ITU Workshop on Quantum key distribution protocols, security and certification, 2022

Brief introduction of ISO/IEC 23837

Hongsong Shi

Expert, ISO/IEC JTC1/SC27

Where are we?

- ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection” includes 5 working groups
- Over the past 30 years, SC27 has developed lots of security standards
- Quantum-Safe Cryptography standards have been initiated and developed in WG2 and WG3
- This presentation will introduce the work ISO/IEC 23837 in WG3
  - WG3 – Security evaluation, testing and specification

WG3 standardization work on QKD

- ISO/IEC 23837 will standardize the security requirements and evaluation methods of QKD modules
  - A Study Period was initialized by SC 27/WG3 in Oct. 2017
  - Development work started from April 2019, to be published in 2023
  - Comprise two parts

Schedule

- 6 drafts (3 WDs, 2 CDs, 1 DIS) have been commented, now it is going to the publication phase
- Publication is planned for the first half of 2023.

Liaisons

- ETSI ISG QKD
- ITU-T SG 17
- ITU-T FG QIT4N

ISO/IEC 23837-1: Requirements
Jiajun Ma,
Andrew Shields,
Charles Ci Wen Lim

Information security—Security requirements, test and evaluation methods for quantum key distribution— Part 1: Requirements

ISO/IEC 23837-2: Test and evaluation methods
Hongsong Shi, Gaetan Pradel, Martin Ward

Information security—Security requirements, test and evaluation methods for quantum key distribution— Part 2: Test and evaluation methods

Position of ISO/IEC 23837

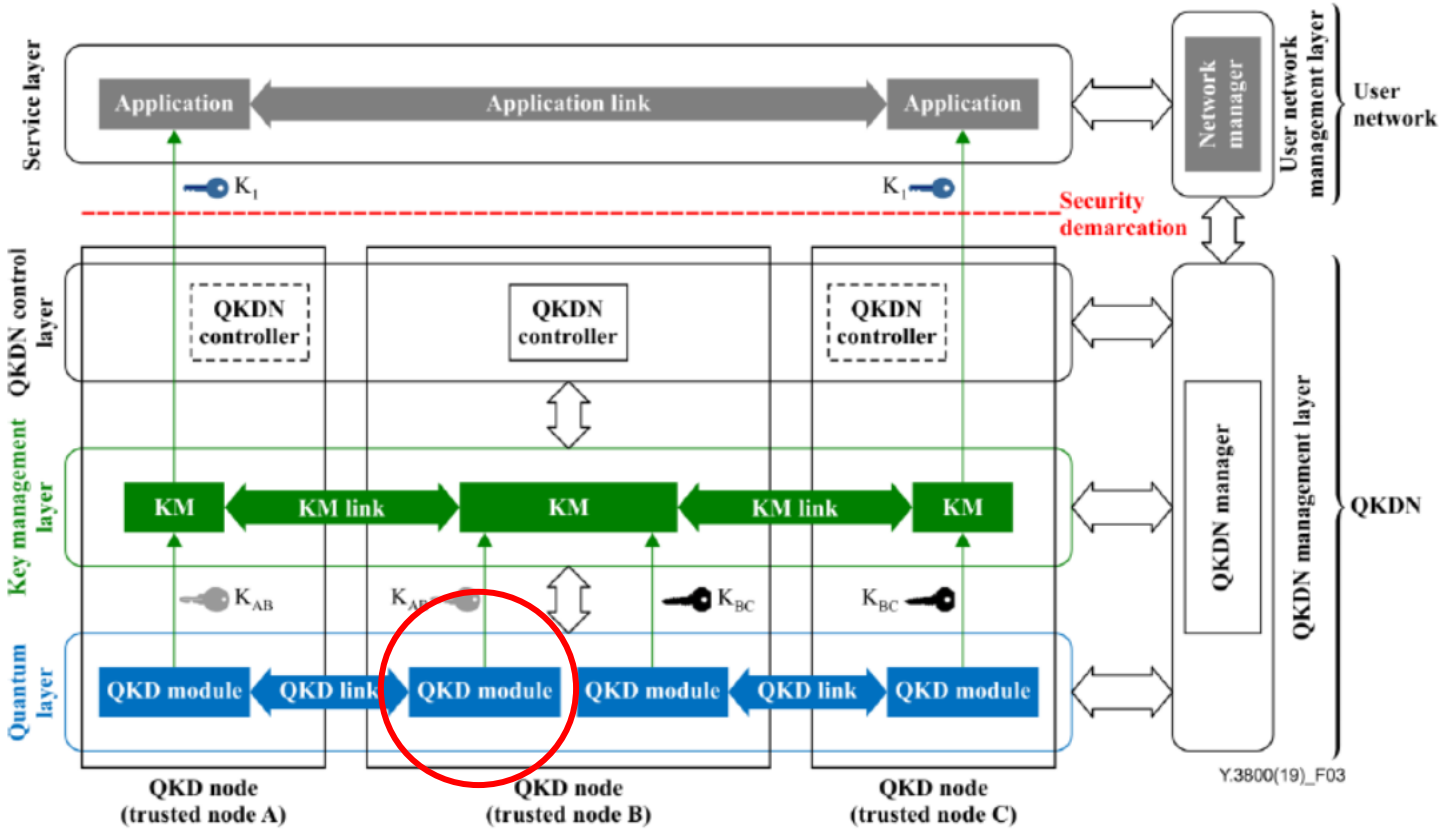
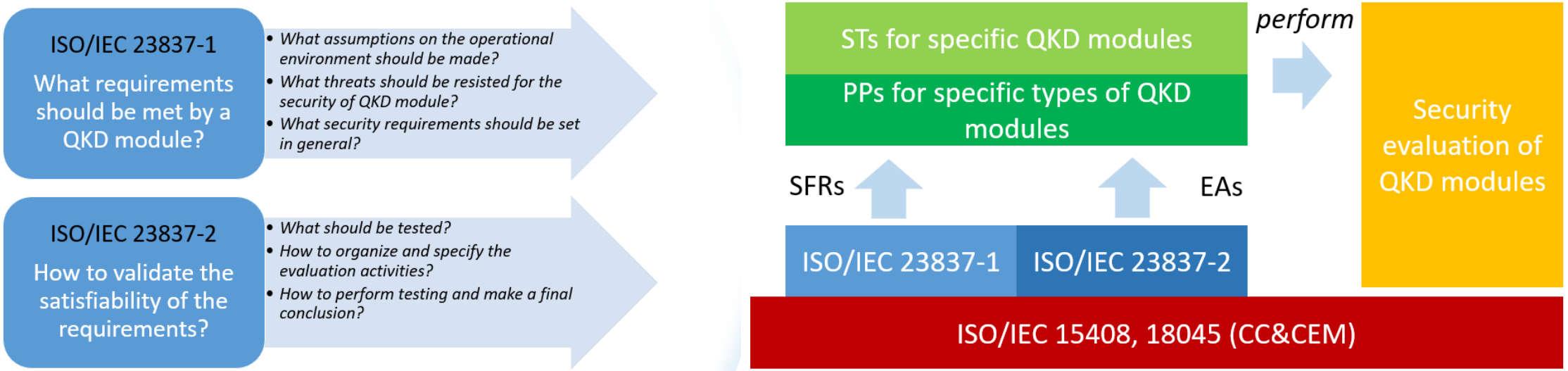


