QuNET$^+$ BlueCert

Approach to a National Evaluation Laboratory and Metrology

Dr. Ulrich Seyfarth, BearingPoint

QuNET

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

BearingPoint®

Quantum Technologies with BearingPoint

Together we are more than business

BearingPoint is a **leading management and technology consultancy** that stands for innovation and excellence in quantum technologies. These are a key factor for digital transformation and offer enormous **potential for the economy, society and the environment**.

Our **team of experts** with experience in various subject areas is **closely networked** with leading research institutes, universities and industrial partners. We support customers in understanding and exploiting the **opportunities and challenges** of quantum technologies. For this we offer holistic consulting, ranging from strategy to implementation and operation.

Know-how in technology, transformation and sustainability

BearingPoint Quantum

- Quantum Computing
- Quantum Communication
- Quantum Sensing

References (Selection)

- Publication: (BSI) Implementation Attacks against QKD Systems
- Project: QuNET+SKALE
- Project: QuNET+BlueCert
- Product: Security Quick-Check

Content

1

The QuNET+BlueCert Project

2

Motivation and approach

3

Developing a blueprint for a certification ecosystem

4

What comes after?

Project Summary

A Blueprint of a Certification Eco-System for QKD Systems and Applications

QuNET⁺ BlueCert

Quantum communication is the most promising technology in protecting our future data, but its usability requires a complex infrastructure

- **QuNET+BlueCert project aims to support the German industry in testing, qualifying, and certifying quantum communication technologies**
- **The Project develops missing methods, competencies, and test environments**
- **Analyzing existing certification efforts to create test procedures, measuring devices, and evaluation metrics**
- **It creates a blueprint of a neutral laboratory environment to guide certification efforts**
- **It will contribute significantly to the market readiness of quantum communication technology**

Project Duration:
01/2024 – 12/2026

Project Volume:
3,28 Mio. €

The Team

Overview, scientific-technical experience, requirements analyses, broad client experience	BearingPoint
Quantum information processing, implementation of QKD protocols; **CV QKD System**	FAU
Photonic quantum technologies, single photon detectors; **BB84-DV QKD System**	Fraunhofer HHI
Quantum photonics for science and industry applications; Entanglement-based **BBM92 QKD System**	Fraunhofer IOF
Applied research in IT Security and cryptography	Fraunhofer AISEC

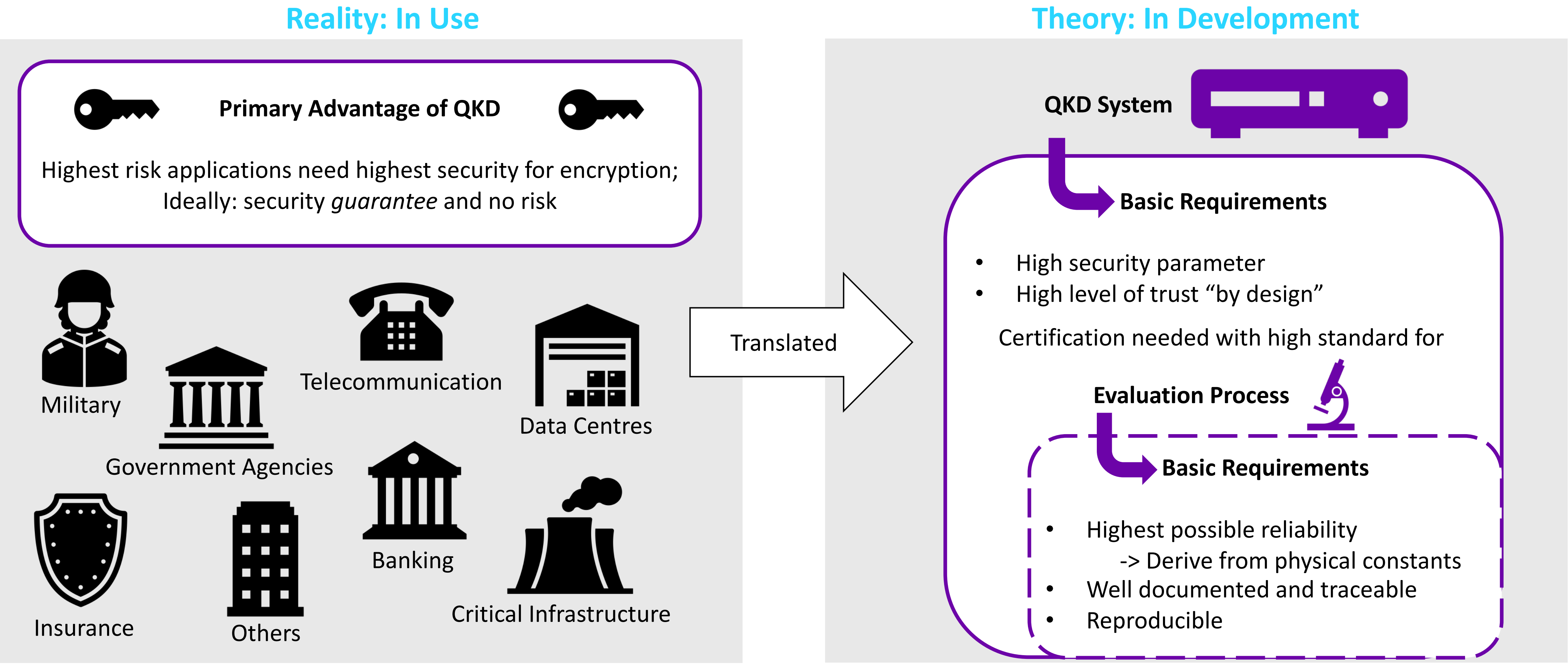
Pixel Photonics	Characterization of SNSDP QKD Systems
PTB	Metrology and pioneer for characterization of single photon sources; new device development
TÜVIT TÜVNORDGROUP	Certificate evaluations of IT security systems; realization of exemplary laboratory

Associated Partners

QUANTUM OPTICS JENA	Commercialization of QKD terminals
qssys Quantum Space Systems	Free-space QKD systems; Implementation attacks and countermeasures

Deriving Requirements for QKD Devices and Measurements from Practice

Based on the projected primary application of QKD systems, certification is needed to establish a high level of trust into the products.



