# DEUTSCHE TELEKOM SECURITY GMBH

Support for QKD device evaluations:
The Protection Profile for Prepare and Measure Quantum Key Distribution Modules
Dr. Lars Hanke
ITU Workshop on Quantum key distribution protocols, security and certification
Singapore 8 November 2022

ERLEBEN, WAS VERBINDET.

# COLLABORATIVE WORK

- PP sponsored and contributed to by German Federal Office for Information Security (BSI) [ M.Lochter, T.Hemmert, S.Reinhardt, D.Fischer ]
- PP initiated and contributed to by ETSI ISG QKD [ M.Ward (Toshiba), N.Lütkenhaus (U Waterloo) ]
- PP authored by Deutsche Telekom Security [ L.Hanke, G.Wicke, D.Zawadka ]
- Currently under evaluation by SGS Brightsight

Further contributors through ETSI ISG QKD comments

- Deutsche Telekom
- Huawei
- ID Quantique
- NICT
- OHB
- Rohde & Schwarz
- Télécom Paris
- Toshiba
- and still more contributors

# WHAT IS CC?

ERLEBEN, WAS VERBINDET.

# CC - A METRIC FOR SECURITY ASSURANCE

## Information Theoretic Security

- **The predominant view towards security in the QKD community builds on security proofs**
  - mathematical proof
  - based on assumptions
  - based on a mathematical model of the device and its environment
  - may be composable, but
  - does not adapt easily to modified assumptions
- **provides a precise figure for the remaining risk (aka ε)**

## Practical Security

- **Real implementations never match any model, ideally**
- **Attacker may use unforeseen methods to probe the physical implementation i.e., by-pass assumptions of the security proof**
  - probe components, which generate, prepare, or measure quanta
  - attack the device controller
  - analyse emanations of components or the controller
  - modify the device
  - etc.
- **Risk owner needs assurance that the implementation reasonably matches the model for the security proof**

# CC – A METRIC FOR SECURITY ASSURANCE

The common metric of a contemporary evaluation comprises:

**Criteria**

- Common Criteria (CC)
- The current version of CCMC is 3.1/Rev. 5, https://www.commoncriteriaportal.org
- ISO/IEC 15408

