8th Nov. 2022
ITU Workshop on
"Quantum key distribution protocols, security and certification"

Japan activities for QKD standardization and certification development

Kaoru Kenyoshi, NICT, Japan
○ Yoshimichi Tanizawa, Toshiba, Japan

- This work is partly supported by the Ministry of Internal Affairs and Communications (MIC), “R&D of ICT Priority Technology Project (JP MI00316)”.
- A part of this work was performed for Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Photonics and Quantum Technology for Society 5.0”(Funding agency : QST).

Contents:

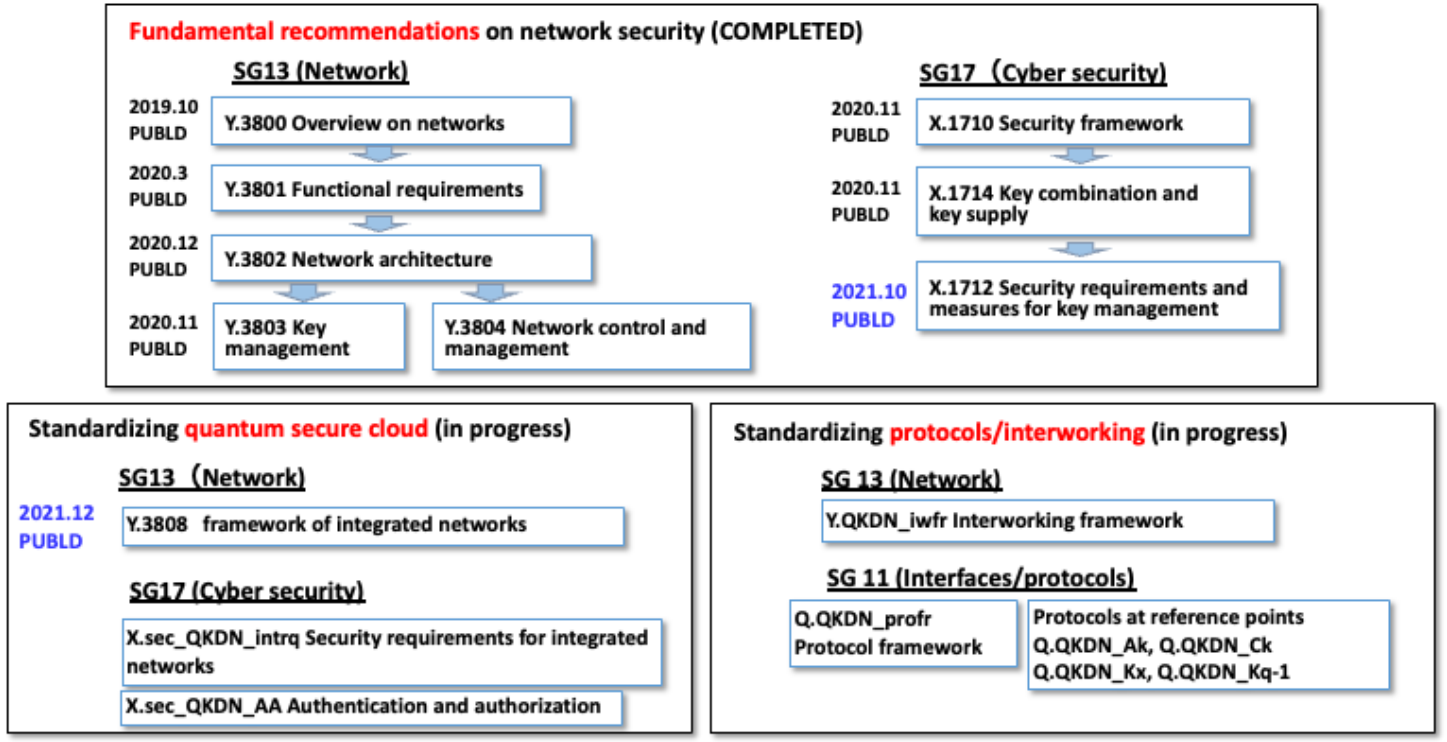
- Japan contribution to QKD standard
- QKD certification scheme (plan)

Japan’s standardization activities

- Japan team* contributes to QKD standardization activities both on QKD modules and on QKDN, which cover ITU-T, ISO/IEC JTC1, and ETSI.

*The Japan team comprises NICT, Toshiba, NEC, Hokkaido Univ., Tokyo Univ. Keio Univ., ECSEC Laboratory (technical support) and Japanese government ministries.

Japan’s standardization activities on QKDN



We contribute and develop 10+ recommendations related to QKDN in SG13, SG17, and SG11.