Reality: In Use

Primary Advantage of QKD

Highest risk applications need highest security for encryption;
Ideally: security *guarantee* and no risk

Theory: In Development

QKD System

Basic Requirements

- High security parameter
- High level of trust "by design"

Certification needed with high standard for

Evaluation Process

Basic Requirements

- Highest possible reliability
  -> Derive from physical constants
- Well documented and traceable
- Reproducible

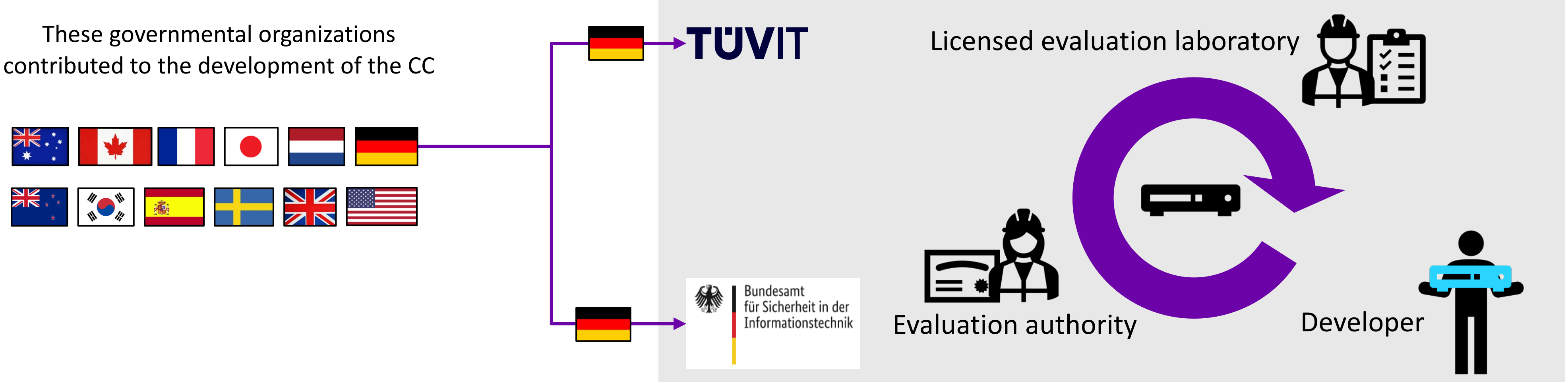
Common Criteria (CC) and Common Evaluation Methodology (CEM) for IT Security Evaluation

A technical basis for an international agreement for the widest available mutual recognition of secure IT products.

The CC ensures that

- **Products** can be evaluated by competent and independent **licensed laboratories** so as to determine the fulfilment of particular security properties
- **Supporting documents** are used within the CC certification process to define how the criteria and evaluation methods are applied when certifying specific technologies
- The certification of the security properties of an evaluated product can be issued by a number of **Certificate Authorizing Schemes**, with this certification being based on the result of their evaluation

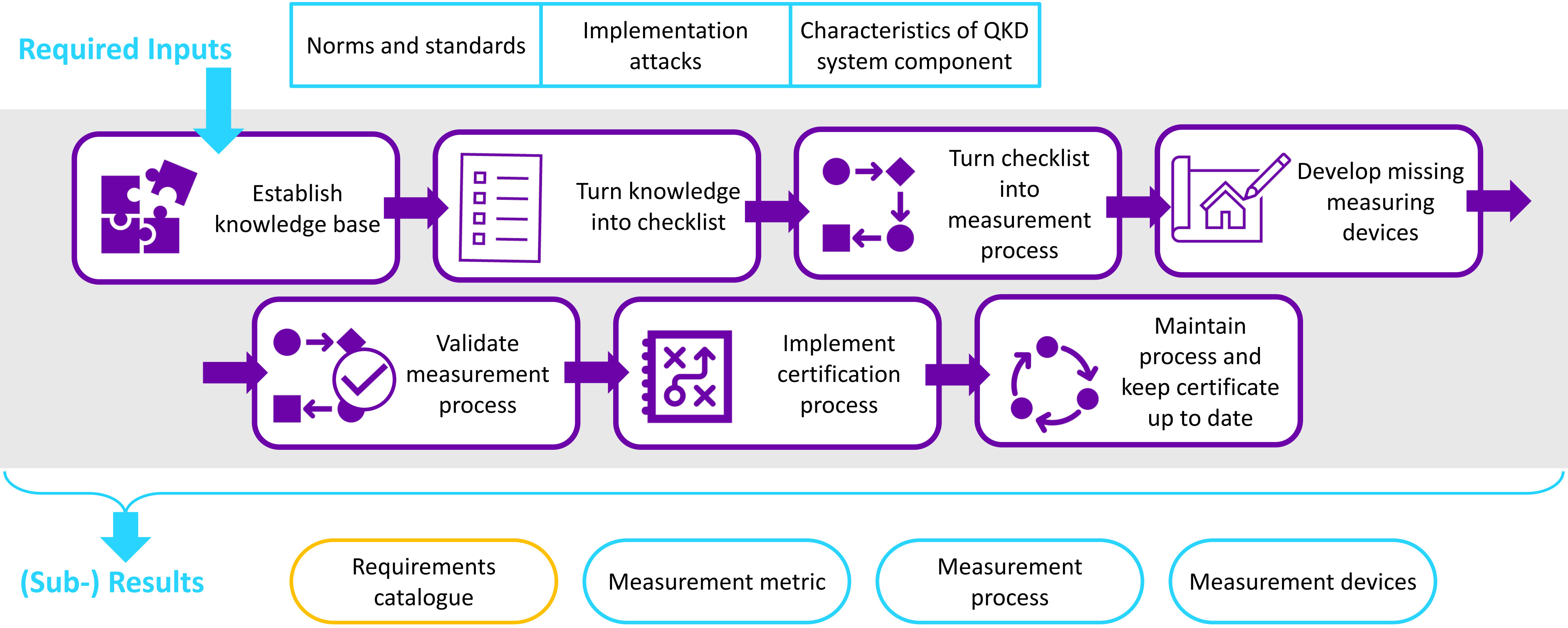
CC	CEM
Definition of Security Functional Requirements + Security Assurance Requirements	**Evaluation Process + Related Tasks**



These governmental organizations contributed to the development of the CC
TÜVIT
Licensed evaluation laboratory
Bundesamt für Sicherheit in der Informationstechnik
Evaluation authority
Developer

How to Establish an Evaluation/Certification Process for QKD Systems - Overview

Based on research results, an evaluation process for certification of QKD system security can be created.