Figure 3 – Illustration of the conceptual structures of a QKDN and a user network

- from Recommendation ITU-T Y.3800

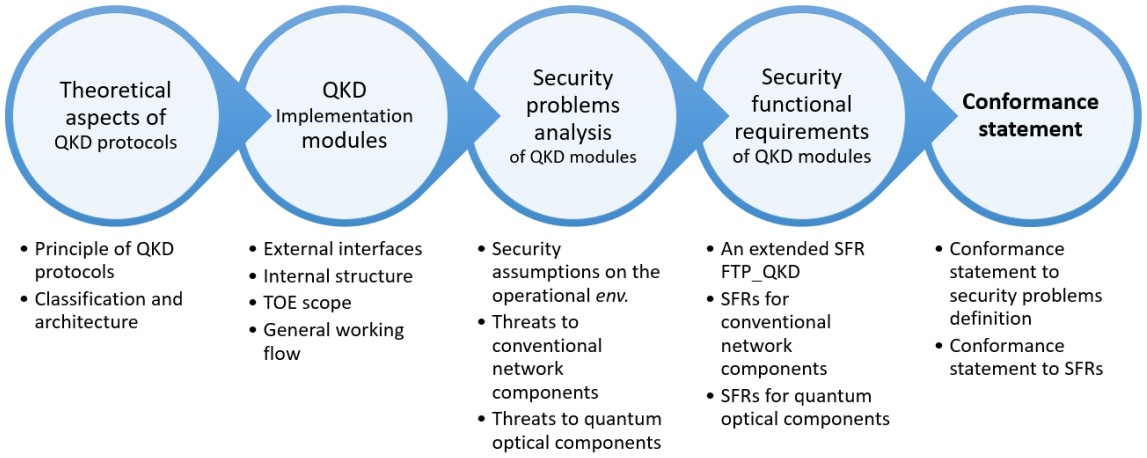
Position of ISO/IEC 23837



- Provide a high-level framework for standardizing the security evaluation methods and activities for QKD modules under ISO/IEC 15408 *(i.e., the Common Criteria for IT security evaluation)*
  - Specify a baseline set of **Security Functional Requirements** (SFRs), and relevant **Evaluation Activities** (EAs)
  - Serve as a basis for developing relevant **Protection Profiles** (PPs) and **Security Targets** (STs)
  - The document is not organized by **Evaluation Assurance Levels** (EALs)
    - *Instead, SFRs and EAs for functional conformance test and vulnerability assessment (up to EAL5 + AVA_VAN.5) are specified*
    - *Specification of expected EALs are left to be specified by PP/STs of QKD modules*