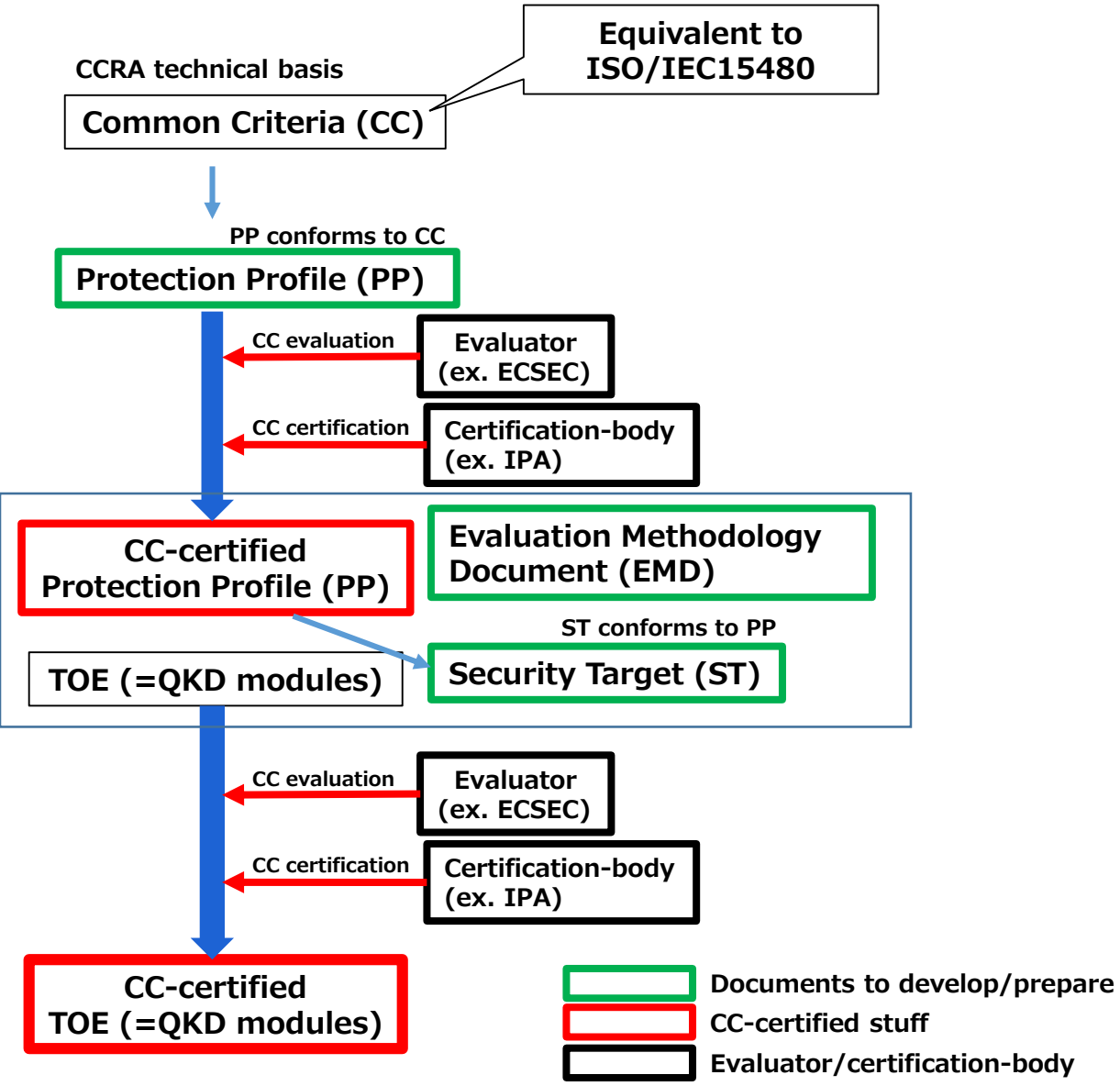
Japan's standardization activities on QKD modules

	Organization	
	ISO/IEC JTC1/WG3	ETSI ISG QKD
Period	Sep 2018 ~	Nov 2018 ~
Drafting	23837-1, 23837-2 (*1)	ISG-QKD 016 PP(EAL4+) (*2)
Japan contributions	39 contributions	160 rev comments

We contribute both to ISO/IEC and to ETSI to develop the QKD security criteria documents.