Required Inputs

Norms and standards

Implementation attacks

Characteristics of QKD system component

Establish knowledge base

Turn knowledge into checklist

Turn checklist into measurement process

Develop missing measuring devices

Validate measurement process

Implement certification process

Maintain process and keep certificate up to date

(Sub-) Results

Requirements catalogue

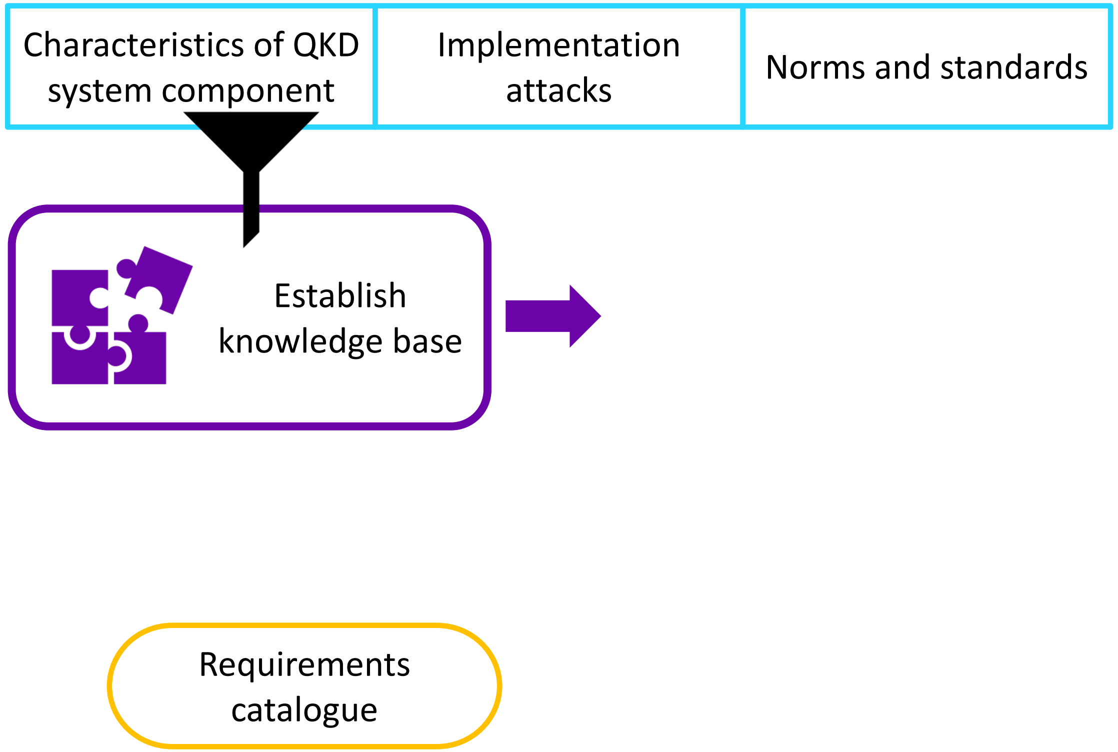
Measurement metric

Measurement process

Measurement devices

How to Establish an Evaluation/Certification Process for QKD Systems 1/2

Based on research results, an evaluation process for certification of QKD system security can be created.



Characteristics of QKD system component

Implementation attacks

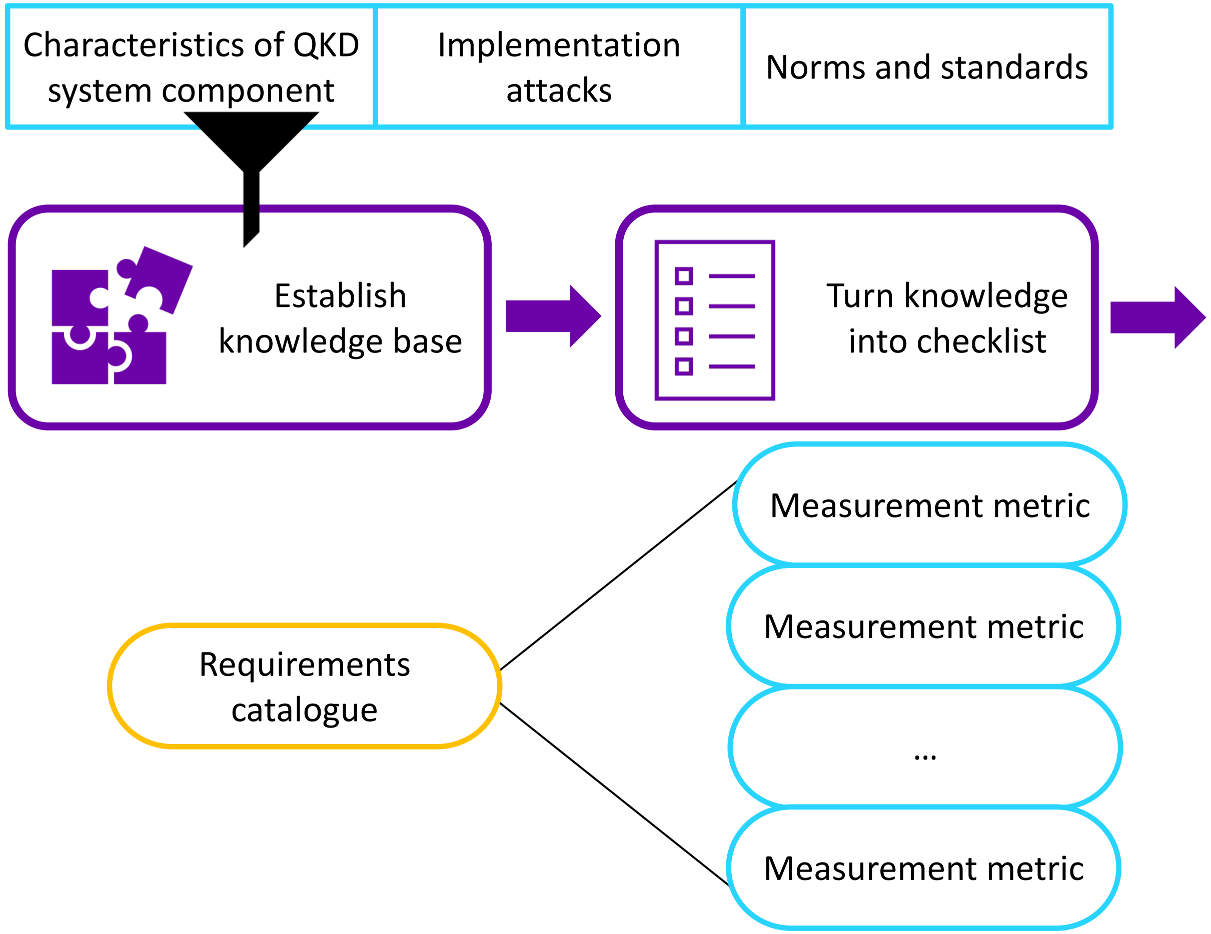
Norms and standards

Establish knowledge base

Requirements catalogue

How to Establish an Evaluation/Certification Process for QKD Systems 1/2

Based on research results, an evaluation process for certification of QKD system security can be created.



