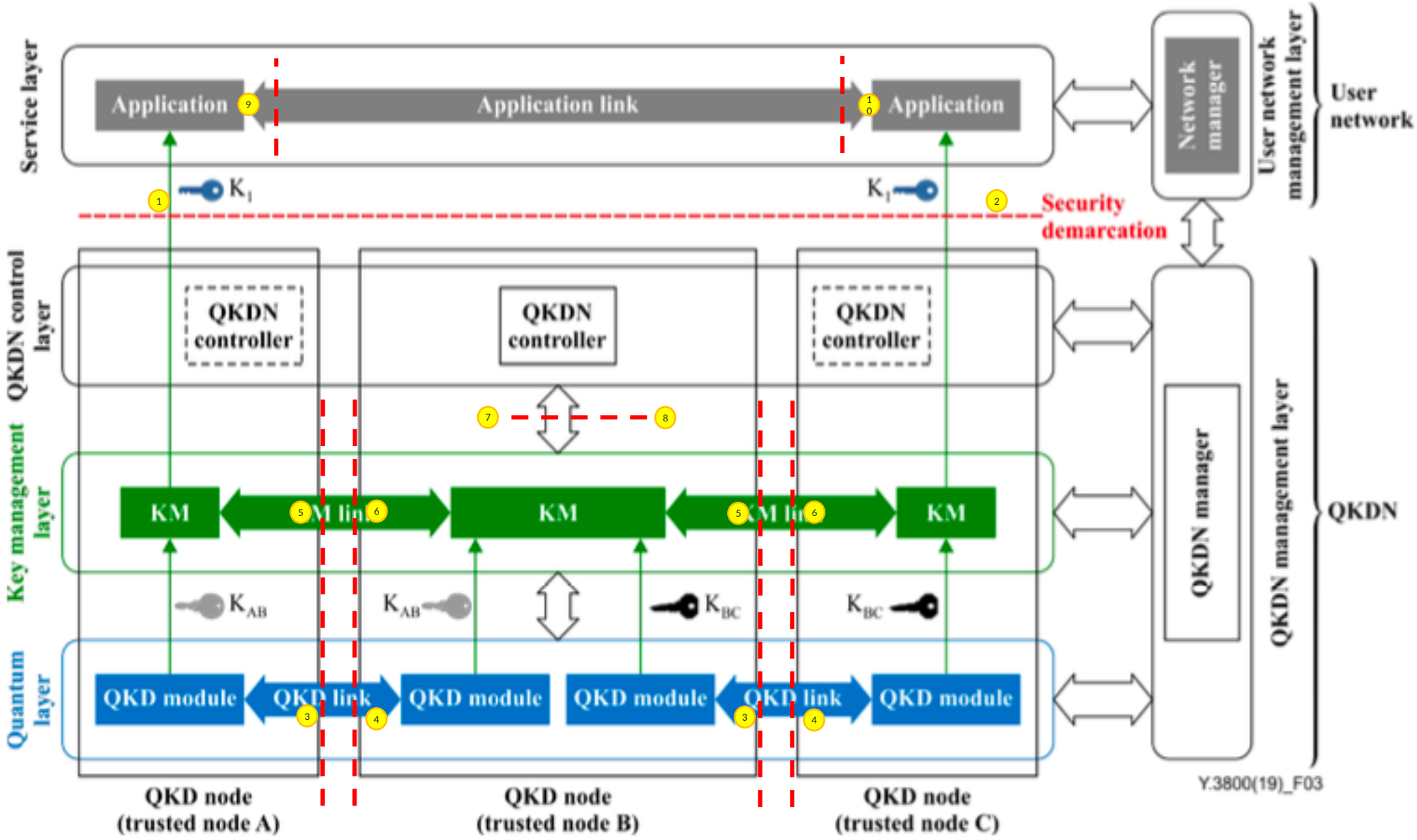
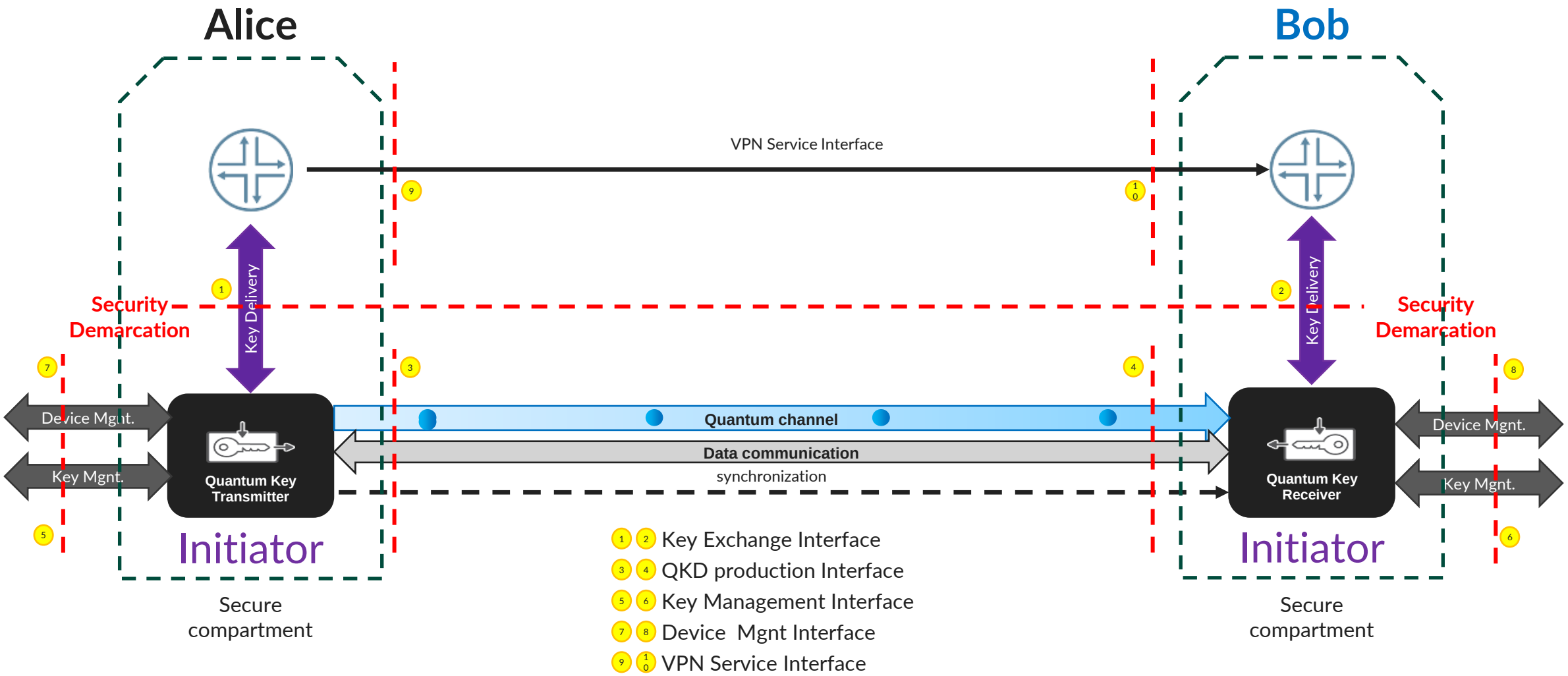