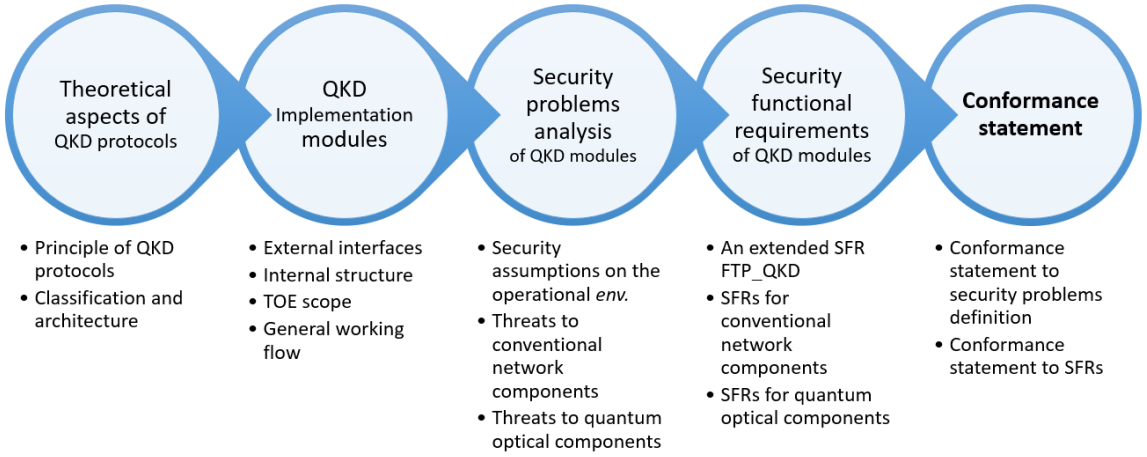
Theoretical aspects of QKD protocols

- The main body consists of 5 parts

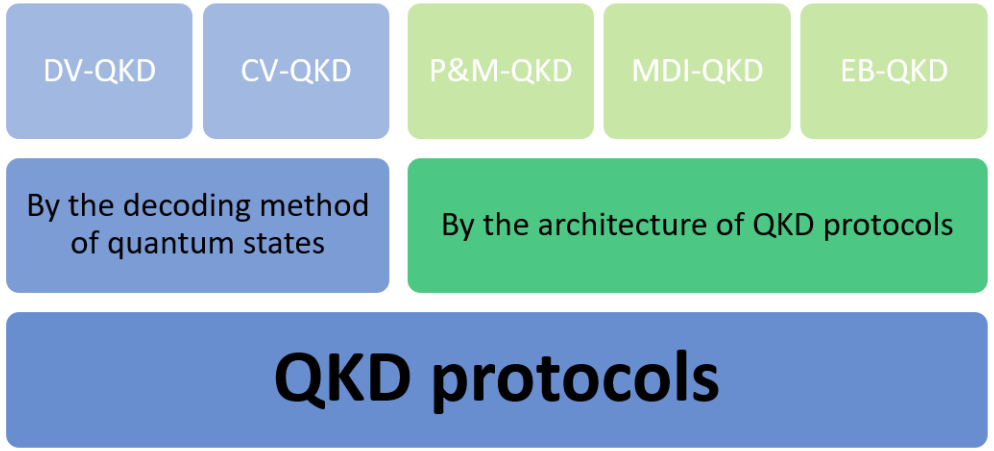


Theoretical aspects of QKD protocols

- The main body consists of 5 parts

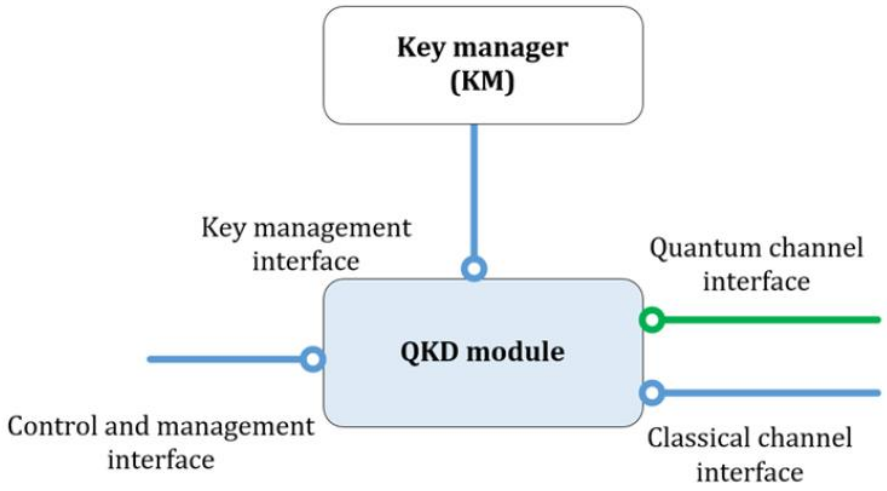


- The possible QKD protocols are covered

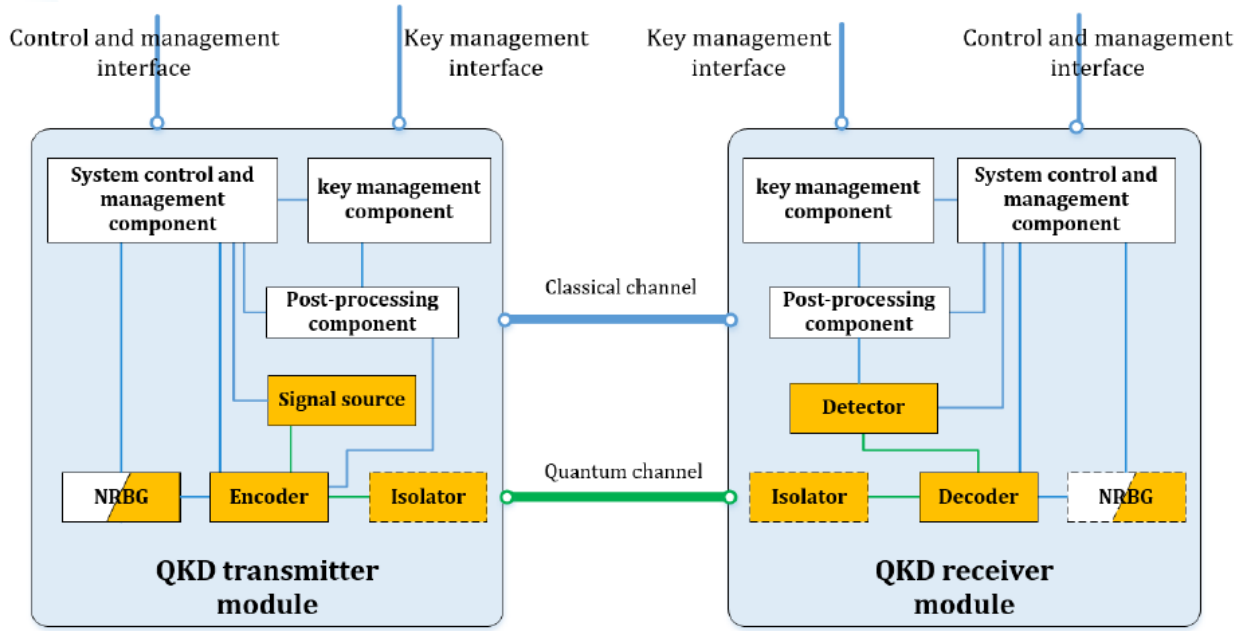


QKD implementation modules

- External interfaces of QKD modules

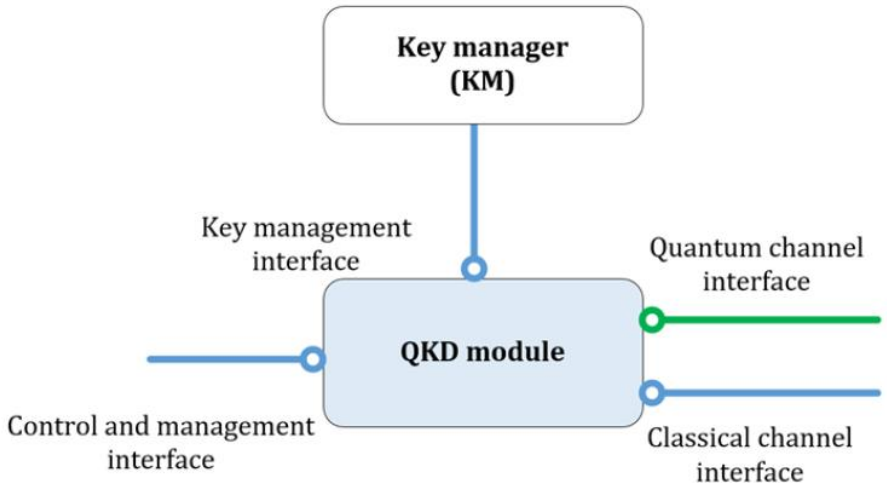


- Generic structure of QKD modules

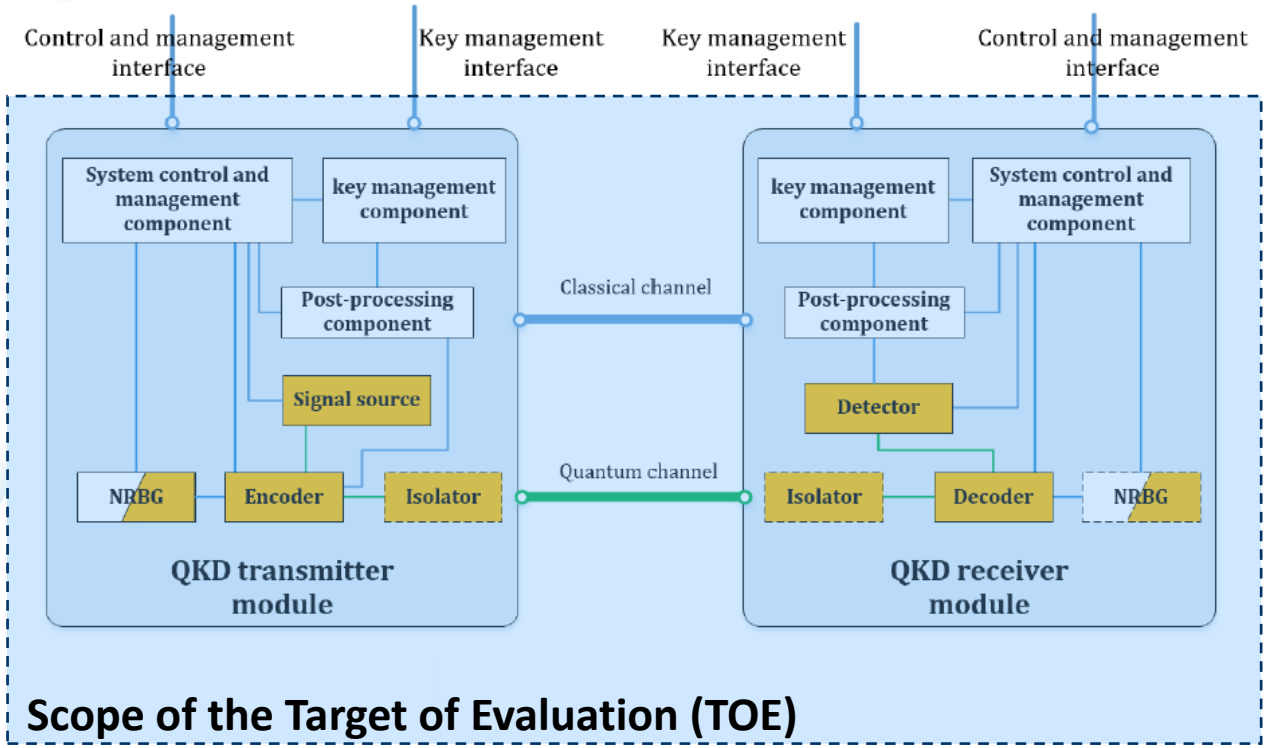


QKD implementation modules

- External interfaces of QKD modules



- Generic structure of QKD modules



- The two modules and their external interfaces
- The classical channel and quantum channel are excluded

Security problems analysis

Assets to be protected

The final key

The relevant security-related information shall also be protected

- *the raw data, sifted data, error corrected data produced during the execution*
- *The QKD authentication key for message authentication over the classical channel*
- *The keys used for the confidentiality and integrity protection of communications between the KM and the QKD module for final key uploading*

The functionalities of QKD modules

need to be protected from misuse by illegitimate users

Assumptions for the security of QKD modules

The QKD module is physically protected in its operational environment

- *The TOE is assumed to operate in a protected environment such that any threat agents cannot approach the QKD module*
- *This assumption is not meant to remove the possible threats via the external interfaces to the QKD module*

Operators are trusted