Characteristics of QKD system component

Implementation attacks

Norms and standards

Establish knowledge base

Turn knowledge into checklist

Requirements catalogue

Measurement metric

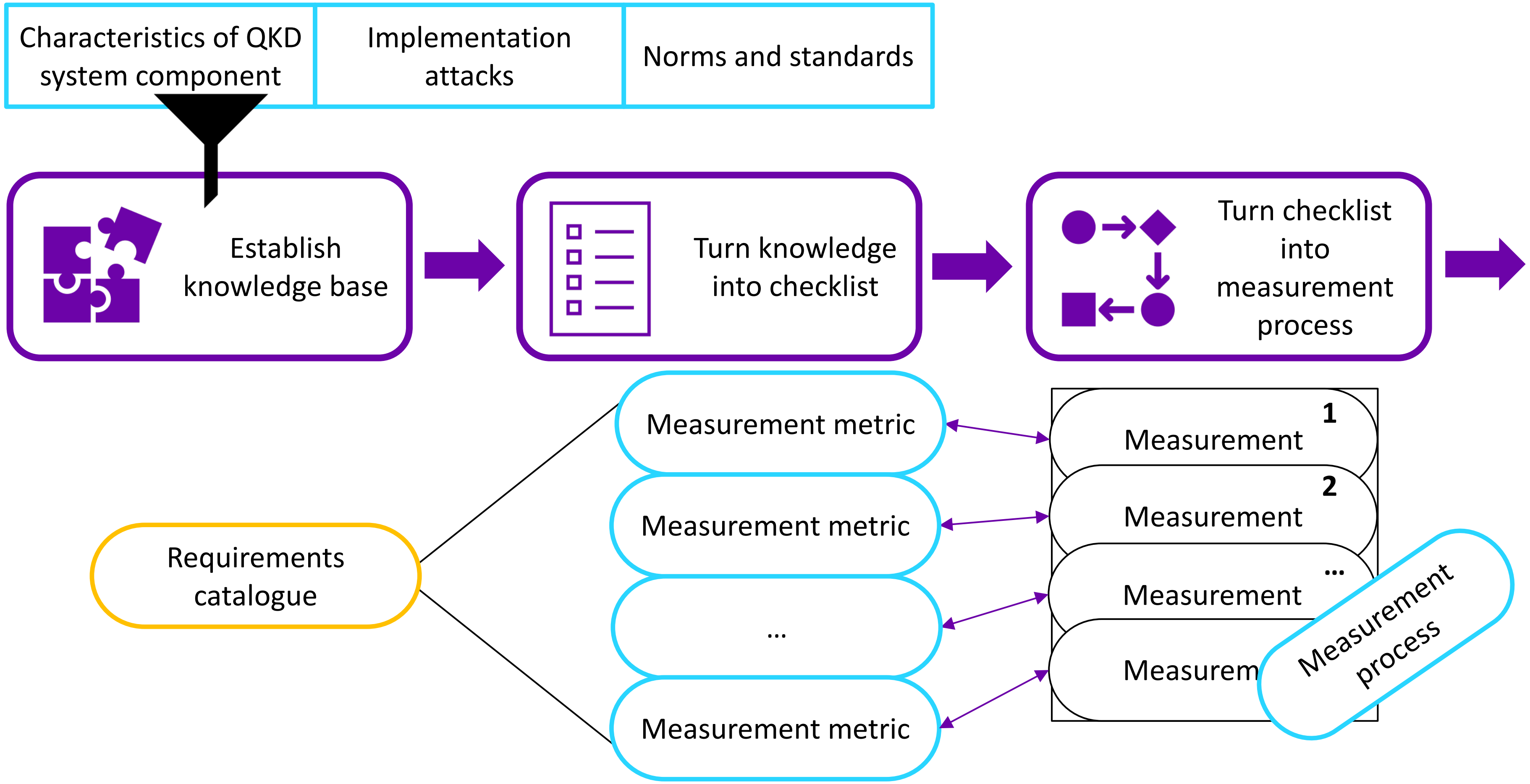
Measurement metric

…

Measurement metric

How to Establish an Evaluation/Certification Process for QKD Systems 1/2

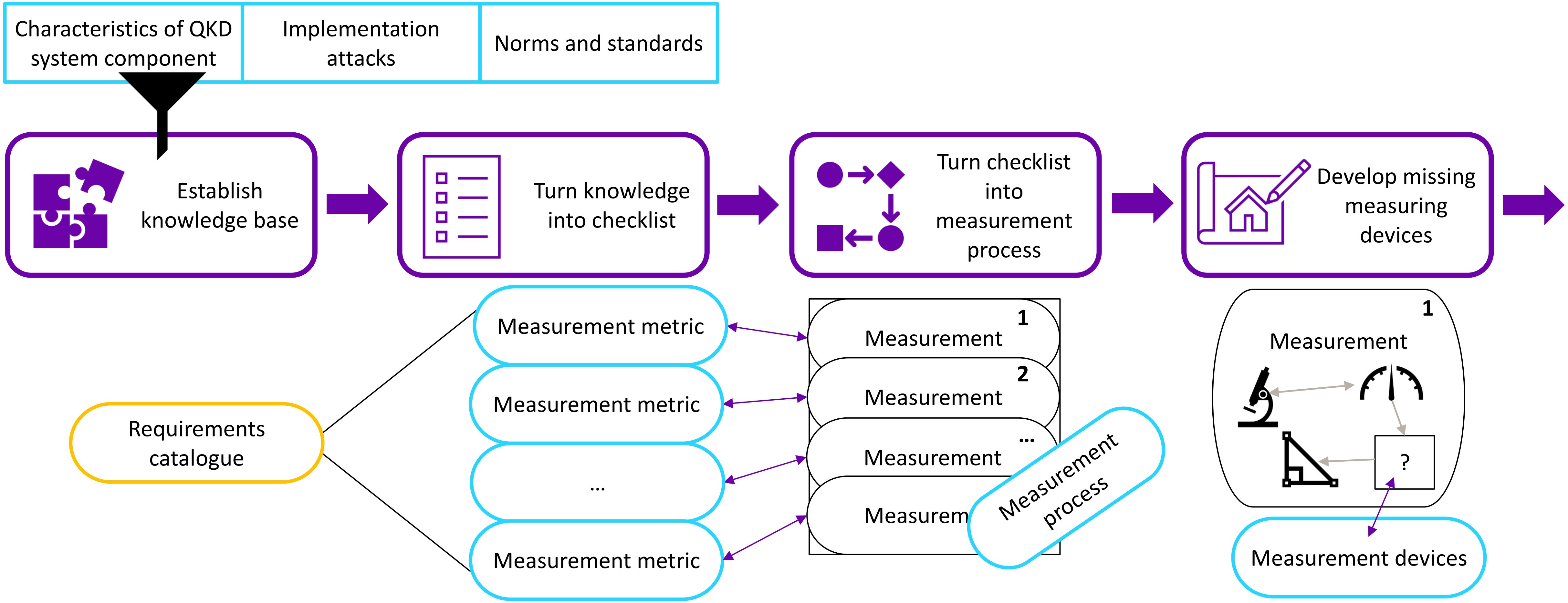
Based on research results, an evaluation process for certification of QKD system security can be created.



BearingPoint®

How to Establish an Evaluation/Certification Process for QKD Systems 1/2

Based on research results, an evaluation process for certification of QKD system security can be created.