Figure 2: Conceptual structure of a QKDN as in ITU-T Y.3800 [1].

Y3800 “Black-Box” Model



Black-Box Model

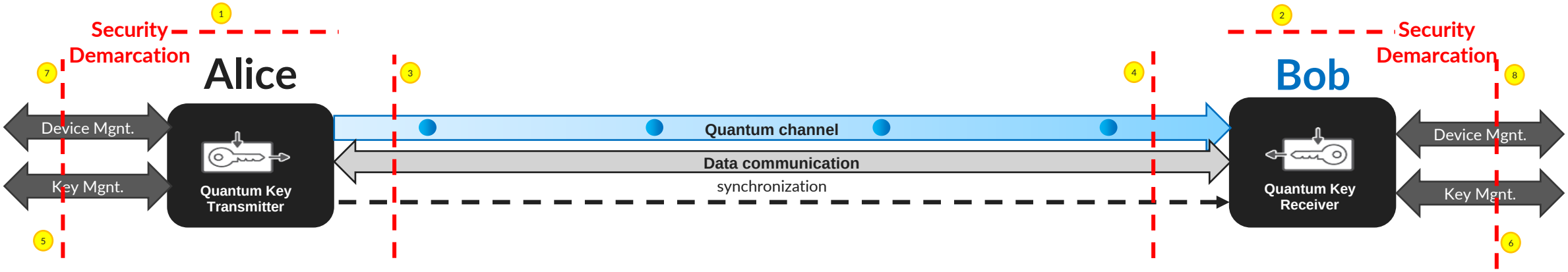
- The Black-Box model considers a physical entity to be a “Black Box” and all Interfaces to that black box need to be secured and validated.
- The Black-Box architecture MAY consider QKDN and Application as a single solution, identifying interfaces and their protection needs.