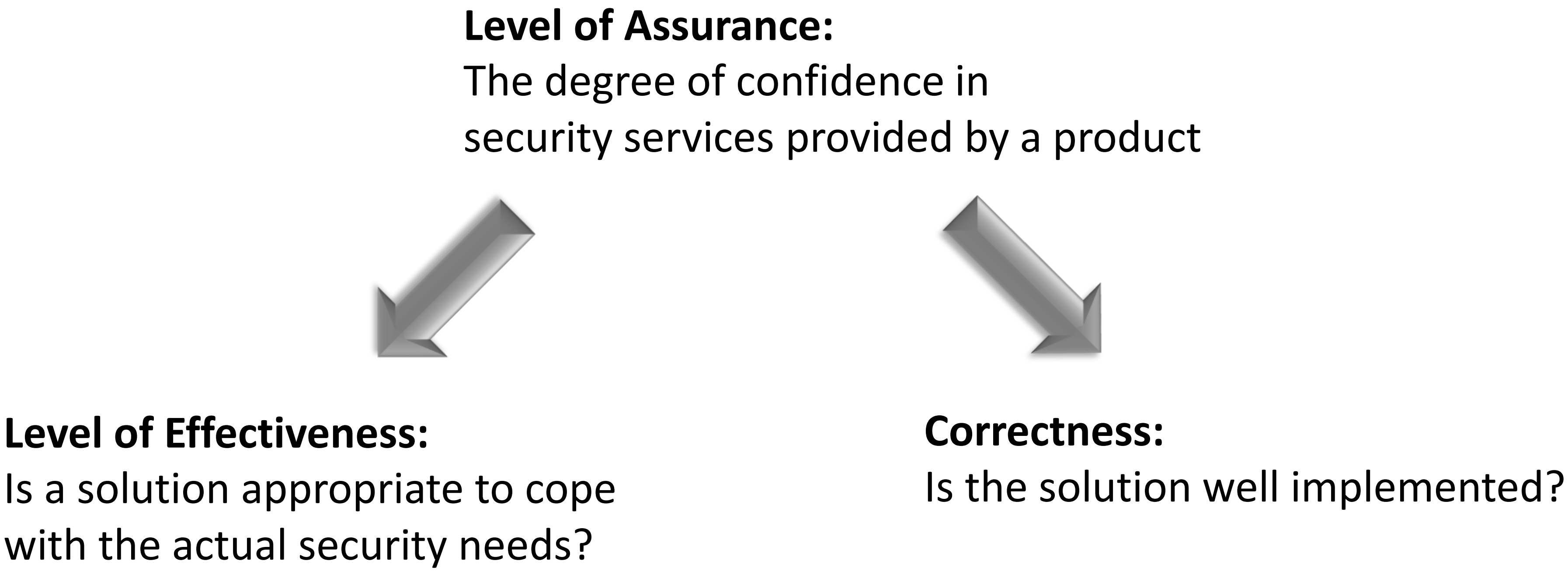
**Methodology**

- CEM according to the relevant CC version

**Interpretations**

- International: CCMC (CC Management Committee)
- European (SOGIS): JIL (Joint Interpretation Library)
- National: Particular national interpretations of the evaluation scheme