Characteristics of QKD system component

Implementation attacks

Norms and standards

Establish knowledge base

Turn knowledge into checklist

Turn checklist into measurement process

Develop missing measuring devices

Requirements catalogue

Measurement metric

Measurement metric

…

Measurement metric

Measurement 1

Measurement 2

Measurement …

Measurem

Measurement process

1

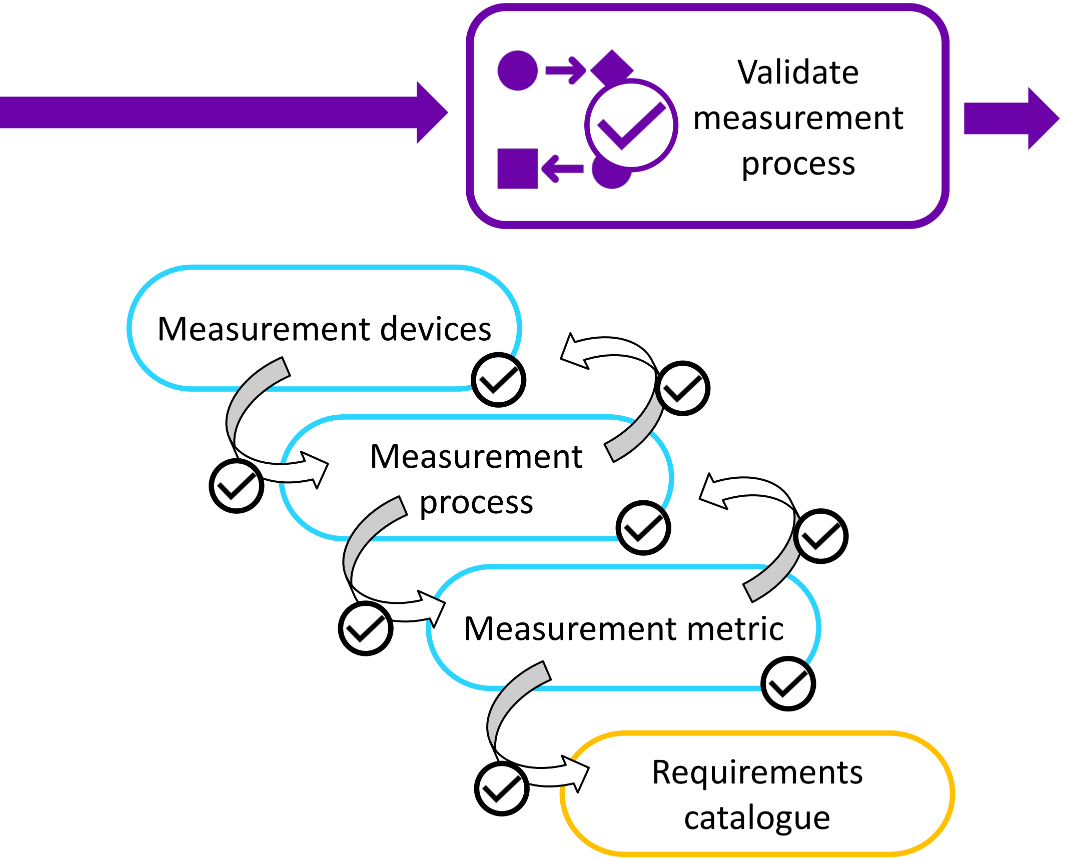
Measurement

?

Measurement devices

How to Establish an Evaluation/Certification Process for QKD Systems 2/2

Based on research results, an evaluation process for certification of QKD system security can be created.