- *It is assumed that operators (including system administrator, auditor or any other legitimate roles operating the TOE) of the TOE act in the best interest of security for the 833 organization*

The pre-shared key is confidential and randomly generated before it is input into the QKD module

Security problems analysis

- Threats to QKD modules

Threats to conventional network components

- Audit circumvention
- Cryptographic vulnerability exploitation
- Failure exploitation
- Functions abuse
- **Physical security violation**
- Randomness defect exploitation
- Residual data misuse
- Unauthorized access

Threats to quantum optical components

- Threats exploiting optical source flaws
- Threats exploiting optical detection vulnerabilities
- Threats exploiting parameter adjustment vulnerabilities

- As for physical security violation, this document only considers remotely exploitable physical non-invasive attacks
  - *timing attacks*
  - *cache-timing attacks*
  - *or any other attacks not requiring direct contact with the QKD module to retrieve exploitable side-channel information*

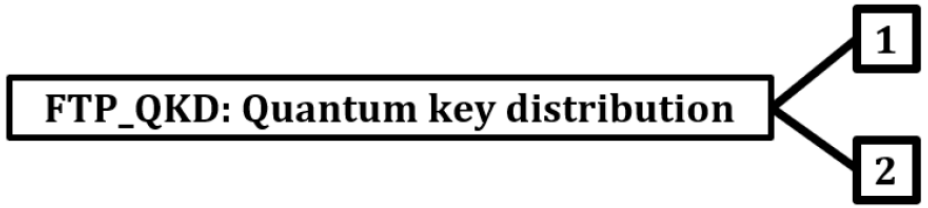
Table 11 — Assignment of FPT_PHP.3.1

Physical tampering scenarios	TSF devices/elements
Trojan horse attack	Encoder, Decoder
Laser damaging attack	Encoder, Decoder
Laser seeding attack	Encoder
Phase-remapping attack	Encoder
Pulse energy monitor attack	Encoder
Wavelength-dependent attack	Decoder
Detector blinding attack	Detector
Detector efficiency attacks	Detector
After-gate attack	Detector
Detector superlinearity attack	Detector
Dead time attack	Detector
Double-click attack	Detector
Parameter adjustment attack	QKD module
Local oscillator attack	QKD module