# CC – A METRIC FOR SECURITY ASSURANCE

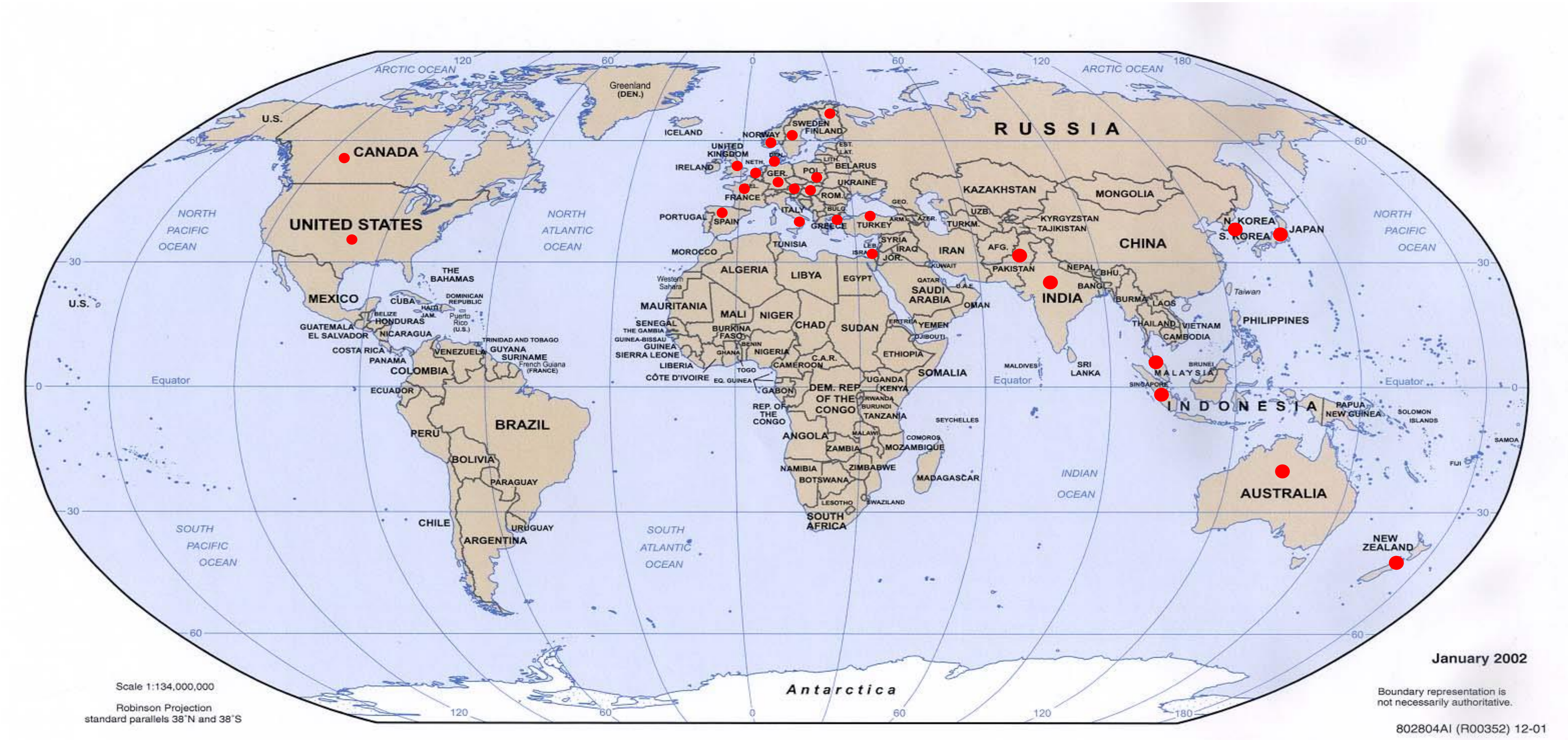


**Level of Assurance:**
The degree of confidence in
security services provided by a product

**Level of Effectiveness:**
Is a solution appropriate to cope
with the actual security needs?

**Correctness:**
Is the solution well implemented?

# CC – A METRIC FOR SECURITY ASSURANCE



Scale 1:134,000,000

Robinson Projection
standard parallels 38°N and 38°S

January 2002

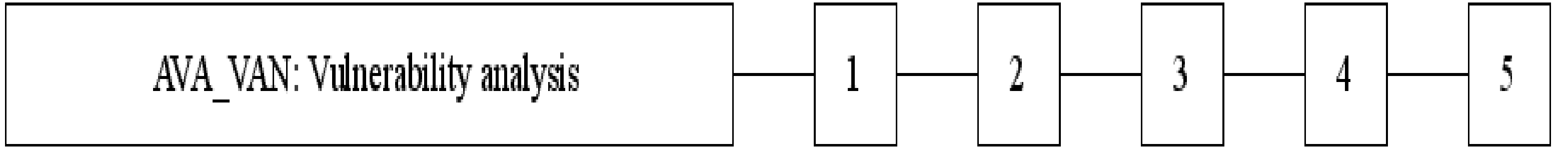
Boundary representation is
not necessarily authoritative.

802804AI (R00352) 12-01

# CC – A METRIC FOR SECURITY ASSURANCE

| The general idea | Core Concepts |
|---|---|
| • Risk owner defines the security problem | • Protection Profile (PP), normative if conformance is claimed |
| • Manufacturer defines solution | • Security Target (ST), normative for evaluation |