A Black Box Model exposes Implementation details at external interfaces and allows to efficiently validate whether the implementation is secure.

What are Attack and Prevention Mechanisms in QKD?

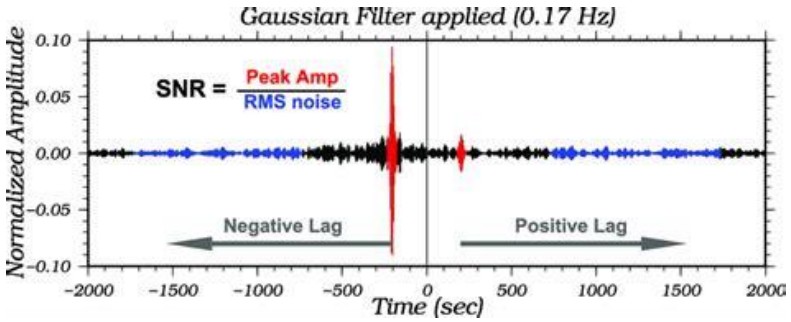
1. Photon-Number-Splitting Attack
2. Intercept-and-Resend Attack
3. Faked-state Attack
4. Decoy-State Method to detect PNS Attacks

Validating Attack resistance and detection need to look at all the components of the Quantum Channel



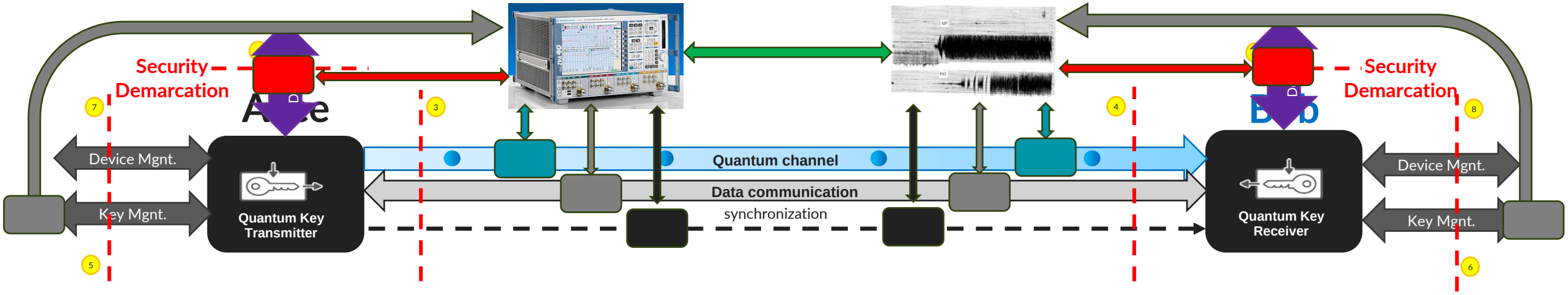
Black Box Models benefit from vendor-agnostic Standardization

1. Definition of how to measure Noise and QBER
2. Definition of how to measure the Signal
3. Definition of how to determine the Signal quality
4. Defined way to perform attacks
5. Defined Monitoring points and monitoring parameters for early detection of attacks
6. Defined threshold levels to protect against interference
7. Defined functionality e.g loopback, test-modes, boundary testing
8. Measurement equipment providing above functionality as neutral 3rd-party implementation



Benefits of standardization and Black-Box Model

- Well defined self-test functionality allows to quickly assess baseline functionality and performance
- Attack vector testing can be automated and reproduced
- Standardized Test and performance measurement enables to develop vendor-neutral 3rd-party Test equipment needed for validation
- Standardized performance measurement enables a market for product sub-modules that can be independently tested and validated in a well defined manner for quality assurance