Security functional requirements

- The security functional requirements relevant for QKD protocols are defined by an extended security functional family FTP_QKD

- Why this extension of security function components?
  - *The standardized security functional class FTP (Trusted path/channels) in ISO/IEC 15408-2 is defined to specify requirements on the establishment of a trusted channel between network-connected parties*
  - *QKD protocols can be used to achieve a similar goal (by noting that the final key generated by QKD protocols can be used to establish trust channels between the users of the keys), thus it is appropriate to extend the security functional components in the class of FTP to cover QKD security functions.*



Security functional requirements

- The extended family FTP_QKD

FTP_QKD.1 QKD protocol and raw key generation

The component requires symmetric keys to be established in accordance with a defined protocol involving the transmission and detection of quantum signals. This includes configurations negotiation and parameter adjustment where needed.

a) FTP_QKD.1.1

The TSF shall implement [assignment: *QKD protocol*] acting as [assignment: *defined protocol role(s)*].

b) FTP_QKD.1.2

The TSF shall implement one or more of the following mechanisms: [assignment: *list of secure message authentication schemes*] to authenticate relevant data transmitted over the classical channel, according to the following rules: [assignment: *list of rules for carrying out the authentication*].

c) FTP_QKD.1.3

The TSF shall permit [assignment: *list of QKD modules of the TOE*] to initiate execution of the QKD protocol.

d) FTP_QKD.1.4

The TSF shall enforce the following static protocol options: [assignment: *list of options*].

e) FTP_QKD.1.5

The TSF shall negotiate one of the following protocol configurations between the QKD modules of the TOE: [assignment: *list of configurations*] over the classical channel.

f) FTP_QKD.1.6

The TSF shall initiate [assignment: *list of parameter adjustment procedures*] to adjust parameters of it, with each of the assigned parameter adjustment procedures specified as follows:

1) **Trigger methods: [selection: *on demand by an authorized user, triggered by [assignment: list of detected failure events], triggered by [assignment: list of other trigger events]*];**
2) **Restrictions on execution: [selection, choose one of: allowed *to run simultaneously with QKD session(s), not allowed to run simultaneously with QKD session(s), [assignment: list of other restrictions]*];**
3) **Parameters to be adjusted: [assignment: *list of parameters to be adjusted*].**

g) FTP_QKD.1.7

During the execution of a parameter adjustment procedure, the TSF shall preserve a secure state. The TSF shall not execute any parameter adjustment procedure simultaneously with a QKD session, unless the parameter adjustment procedure is allowed to run simultaneously with QKD session(s).

h) FTP_QKD.1.8

The TSF shall indicate the status when the TOE is running the following operations: [selection: *key generation, parameter adjustment procedures not allowed to run simultaneously with, or [assignment: list of other operations]*].

i) FTP_QKD.1.9

The TSF shall generate raw data and pass it to the post-processing procedure.

Security functional requirements

- The extended family FTP_QKD

FTP_QKD.1 QKD protocol and raw key generation

The component requires symmetric keys to be established in accordance with a defined protocol involving the transmission and detection of quantum signals. This includes configurations negotiation and parameter adjustment where needed.

a) **FTP_QKD.1.1**

The TSF shall implement [assignment: *QKD protocol*] acting as [assignment: *defined protocol role(s)*].

b) **FTP_QKD.1.2**

The TSF shall implement one or more of the following mechanisms: [assignment: *list of secure message authentication schemes*] to authenticate relevant data transmitted over the classical channel, according to the following rules: [assignment: *list of rules for carrying out the authentication*].

c) **FTP_QKD.1.3**

The TSF shall permit [assignment: *list of QKD modules of the TOE*] to initiate execution of the QKD protocol.

d) **FTP_QKD.1.4**

The TSF shall enforce the following static protocol options: [assignment: *list of options*].

e) **FTP_QKD.1.5**

The TSF shall negotiate one of the following protocol configurations between the QKD modules of the TOE: [assignment: *list of configurations*] over the classical channel.

f) **FTP_QKD.1.6**

The TSF shall initiate [assignment: *list of parameter adjustment procedures*] to adjust parameters of it, with each of the assigned parameter adjustment procedures specified as follows:

1) **Trigger methods: [selection: *on demand by an authorized user, triggered by [assignment: list of detected failure events], triggered by [assignment: list of other trigger events]*];**
2) **Restrictions on execution: [selection, choose one of: allowed *to run simultaneously with QKD session(s), not allowed to run simultaneously with QKD session(s), [assignment: list of other restrictions]*];**
3) **Parameters to be adjusted: [assignment: *list of parameters to be adjusted*].**

g) **FTP_QKD.1.7**

During the execution of a parameter adjustment procedure, the TSF shall preserve a secure state. The TSF shall not execute any parameter adjustment procedure simultaneously with a QKD session, unless the parameter adjustment procedure is allowed to run simultaneously with QKD session(s).

h) **FTP_QKD.1.8**

The TSF shall indicate the status when the TOE is running the following operations: [selection: *key generation, parameter adjustment procedures not allowed to run simultaneously with, or [assignment: list of other operations]*].

i) **FTP_QKD.1.9**

The TSF shall generate raw data and pass it to the post-processing procedure.

Security functional requirements

- The extended family FTP_QKD

FTP_QKD.2 QKD post-processing

a) **FTP_QKD.2.1**

The TSF shall implement the post-processing procedure aligned with the QKD protocol specified in FTP_QKD.1.1.

b) **FTP_QKD.2.2**

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: *sifting schemes*] for sifting.

c) **FTP_QKD.2.3**

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: *parameter estimation schemes*] for parameter estimation.

d) **FTP_QKD.2.4**

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: *error correction schemes*] for error correction.

e) **FTP_QKD.2.5**

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: *privacy amplification schemes*] for privacy amplification.