| • Evaluator verifies formal consistence | • Internal consistence and suitability of ST and conformance to PP, if any |
| • Evaluator verifies implementation | • Are the security functional requirements actually implemented as defined in the ST? |
| • Evaluator determines efforts required to compromise the implementation | • AVA_VAN.x, attack potential |
| • Official body certifies evaluation | • CC Certificate |

# CC – A METRIC FOR SECURITY ASSURANCE



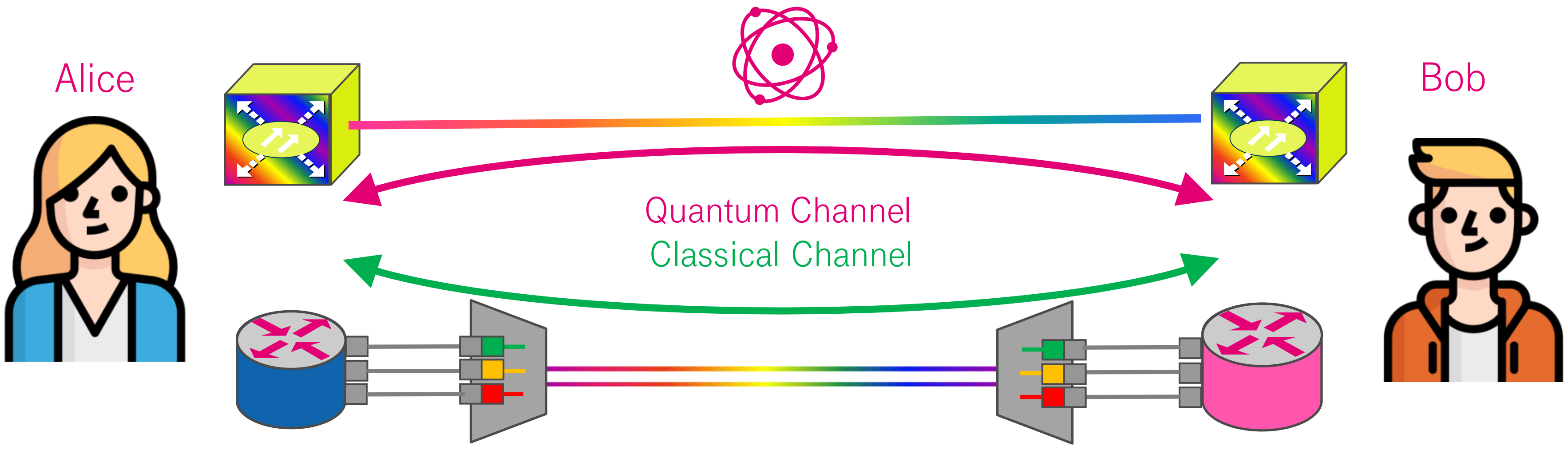
- AVA_VAN.1 Vulnerability survey
  (TOE Resistance against Basic Attack Potential)
- AVA_VAN.2 Vulnerability analysis
  (TOE Resistance against Basic AP)
- AVA_VAN.3 Focused vulnerability analysis
  (TOE Resistance against Enhanced-Basic AP)
- AVA_VAN.4 Methodical vulnerability analysis
  (TOE Resistance against Moderate AP)
- AVA_VAN.5 Advanced methodical vulnerability analysis
  (TOE Resistance against High AP)

# WHY HAVE A PP?

ERLEBEN, WAS VERBINDET.

