TTC標準草案
（Draft TTC Standards）

Network Vision専門委員会

2020年9月23日

新規標準の制定について（JT）

- 我が国では、2010年に構築した実証テストベッドTokyo QKD Networkで量子鍵配送(QKD)ネットワーク技術の開発、長期運用試験、様々なセキュリティアプリケーションの開発に取り組んでいる。 Y.3800は、ITU-T初のQKDに関する国際標準として2019年10月ITU-T SG13会合にて承認された。本勧告には、日本のQKDネットワーク技術をベースとする提案が採用され、その骨格を形成している。
- ITU-T 勧告Y.3800は、QKDネットワークの能力、及び基本構成と機能などを規定する。 ITU-T 勧告Y.3801は、Y.3800をベースとして、QKDNの機能要求条件を規定する。 ITU-Tでのこれらの国際標準の成立により、QKDを用いた秘匿性の高い暗号通信サービスの実用化と普及が加速すると期待される。
- 国内ではQKDNの商用化に向けたプロジェクトが進んでいる。Y.3800の完成により、関連する標準化の検討が加速し、 QKD関連の製品開発やサービス創出に向けて企業が投資しやすくなり、ユーザは導入を検討しやすくなると期待される。

QKDN関連 JT標準

- Network Vision専門委員会は、国内のQKDN製品開発、市場拡大、普及促進のため、以下のQKDN関連のITU-T勧告をベースとするTTC標準の制定を提案する。

		標準類	版数	タイトル
1	新規	JT-3800	1	量子鍵配送ネットワークの概要
2	新規	JT-3801	1	量子鍵配送ネットワークの機能要求条件

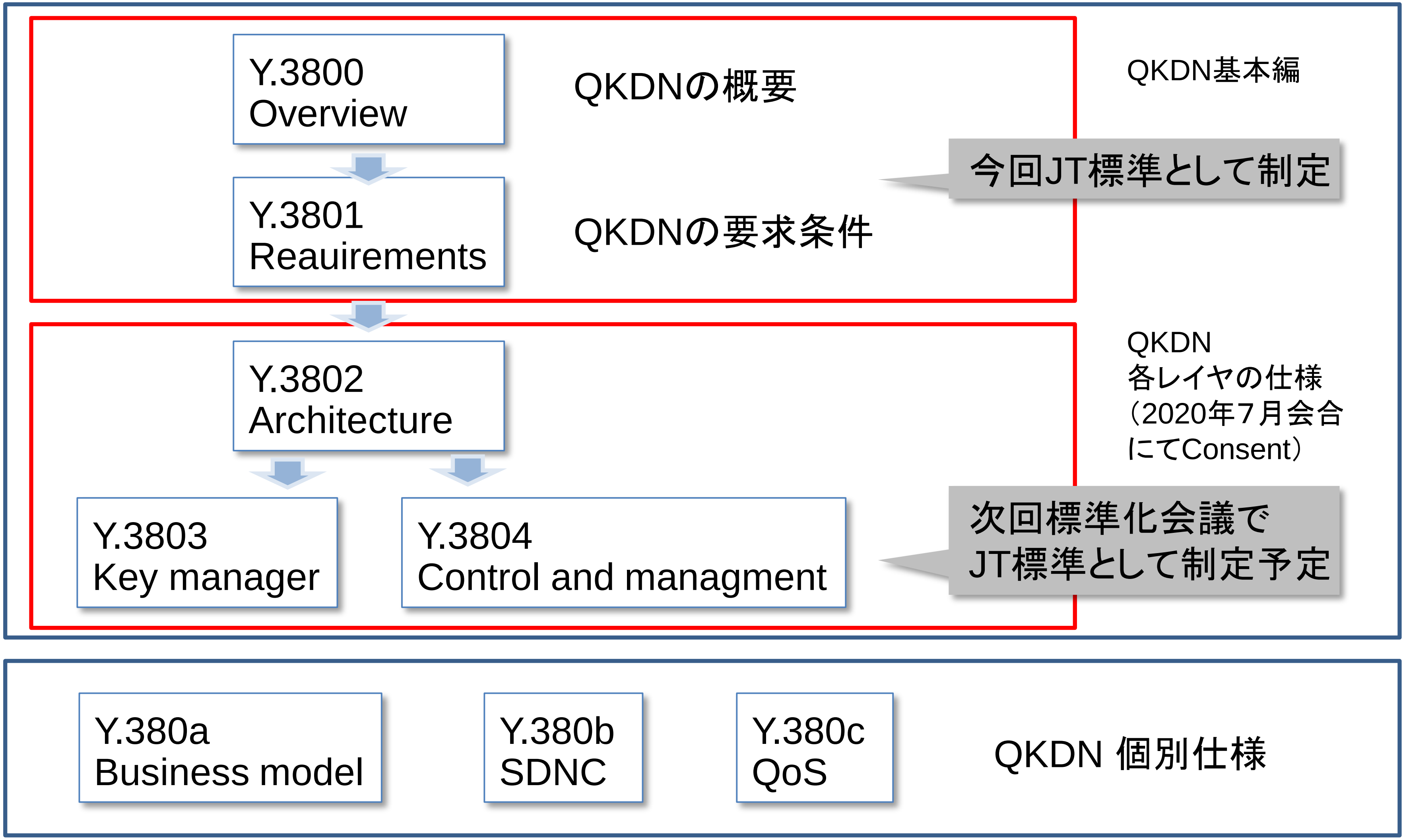
- ITU-T SG13では、Y.3800, Y.3801に続くQKDN関連勧告の開発が進められている。Network Vison専門委員会は、引き続きこれらITU-T勧告をベースとしたTTC標準の開発に取り組み、次回第129回標準化会議に提案する予定である。