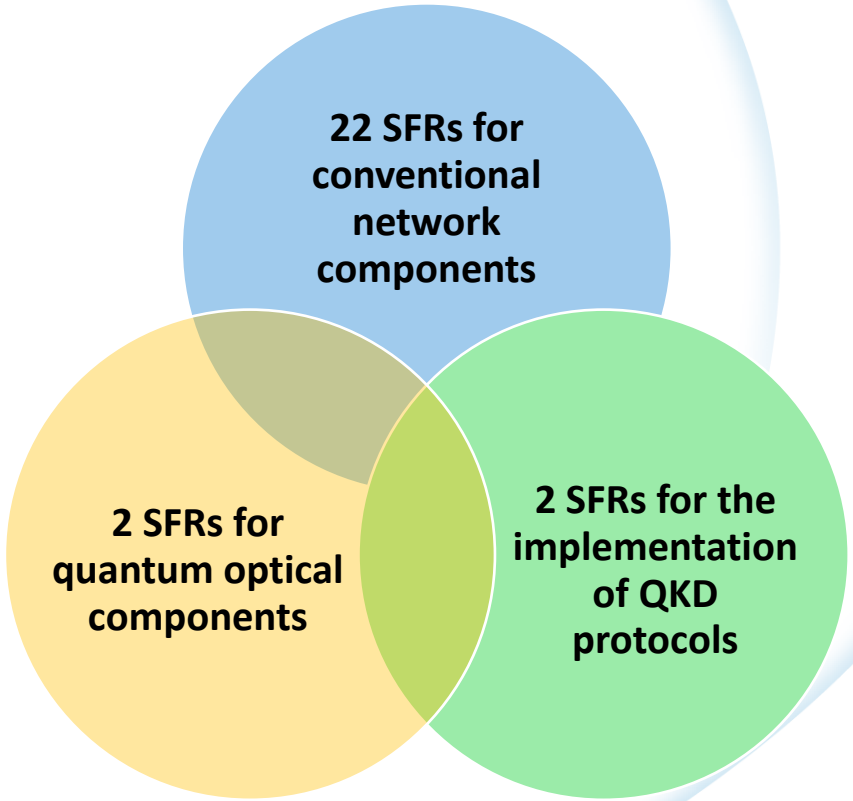
f) **FTP_QKD.2.6**

During the post-processing stage, the TSF shall check the consistency of the relevant keying material between the QKD modules of the TOE after error correction or the chosen error correction scheme includes the consistency check. This integrity check shall use one or more of the following consistency check schemes: [selection: *error correction schemes, [assignment: list of other schemes]*]. If an inconsistency is detected the TSF shall [selection: *abort the QKD session without producing a final key, [assignment: list of actions]*].

The component requires symmetric keys to be securely established by the QKD modules from the raw data according to the QKD protocol

Security functional requirements

- A baseline set of Security Functional Requirements (SFRs)



- The SFRs are chosen from ISO/IEC 15408-2 or extended components to resist the possible threats analyzed
- Requirements and recommendations for the completion of operations in the SFRs are given as application note for each SFR

9.2.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application note:

This requirement is intended to protect the QKD module from the threats of cryptographic analysis and unauthorized access.

The first assignment specifies the cryptographic algorithms, which may provide:

— Confidentiality and integrity protection of the communications between a QKD module and an external KM;

— Confidentiality and integrity protection of the communications between a QKD module and an operator via the control and management interface;

— Support to the user authentication function.

Conformance statement to ISO/IEC 23837-1

- To provide enough **flexibility for implementations** by considering the various implementations of QKD modules and their operational environment
- The requirements for a PP/ST to claim conformance
  - Generally, the PP/ST shall offer a solution to the generic security problem described in this document, mainly related to the security problem definition and the security functional requirements.
  - The PP/ST may do so in any way that is equivalent to or more restrictive than the requirements in this document
    - *The PP/ST may include statements that vary from the relevant content in this document, provided that overall the PP/ST requires equal or even stronger restrictions on the TOE,*
    - *combined with either equal or weaker assumptions on the operational environment of the TOE*
  - In order to provide more flexibility in practice, some permitted exceptions to conformance are described
    - *Replacing, adding assumptions on the operational environment*
    - *Removing, tailoring and adding SFRs*