# Quantum Key Distribution QKD

- ... uses quantum mechanical properties to convey information
- ... provably information theoretically secure (ITS) even against yet unknown attacks
- ITS is secure against computationally unbound attackers

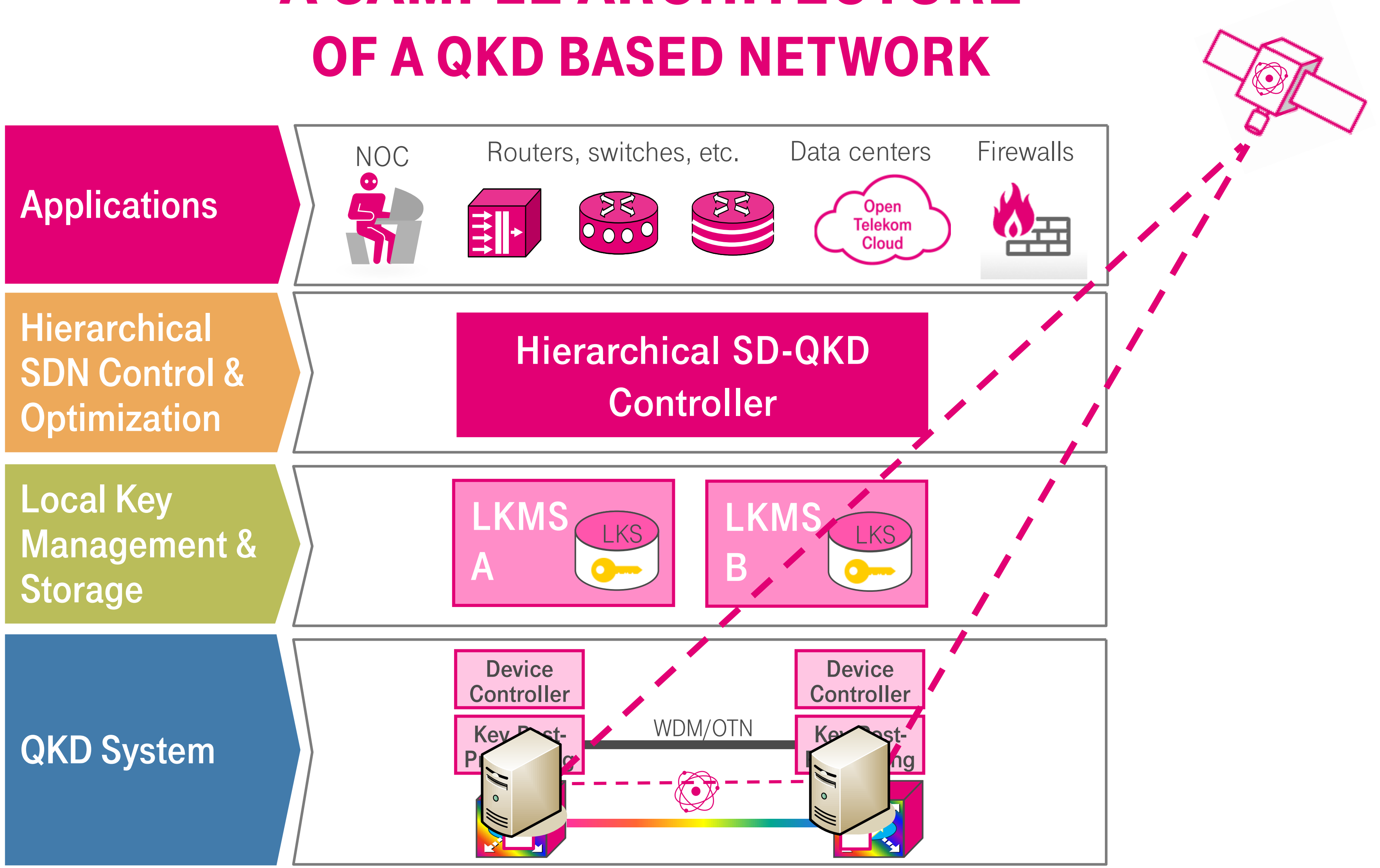


Clipart designed by Flaticon

# QKD ECOSYSTEM

- Governments aim to equip high-security networks with QC proof technologies (e.g. EuroQCI)
- Telcos also look for a successor technology to protect their backbones
- QKD devices are produced by several manufacturers
- Varying usage scenarios, ranging from
  - Point to Point networks, to
  - meshed crypto-networks for protection of telco backbones
- QKD needs to interface with a broad range of existing, incompatible infrastructures
- Several international programs to foster QKD (e.g. QSafe, OpenQKD, ...)
- QKD manufacturers usually have a physics and mathematics background; classical IT security has not been considered deeply
- No normative understanding for many core terms, yet!
- Security proofs apply to models and cannot be easily adapted to findings in real devices
- What security actually means often is unclear, and users cannot compare security features
- In particular, the term *security* in the QKD community is not identical with the conventional meaning e.g., in the CC community

# A SAMPLE ARCHITECTURE OF A QKD BASED NETWORK



# PP TO PROVIDE BASELINE SECURITY

- Risk owners need a meaningful security policy for QKD devices, which allows to compare solutions
- ETSI standardizes vocabulary and ITS methodology
- ETSI decided to provide a PP as a sound, normative reference
- Germany through the BSI (German Federal Office for Information Security) volunteered to provide a pertinent PP
- Deutsche Telekom Security contracted this task
- The draft has been discussed with BSI, ETSI, vendors, and QKD scientists

Intent

- Get off the narrative of unconditional security
- Provide transparency for vendors and integrators about security expectations
- Put a meaningful baseline i.e., it‘s not worth the fuzz for *Basic* attack potential!
- Delineate the security boundary of QKD
  - What it expects from the environment, and
  - What it provides

# WHAT IS SPECIAL ABOUT QKD?

What we learned mostly on the route ...

ERLEBEN, WAS VERBINDET.

# ONE SIZE FITS ALL?

- If the PP shoud be useful, it shall cover a broad range of use cases e.g.,
  - Point to Point connections between two guarded rooms with screened human users
  - Telco Modules installed at switch cabinets in public places interfacing to standard network equipment
- It shall not ignore the concept of ITS, but
  - CC has no concept for „ε-security“
  - „ε-security“ has no perturbation theory i.e., it does not work well with AVA_VAN.
- Broad range of QKD protocols and implementations
- Uncommon properties e.g.,
  - Authentication keys for the classical channel shall be regenerated for each transaction, but
  - Using self-established keys causes them to deteriorate
- So far no common approaches for obvious standard tasks e.g.,
  - personalization of QKD devices,
  - Initial and re-keying procedures, or
  - User role model.
- High security requires AVA_VAN.5

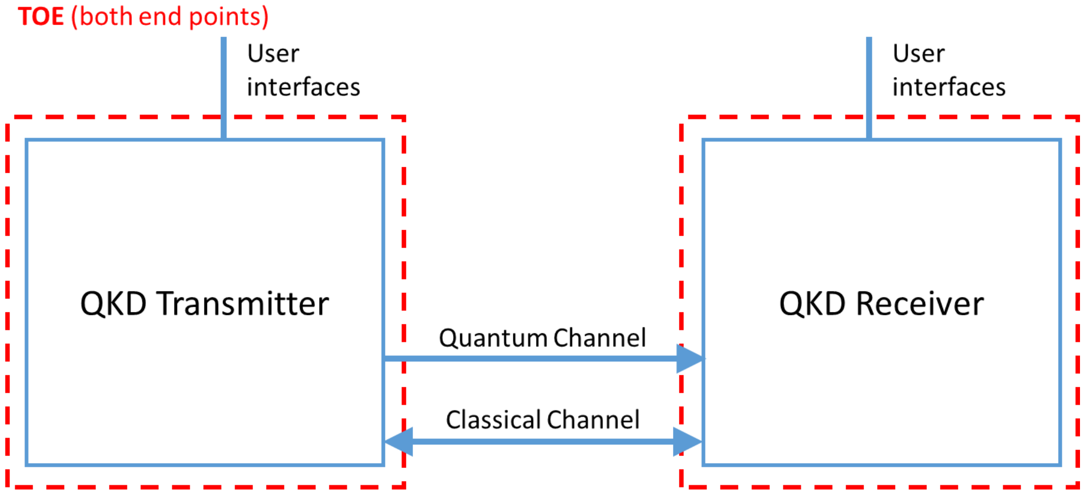
# A TOE TO GET STARTED: P&M

No, one size definitely does not fit all!