Validate measurement process

Measurement devices

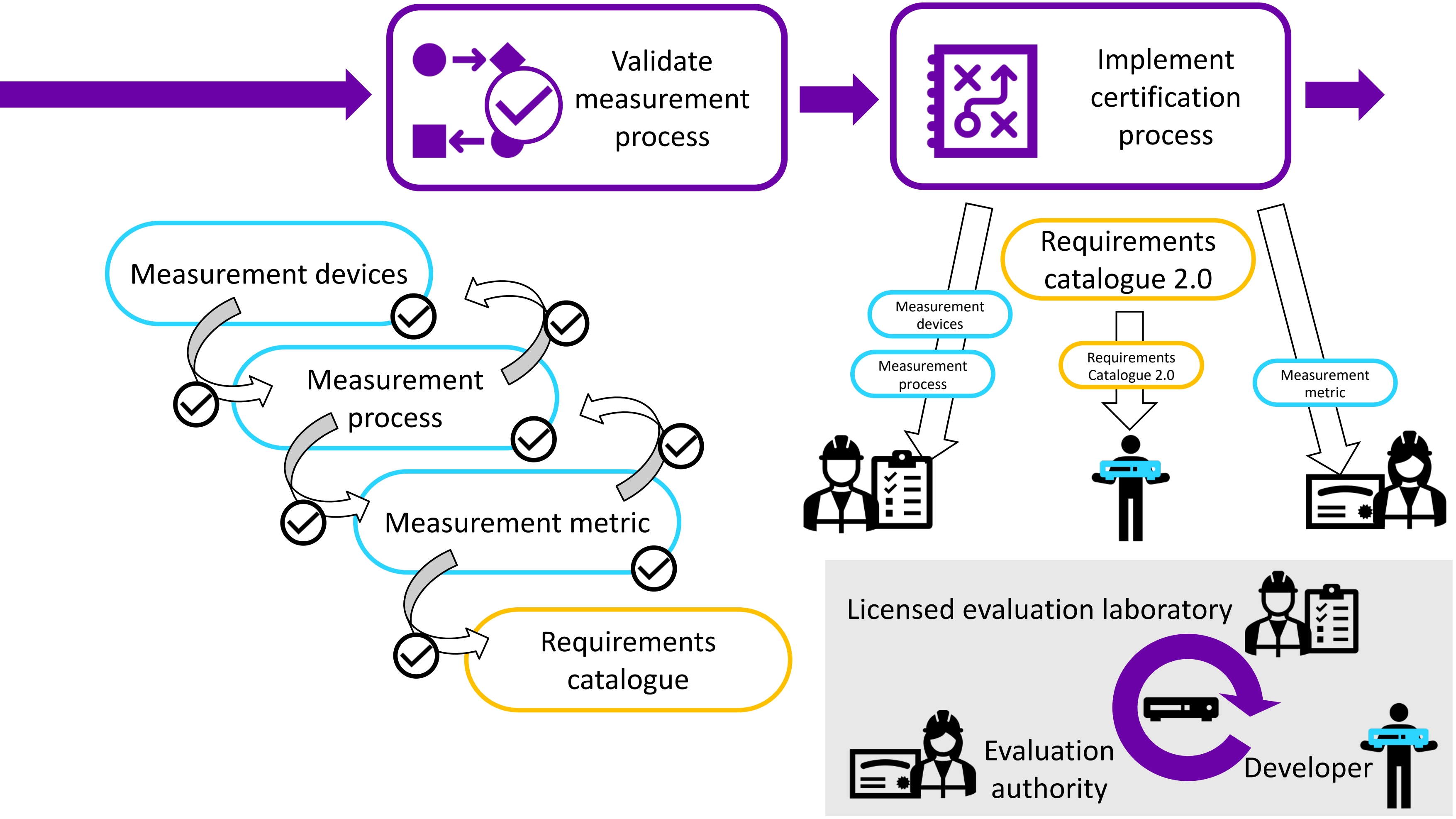
Measurement process

Measurement metric

Requirements catalogue

How to Establish an Evaluation/Certification Process for QKD Systems 2/2

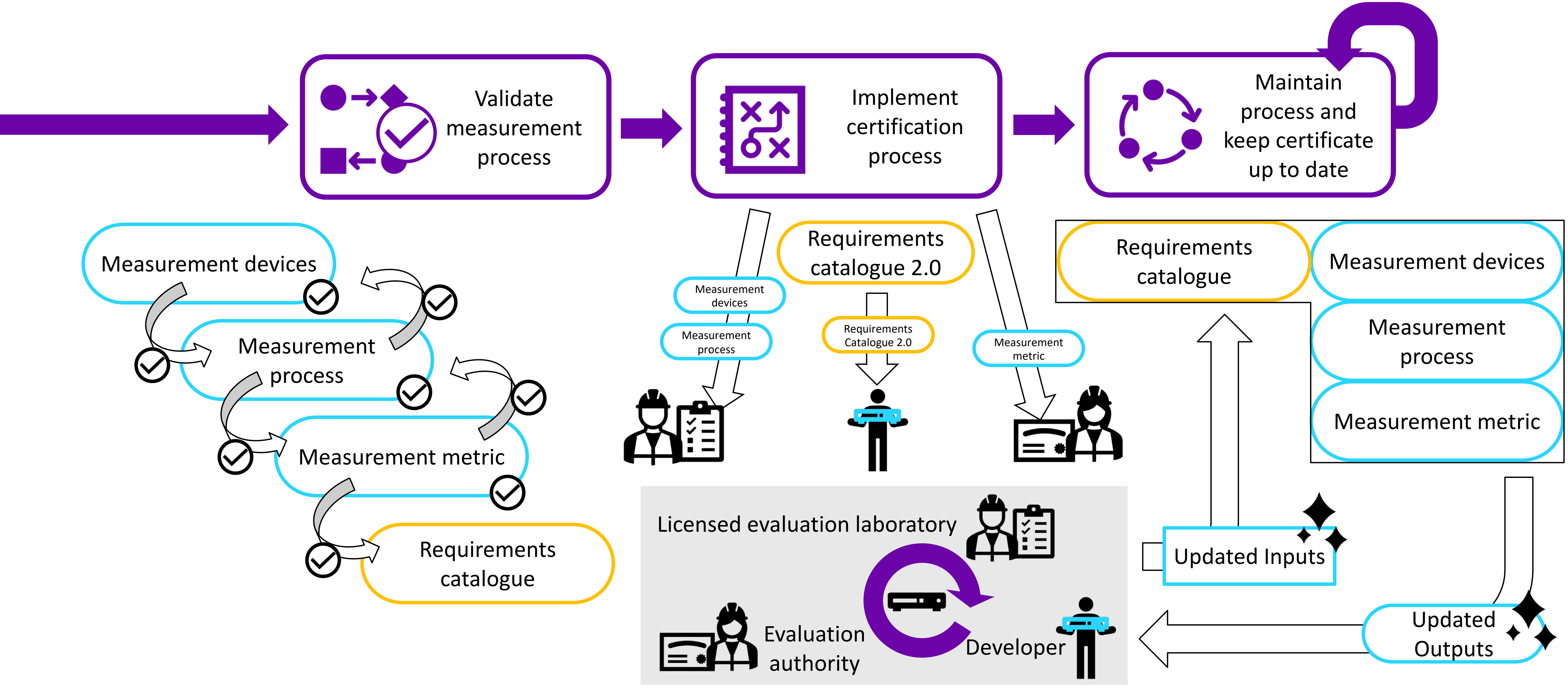
Based on research results, an evaluation process for certification of QKD system security can be created.



BearingPoint®

How to Establish an Evaluation/Certification Process for QKD Systems 2/2

Based on research results, an evaluation process for certification of QKD system security can be created.



Validate measurement process

Implement certification process

Maintain process and keep certificate up to date

Measurement devices

Measurement process

Measurement metric

Requirements catalogue

Requirements catalogue 2.0

Measurement devices

Measurement process

Requirements Catalogue 2.0

Measurement metric

Licensed evaluation laboratory

Evaluation authority

Developer

Requirements catalogue

Measurement devices

Measurement process

Measurement metric

Updated Inputs

Updated Outputs

Current Standards Situation for QKD Technologies

Currently, there exists a diverse landscape of norms and standards but there is no established process to evaluate actual system.

Many (inter)national organizations publishing norms and standards in the field of QKD technologies

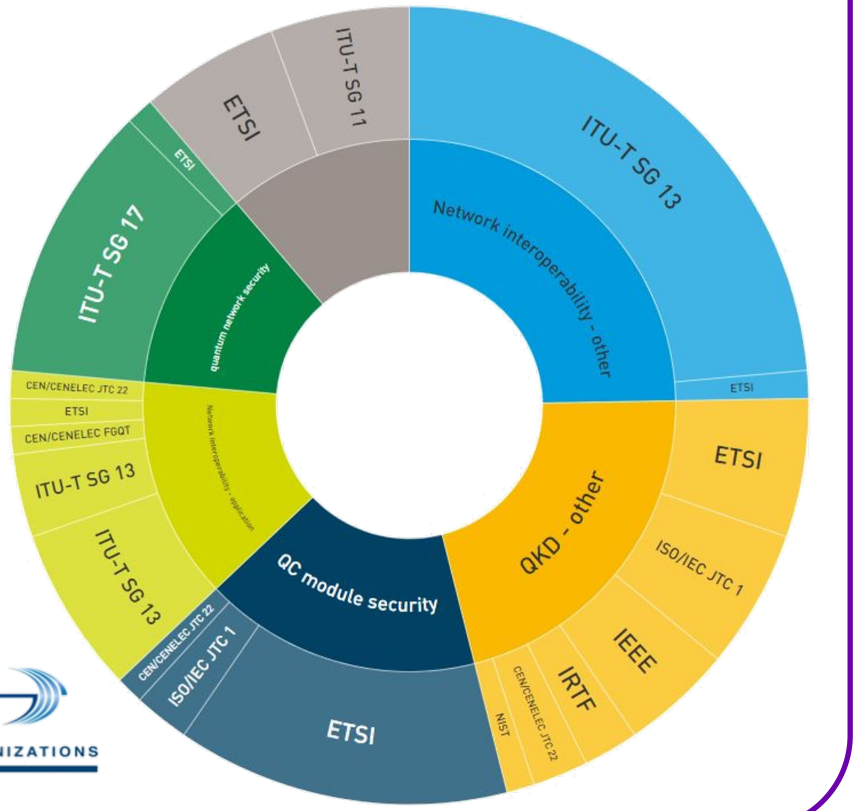


Image Source: https://www.din.de/de/forschung-und-innovation/partner-in-forschungsprojekten/ki/squad-1039236

? ¿

No established / accepted / recognized evaluation process for QKD technologies!

? ¿ ?