Structure of ISO/IEC 23837-2

- The evaluation method for QKD modules are considered under ISO/IEC 18045

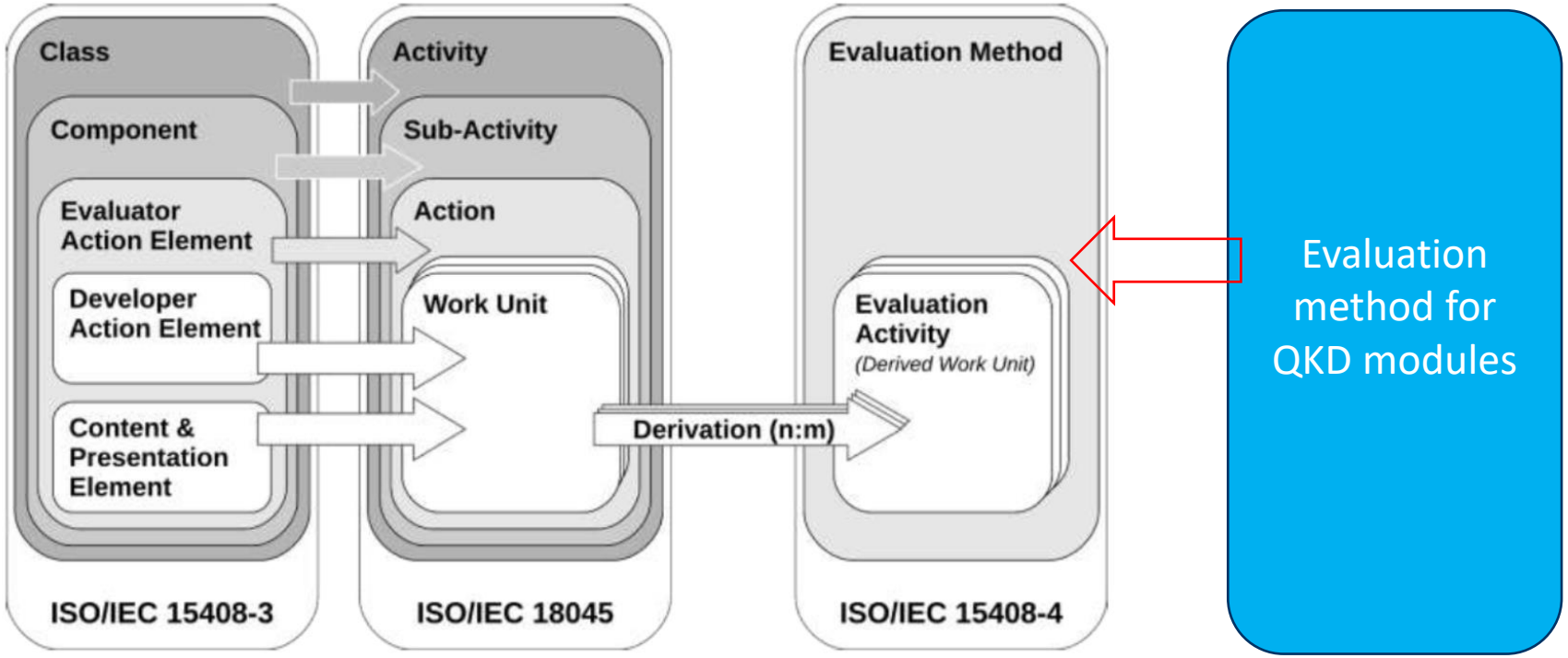
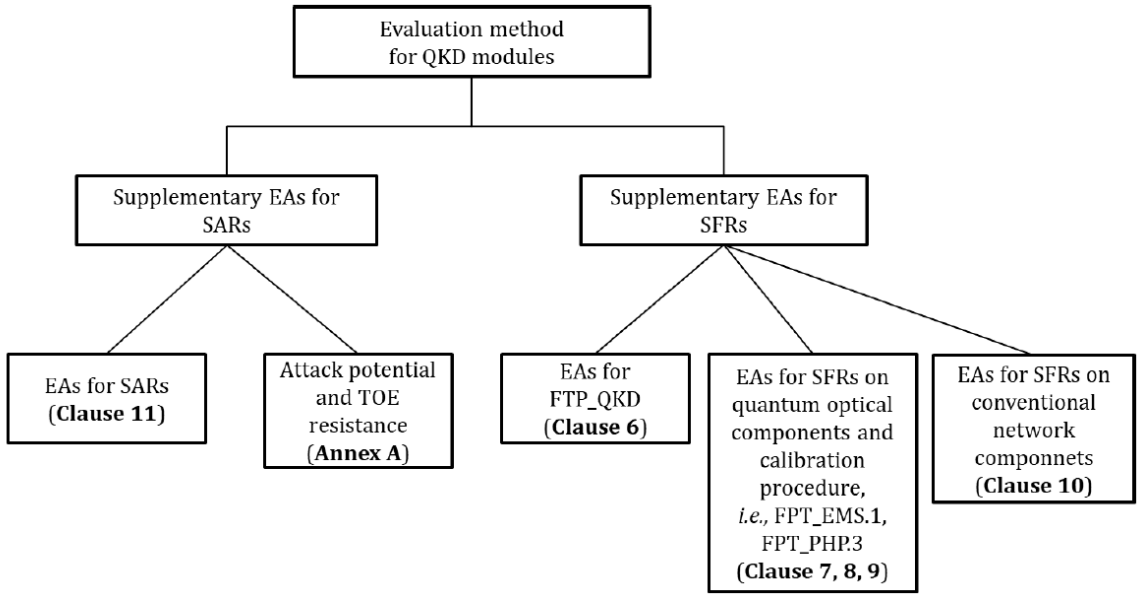
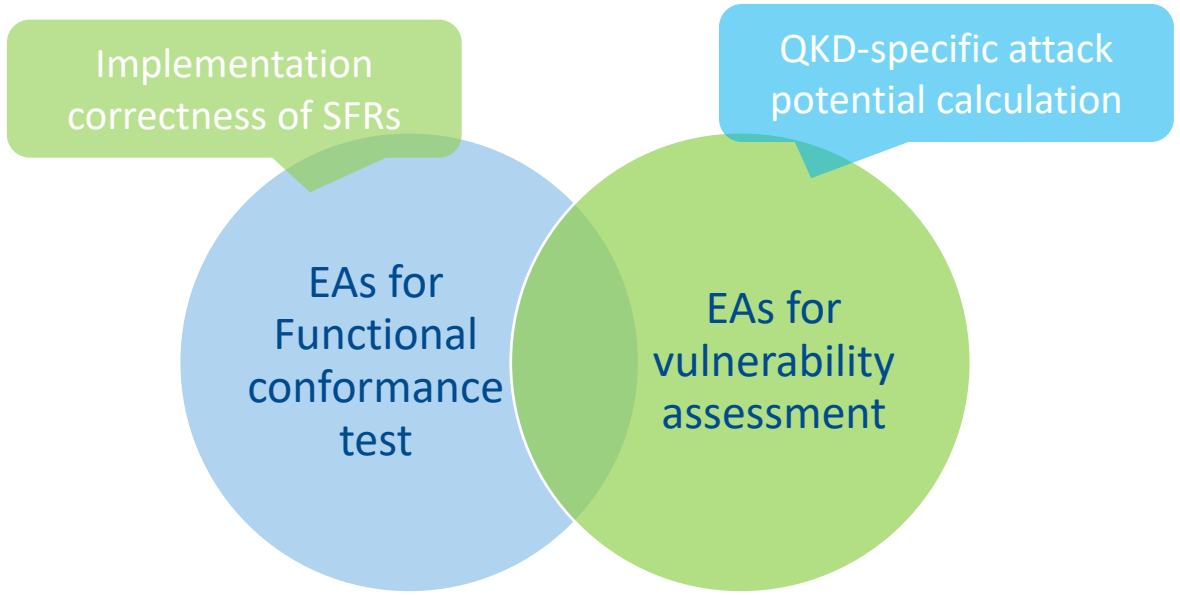


Figure 1 - Mapping of ISO/IEC 15408-3 and ISO/IEC 18045 structures to ISO/IEC 15408-4 structures