ERLEBEN, WAS VERBINDET.

# CHOICES TO TRIM TO FIT

- Limit to a single class of QKD protocols i.e., prepare and measure
- Put both end points into the same kind of environment
- Leave assessment of QKD security proofs to certification bodies, instead of analyzing them e.g., by ADV_SPM.
- Define a user role concept which is deemed minimal
- Restrain to the uttermost core functionality, and
- provide extended packages to closely guide PP/ST authors to approach realistic scenarios

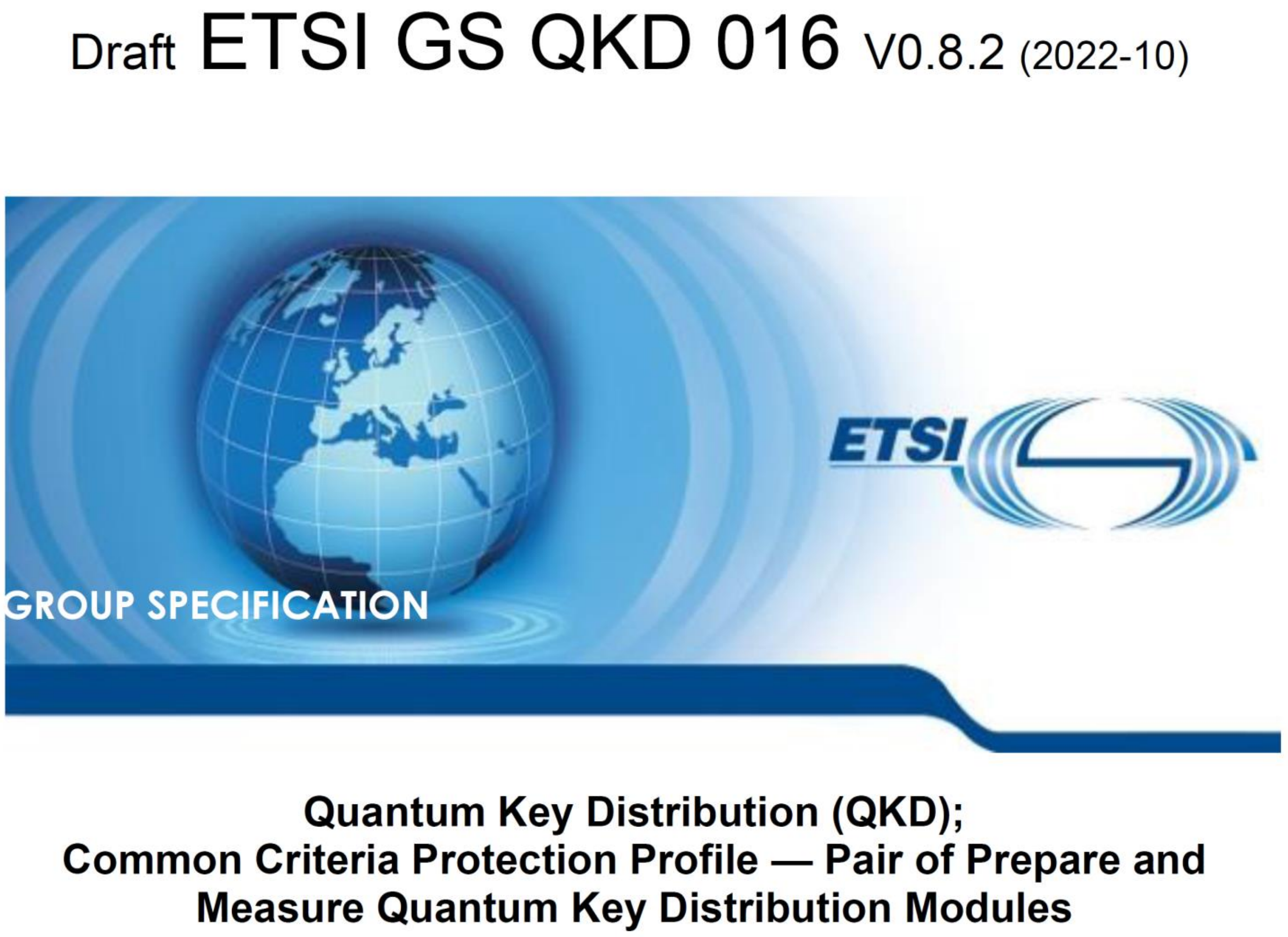


# SOME KEY ASPECTS OF THE PP

ERLEBEN, WAS VERBINDET.