BearingPoint

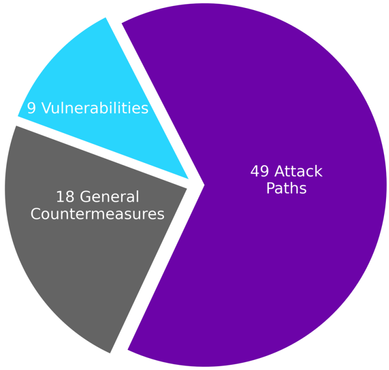
Project 575: Implementation attacks on QKD systems

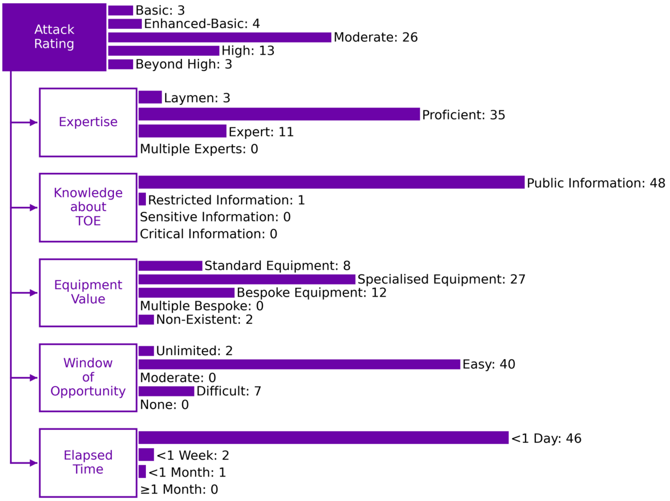
Insights into different attack paths and applicable countermeasures are important inputs to evaluate QKD systems.

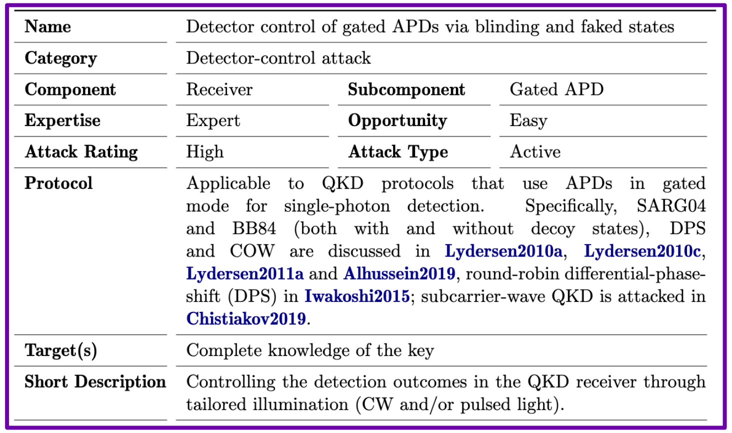
Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

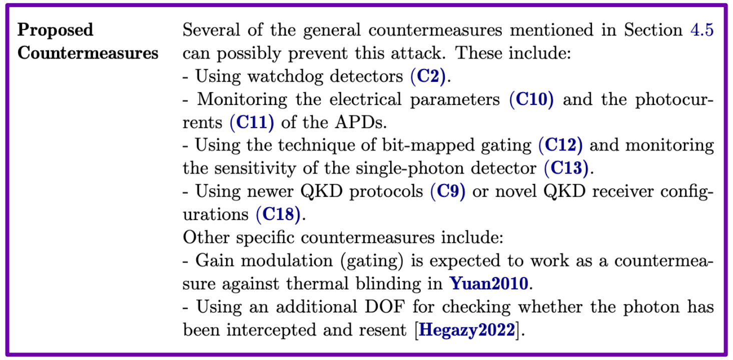
Implementation Attacks against QKD Systems







Name	Detector control of gated APDs via blinding and faked states		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Gated APD
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use APDs in gated mode for single-photon detection. Specifically, SARG04 and BB84 (both with and without decoy states), DPS and COW are discussed in Lydersen2010a, Lydersen2010c, Lydersen2011a and Alhussein2019, round-robin differential-phase-shift (DPS) in Iwakoshi2015; subcarrier-wave QKD is attacked in Chistiakov2019.		
Target(s)	Complete knowledge of the key		
Short Description	Controlling the detection outcomes in the QKD receiver through tailored illumination (CW and/or pulsed light).		



Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (C2). - Monitoring the electrical parameters (C10) and the photocurrents (C11) of the APDs. - Using the technique of bit-mapped gating (C12) and monitoring the sensitivity of the single-photon detector (C13). - Using newer QKD protocols (C9) or novel QKD receiver configurations (C18). Other specific countermeasures include: - Gain modulation (gating) is expected to work as a countermeasure against thermal blinding in Yuan2010. - Using an additional DOF for checking whether the photon has been intercepted and resent [Hegazy2022].

→ **Leverage knowledge** from the study to refine the **requirements catalogue** and **evaluation activities**!

Filling the Measurement Gaps with new Devices

Not every identified measurement metric will be covered by existing devices, so new tools are needed to fulfill requirements.

What characterizations cannot be measured with existing measurement devices?

Developing the new devices

- Measurement capability and functions
- Calibration
- Reliability and reproducibility

Studying the new devices

- Characteristics, functions and limitations
- Suitability to measurement purpose
- Statistical and systematic uncertainties