Structure of ISO/IEC 23837-2

- Evaluation method for QKD modules





EAs in ISO/IEC 23837-2

- The evaluation method is composed of dozens of defined Evaluation activities

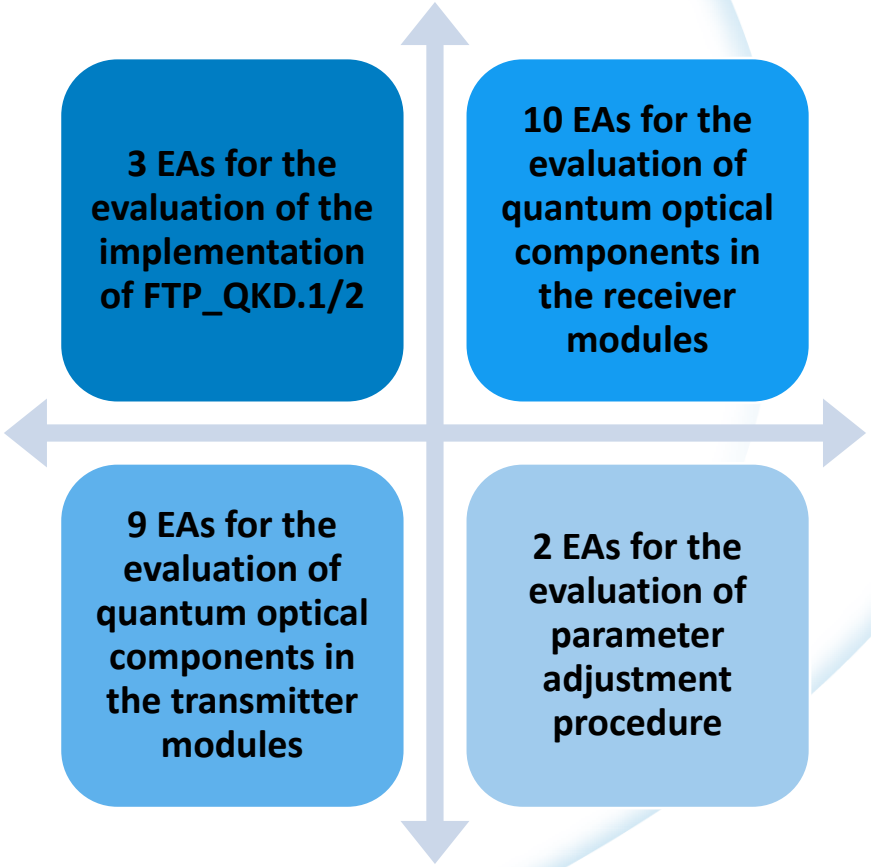


Table 1 — EAs for the evaluation of FTP_QKD

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test quantum state transmission and sifting procedures	Test the correctness of functionality of quantum state encoding, transmission and detection and the related generation of raw data between the TX module and the RX module, and sifting of the resulting data in post-processing procedures	FTP_QKD.1 FTP_QKD.2	6.2	DV-P&M-QKD; DV-MDI-QKD; DV-EB-QKD; CV-P&M-QKD; CV-MDI-QKD; CV-EB-QKD
Test other post-processing procedures	Test the correctness of the implementation of the post-processing procedures in the TOE, subsequent to any sifting that forms part of the QKD protocol	FTP_QKD.2	6.3	DV-P&M-QKD; DV-MDI-QKD; DV-EB-QKD; CV-P&M-QKD; CV-MDI-QKD; CV-EB-QKD
Test parameter adjustment procedure(s)	Test the correctness of the implementation of the parameter adjustment procedure(s) in the TOE	FTP_QKD.1	6.4	DV-P&M-QKD; DV-MDI-QKD; DV-EB-QKD; CV-P&M-QKD; CV-MDI-QKD; CV-EB-QKD

EAs in ISO/IEC 23837-2

- Inside each EA for SFR

General aspects

- Objective of the evaluation activity
- Required inputs
- Required tool types and setup
- Rationale
- Dependencies

Test procedure

Pass/fail criteria

- General procedures for testing are specified, different testing method are permitted for conformance if justified
- Pass/fail criteria are defined with some non-specified thresholds so as to allow flexibility and improve applicability of the evaluation method, concrete values for thresholds can be set in PP/STs

7.3.3 Pass/fail criteria

If each of the $K \times M$ measured mean photon numbers is within the range defined by *threshold_mpn_min_k* and *threshold_mpn_max_k*, the test is passed; otherwise, it is failed.

Table 6 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 6 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	*threshold_mpn_min_k*	The minimum acceptable mean photon number (this threshold may be zero). There is one such threshold for each intensity *k* that the TX module is required to emit under a QKD protocol.
2	*threshold_mpn_max_k*	The maximum acceptable mean photon number output by the TX module. There is one such threshold for each intensity *k* that the TX module is required to emit under a QKD protocol.

EAs in ISO/IEC 23837-2

- The recommended calculation of attack potential

Table A.1 — Calculation of attack potential

Factor	Value	
	Identification	Exploitation
Elapsed Time		
<= one day	0	0
<= one week	1	2
<= two weeks	2	4
<= one month	4	8
<= three months	8	12
> six months	12	16
Expertise		
Laymen	0	0
Proficient	2	4
Expert	4	8
Multiple experts	8	12 or *
Knowledge of TOE		
Public	0	0
Restricted	2	2 or **
Sensitive	4	4 or **
Critical	8	8 or **
Window of Opportunity		
Unlimited access	0	0
Easy	1	2
Moderate	2	4
Difficult	4	8
Not practical	#	#
Equipment		
Standard	0	0
Specialized	2	4
Bespoke	4	8

Conformance statement to ISO/IEC 23837-2

- To provide enough **flexibility for evaluations** by considering the various implementations of QKD modules and their operational environment
- The requirements for conformance
  - Generally, when an evaluation process claims to conform to ISO/IEC 23837-2, it means the method used in the evaluation process of QKD modules follows exactly the specified EM and then EAs in this document for all the related SFRs and SARs.
  - The evaluator shall demonstrate that the new EM and EAs used for evaluation are equivalent or more restrictive than those specified in this document.
  - In order to provide more flexibility in practice, some permitted exceptions to conformance are described
    - *omitting, adding EAs when doing evaluation if it can be justified appropriately*

The next

- Prepare and submit the final documents for publication according to the directives of ISO
- Build protection profiles for specific QKD protocols and implementations
  - Consider to establish *iTC* in the Common Criteria User Forum (CCUF) to develop collaborative Protection Profile (cPP)
  - The standard can find more compatible applications if QKD protocols can be standardized internationally, *considering the completion of FTP_QKD.1.1*
- Apply the standard to perform security evaluation in near future
- More cooperation within the community are required to promote QKD technology

Further Questions?

Contact

hsshi@163.com