# PP ISSUED BY ETSI

- Current state of PP
- Version 0.8.2
- Under evaluation by SGS Brightsight



Draft ETSI GS QKD 016 V0.8.2 (2022-10)

GROUP SPECIFICATION

ETSI

**Quantum Key Distribution (QKD);**
**Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules**

# KEY FIGURES

QKD is for high security applications i.e.,

- EAL4 + AVA_VAN.5, ALC_DVS.2

For minimal requirements of the base PP

- Both QKD modules are assumed in access controlled environment
- Physical access only to well trained, benevolent personnel
- Delivered with complete personalization

... so what is left to do for the TOE?

- Authenticated classical channel
- Side-channel resistance on the QKD connection
- Resistance against malfunction, also induced via the QKD connection
- Role based access control (RBAC) to avoid users as a single point of compromise
- Proper auditing to support forensics and prohibit by-passing the RBAC
- And of course running the core protocol

# KEY FIGURES

QKD is for high security applications i.e.,

- EAL4 + AVA_VAN.5, ALC_DVS.2

For minimal requirements of the base PP

- Both QKD modules are assumed in access controlled environment
- Physical access only to well trained, benevolent personnel
- Delivered with complete personalization

33 SFR in base PP

... so what is left to do for the TOE?

- Authenticated classical channel
- Side-channel resistance on the QKD connection
- Resistance against malfunction, also induced via the QKD connection
- Role based access control (RBAC) to avoid users as a single point of compromise
- Proper auditing to support forensics and prohibit by-passing the RBAC
- And of course running the core protocol

# FCS_QKD.1 – DEFINITION OF EXTENDED SFR

FCS_QKD.1 Prepare and Measure Quantum Key Distribution

Hierarchical to: No other components.

Dependencies: FCS_RNG.1 Random number generation
FPT_FLS.1 Failure with preservation of secure state
FTP_ITC.1 Inter-TSF trusted channel
FCS_CKM.4 Cryptographic key destruction

FCS_QKD.1.1 The TSF shall perform the quantum key distribution protocol according to [assignment: *QKD protocol*] [*between separate parts of the TOE*] in order to establish confidential, shared, random bit strings. The security parameter of the protocol shall not exceed [assignment: *security parameter threshold*] according to the associated security proof.

FCS_QKD.1.3 The TSF shall [*prepare <u>and</u> measure*] [assignment: *description of quantum states*] and support [*transmission <u>and</u> reception*] of these quantum states through an external interface.

# FCS_QKD.1 – QKD SPECIFICS

FCS_QKD.1.2 The TSF may repeat execution of the QKD protocol if it aborted or did not deliver a sufficient number of bits. The TSF shall ensure that the determining factors of the QKD protocol are assured for each individual execution of the QKD protocol. The TSF shall maintain a counter for all attempts of key establishment. The TSF shall [*provide authorized users with the capability to request the current value of the attempt counter and deny protocol execution if the attempt counter exceeds [assignment: threshold for the attempt counter]*].

FCS_QKD.1.4 The TSF shall perform [assignment: *list of post-processing algorithms before privacy amplification*] on the raw data using the authenticated classical channel to establish a shared, corrected bit string.

FCS_QKD.1.5 The TSF shall keep track of deliberately disclosed information during post-processing and perform parameter estimation for [assignment: *list of parameters*]. Using these inputs the TSF shall deduce the privacy amplification ratio.

FCS_QKD.1.6 The TSF shall perform [assignment: *list of privacy amplification algorithms*] on the corrected bit strings using the authenticated classical channel to establish the confidential, shared, random bit strings based on the privacy amplification ratio.

# PACKAGES FOR OTHER USE CASES

Table of contents

11. Packages

11.1 Trusted User Interface with Authentication (TUI+A)

11.2 TOE self-protection (PROT)

11.3 Provisioning after delivery (PERSO)

11.4 Local Authentication of Users (LUA)

**The ST/PP author shall adopt all formal items from a package, if conformance to this PP with that package is claimed.**

In addition to the SFR constituting the package, each package discusses how the changes impact the TOE mode of use and the security problem definition.

Each package proposes refinements to formal items of formal items beyond the SFR. The PP application note requires PP/ST authors to adopt these.

TUI+A and LUA are mutually exclusive, because they define conflicting refinements.

Packages may be used as a blueprint to define ST matching the vendor specific product still able to claim conformance to the base PP.

# WHAT‘S NEXT?

ERLEBEN, WAS VERBINDET.