*1 ISO/IEC **DIS** 23837-1 Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements, SO/IEC **DIS** 23837-2 Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods
*2 ETSI ISG-QKD 016, ETSI ISG-QKD Quantum Key Distribution (QKD); Common Criteria Protection Profile Pair of Prepare and Measure Quantum Key Distribution Modules (**draft**)

Procedures to certify TOE* in the Common Criteria ("CC") framework



- CC-certification system comprises evaluating and certifying whether TOE meets the requirements defined in CC or not. In preparation for CC-certification, we define TOE, develop Protection Profile ("PP") and Evaluation Methodology Document ("EMD") and prepare Security Target ("ST").
  - **TOE**: Target-of-Evaluation. Here, a pair of QKD modules is the TOE.
  - **PP**: Protection Profile. A minimal, baseline set of requirements targeted at mitigating well defined and described threats against the TOE.
  - **EMD**: Evaluation Methodology Document. It defines the refinements of the measures taken during development and evaluation of the TOE.
  - **ST**: Security Target. It identifies the security properties of the TOE.
- A product that has been CC-certified in one of the Certificate Authorizing Members will mutually be recognized as certified in other Certified Authorizing Members and Certificate Consuming Members.

What Japan is now developing

- **EAL2 PP (Protection Profile)**
  - PP specifies the high-level requirement of QKD system
  - Japan develops **EAL2 PP**, which is targeting Japan/US market / private sectors.
  - ETSI develops **EAL4+ PP**, which is targeting EU market.
  - Japan team collaborates with ETSI for developing EAL4+ PP/EAL2 PP.

- **EMD (Evaluation method document), or SD (Supporting Document)**
  - The EMD document is being developed for supporting the above **EAL2 PP**, as well as **EAL4+ PP**.
  - Japan team again collaborates with ETSI for developing EMD.

QKD certification scheme (plan): How the scheme works

- EAL2 PP assume QKD protocol as P&M type protocol, as same as ETSI EAL4+ PP.
- There are many types of implementations and theories of P&M QKD.
- In PP (both of EAL2 and EAL4+), developer must specify a theory that TOE supports in ST.
- The list of acceptable or recommended theory would be provided by an authorized technical expert community of a certification body. PP developer can select theory from the list.
- ST specifies theory in the acceptable list and evaluator evaluates the TOE assuming the specified theory.

Example of theory

M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express 21, 24550-24565 (2013)
https://opg.optica.org/oe/fulltext.cfm?uri=oe-21-21-24550&id=268752

Key rate calculation

$$R_Z = (C_{uZZ} / N_{uZZ}) \cdot r$$

$$= \min\left\{e^{-u}\tilde{y}_Z^{(0)} + ue^{-u}\tilde{y}_Z^{(1)}[1-h(\tilde{q}_X^{(1)})]\right\} - \frac{C_{uZZ}}{N_{uZZ}} f_{EC} h(Q_Z) - \frac{\Delta}{N_{uZZ}} \quad (6)$$

$$= \left\{e^{-u}\underline{y}_Z^{(0)} + ue^{-u}\underline{y}_Z^{(1)}[1-h(\bar{q}_X^{(1)})]\right\} - \frac{C_{uZZ}}{N_{uZZ}} f_{EC} h(Q_Z) - \frac{\Delta}{N_{uZZ}} \quad (7)$$

optimization

$$\underline{y}_Z^{(k)} = \min_{I_{\varepsilon_{PE_Y}}}[\tilde{y}_Z^{(k)}], \quad k=\{0,1\}, \quad \text{and} \quad \bar{q}_X^{(1)} = \max_{I_{\varepsilon_{PE_B}}}[\tilde{q}_X^{(1)}].$$

$$Y_{\mu_j Z}^{-} \le \sum_k \frac{e^{-\mu_j}(\mu_j)^k}{k!}\tilde{y}_Z^{(k)} \le Y_{\mu_j Z}^{+}, \ j=\{0,1,2\}, \quad (11)$$

$$B_{\mu_j X}^{-} \le \sum_k \frac{e^{-\mu_j}(\mu_j)^k}{k!}\tilde{y}_X^{(k)}\tilde{q}_X^{(k)} \le B_{\mu_j X}^{+}, \ j=\{0,1,2\}. \quad (12)$$

- The QKD theory is defined as numerical formulas and several conditions/assumptions based on quantum information theory.
- These types of theory are usually submitted and published as technical and theory papers.

Summary of certification scheme we assume in Japan

- Evaluation criteria: EAL2 PP
  - Based on **ETSI EAL4+ PP**(*1) descriptions
  - The theory the target product based on is referred from **authorized technical expert**.

- Evaluation method: EMD (SD)
  - Partly based on **ISO/IEC 23837** (*2) descriptions.

*1 ETSI ISG-QKD 016, ETSI ISG-QKD Quantum Key Distribution (QKD); Common Criteria Protection Profile Pair of Prepare and Measure Quantum Key Distribution Modules (**draft**)
*2 ISO/IEC **DIS** 23837-1 Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements, SO/IEC **DIS** 23837-2 Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods

conclusion

- Certification scheme plan in Japan was presented.
- Scheme should depend on each country rule/restriction/intention.
- Similar or same scheme based on standardization is preferable for QKD global market growing.