Summary

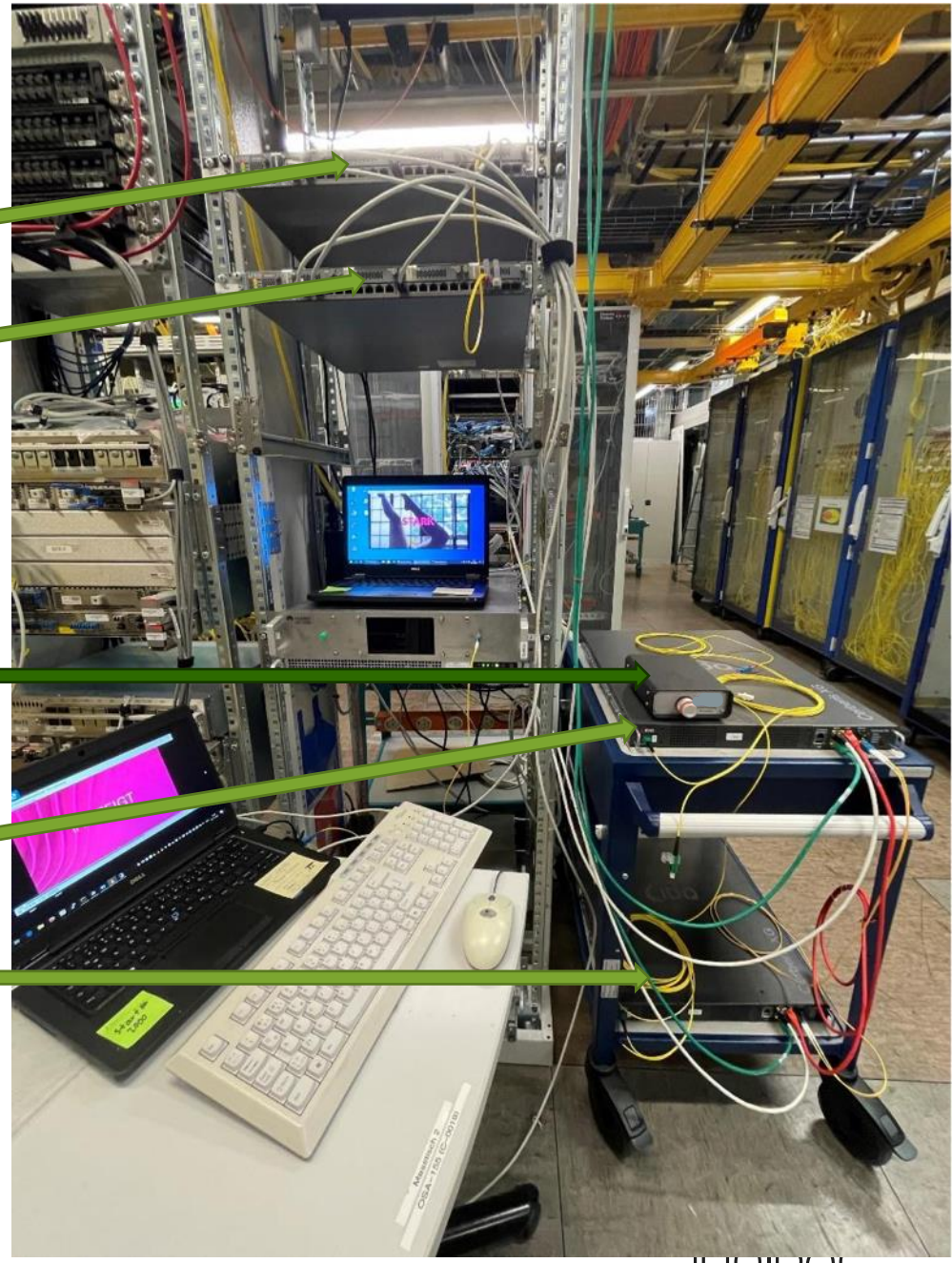
- Black-Link models are designed to describe a functional model:
  - hiding information within layers and expose Layer-crossing
  - do not discriminate between (protected) internal interfaces and vulnerable external interfaces
  - Standardized multi-vendor Test Equipment is hard to achieve
- Test&Validation of QKD systems require a Black-Box Model with well defined
  - Parameter definitions and associated Measurement methods
  - Performance property definitions
  - Test-Attack scenarios
  - Standardized Interface functionality: Protocols, Parameters, Selftests
- Efficient test & Validation relies on the availability of vendor-neutral Test equipment that is applicable to the majority of implementations

Quantum Key Distribution at Deutsche Telecom with Juniper and IDQ in 2021

Alice and Bob
2* Juniper SRX

Eavesdropping simulation device

QKD-Tx & QKD-Rx



Juniper Networks | Driven by Experience™