# THE FINISHING LINE

- Evaluation of the PP by SGS Brightsight
- Certification of the PP by BSI
- Publishing of the PP by ETSI as a standard

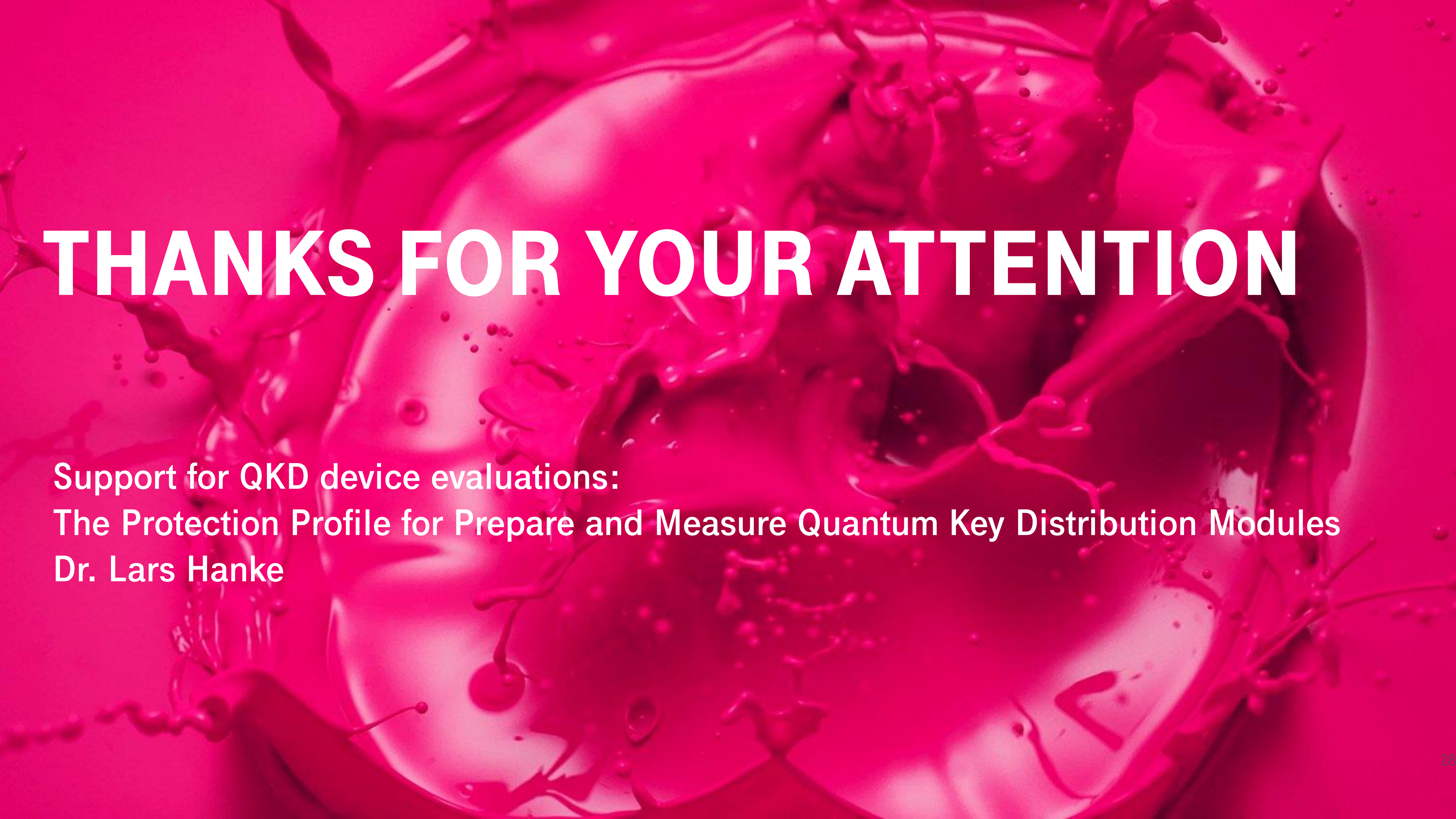
- Create ST for the devices claiming conformance to the PP
- Improve device security to meet the ST

- QKD devices with well defined ITS properties to be certified as resistant against high attack potential

- Install a technical working group for QKD to drive the evaluation methodology

- Derive national requirements to use QKD with classified documents

- Gain experience
- Define usage scenarios and combine with PQC applications
- Establish internationally harmonized standards for security, functionality, and inter-operability



# THANKS FOR YOUR ATTENTION

Support for QKD device evaluations:
The Protection Profile for Prepare and Measure Quantum Key Distribution Modules
Dr. Lars Hanke