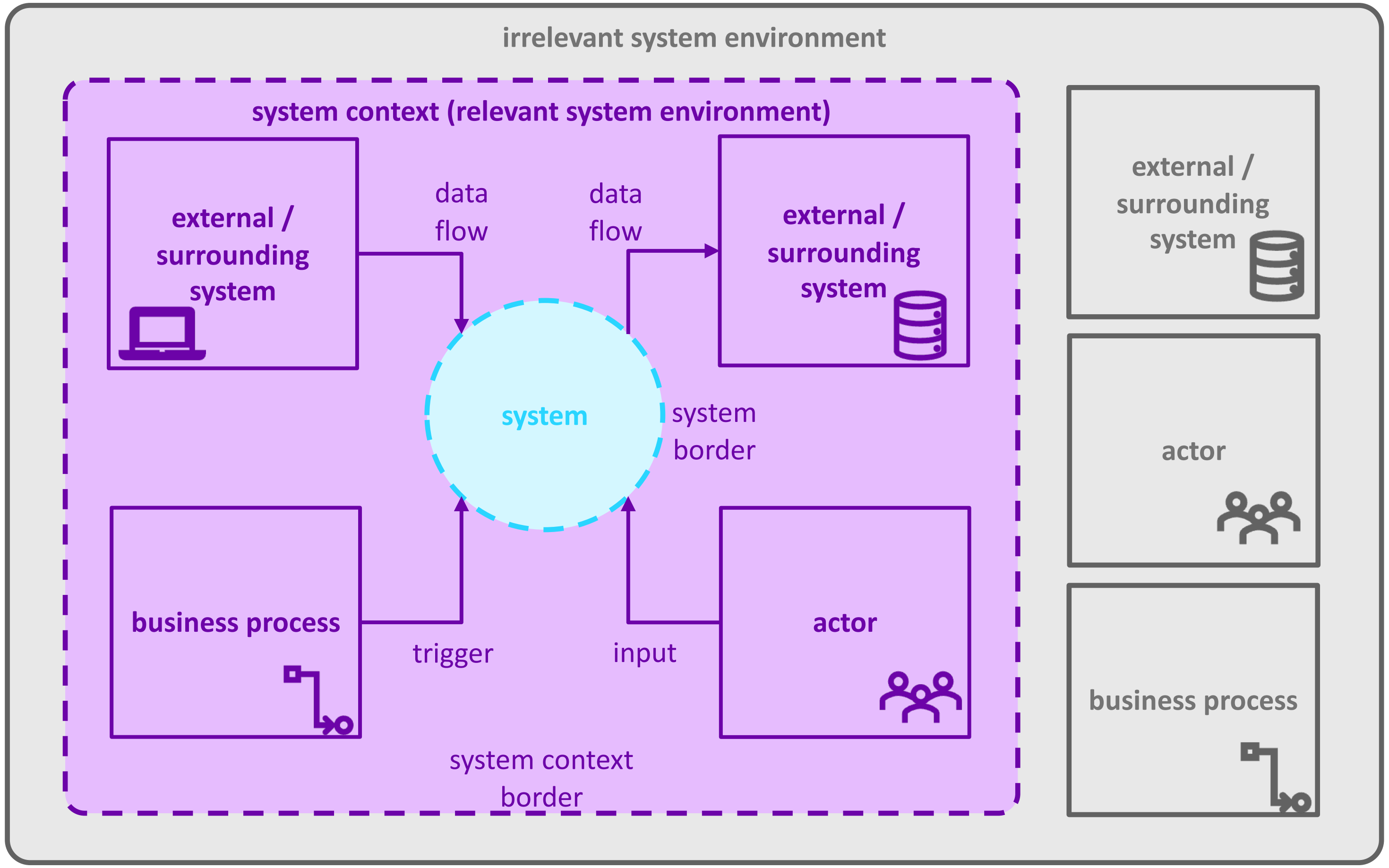
PTB

Metrological significance

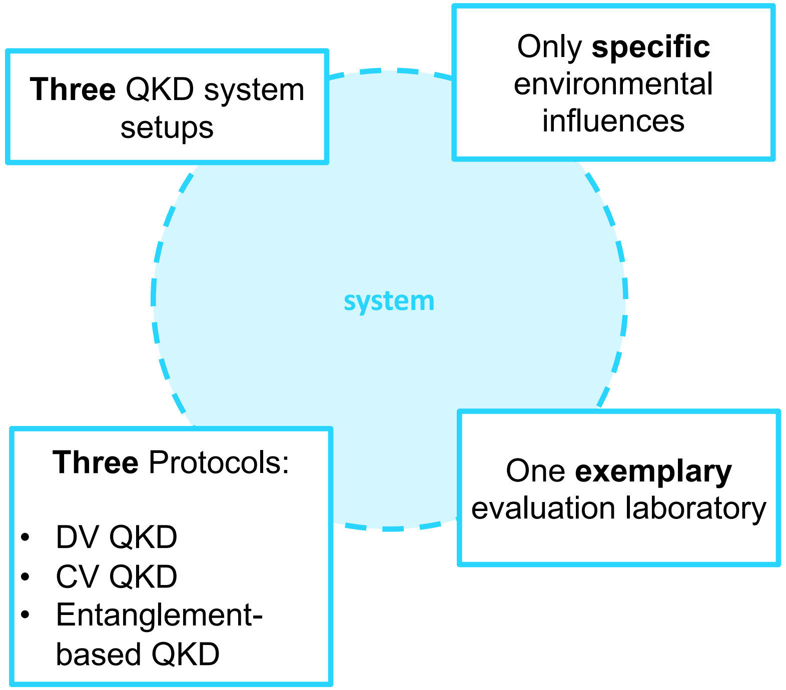
- Insights into characterization of QKD components
- Understanding on how to prove the security of different QKD implementations
- Insights into the variance of security-relevant metrics under realistic operating conditions

Validation in BlueCert done with Selected Factors

The Security of QKD systems encompasses many factors; As initial approach, QuNET+BlueCert focusses on the system itself.


irrelevant system environment
system context (relevant system environment)
external / surrounding system
data flow
data flow
external / surrounding system
system
system border
business process
trigger
input
actor
system context border
external / surrounding system
actor
business process

QuNET+ BlueCert



Three QKD system setups

Only **specific** environmental influences

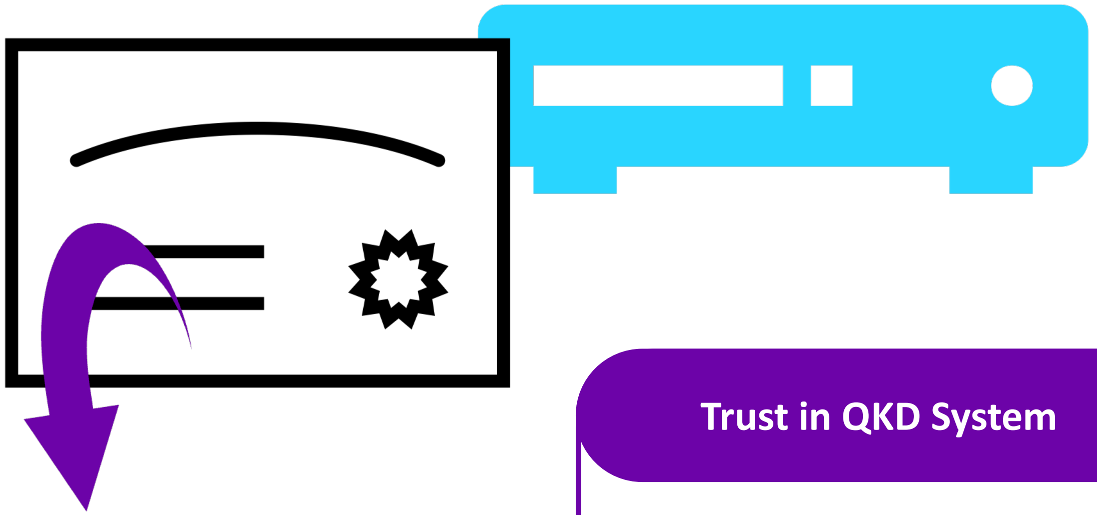
Three Protocols:

- DV QKD
- CV QKD
- Entanglement-based QKD

One **exemplary** evaluation laboratory

Outlook

QuNET+BlueCert builds the blueprint for an ecosystem of which many next steps and questions are still pending to certify QKD security.



Gives trust in security of products

Enables giving official approval for use

Trust in QKD System

- Needs **certifiable standards**
- Needs official **governmental approval of standards** for use in certificate
- Needs **ability to evaluate** based on standards

Next Steps

- Extend analysis and evaluation to all protocols and QKD systems
- Increase knowledge and level of detail on implementation attacks
- Increase maturity level of standards
- Extend and improve measurement checklist
- Extend range of measurement devices
- ... and more

...and there are still many open questions about the certification process itself!

Thank you!

Dr. Ulrich Seyfarth
Senior Technology Consultant

T +49 89 54033 6190
M +49 160 / 94483979

ulrich.seyfarth@bearingpoint.com