		標準類	版数	タイトル
1	新規	JT-3802	1	量子鍵配送ネットワークのアーキテクチャ
2	新規	JT-3803	1	量子鍵配送ネットワークの鍵管理
3	新規	JT-3804	1	量子鍵配送ネットワークの制御と管理

付録
JT標準のベースとなるITU-T勧告の概要

ITU-T SG13: QKDNネットワーク関連の勧告

7月 SG13会合で基本勧告セットが完成



Y.3800
Overview

QKDNの概要

Y.3801
Reauirements

QKDNの要求条件

QKDN基本編

今回JT標準として制定

Y.3802
Architecture

Y.3803
Key manager

Y.3804
Control and managment

QKDN
各レイヤの仕様
（2020年7月会合
にてConsent）

次回標準化会議で
JT標準として制定予定

Y.380a
Business model

Y.380b
SDNC

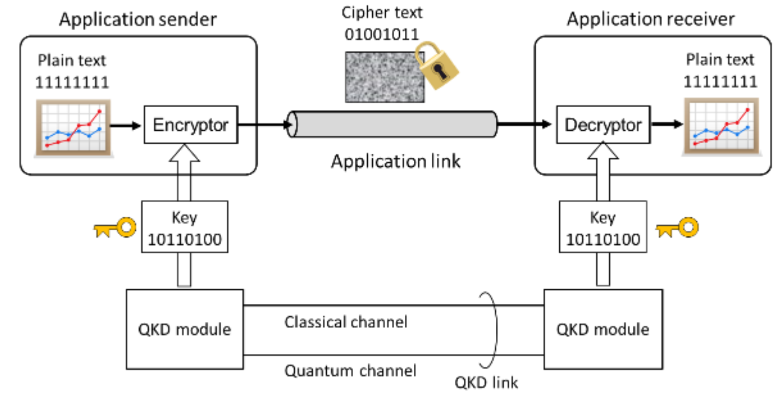
Y.380c
QoS

QKDN 個別仕様

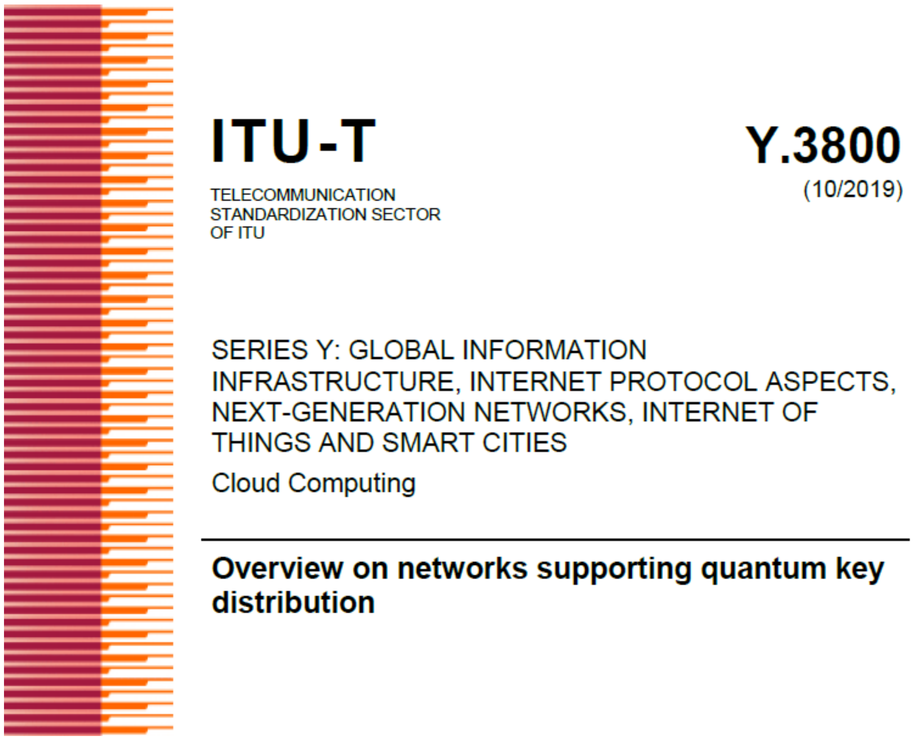
Y.3800: Overview on networks supporting quantum key distribution

SCOPE:

- an overview of QKD technologies;
- network capabilities to support QKD;
- Conceptual structure and basic functions of QKD networks (QKDN)



Basic concept of quantum key distribution



ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3800

(10/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

Overview on networks supporting quantum key distribution

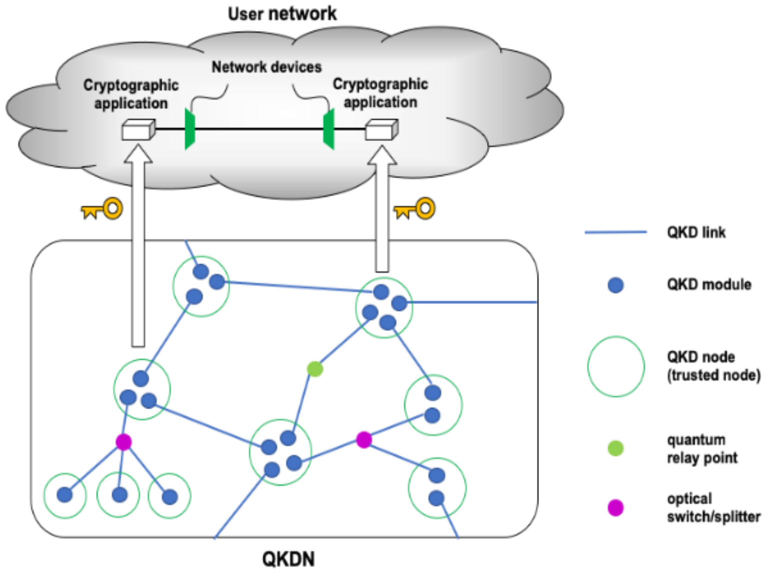


Illustration of QKDN concepts and their relation to a user network

Y.3800: Overview on networks supporting quantum key distribution

QKDネットワークの基本構成と、ユーザーネットワーク（既存NW・アプリケーション）との関係を定義

QKDN design considerations:

- Security, scalability, stability, efficiency, application-oriented, robustness, integratability, interoperability, migratability, manageability

Layer structure of QKDN

- Quantum layer
- Key management layer
- QKDN control layer
- QKDN management layer

Basic functions of QKDN:

- Quantum key generation;
- Key management;
- QKDN control;
- QKDN management.

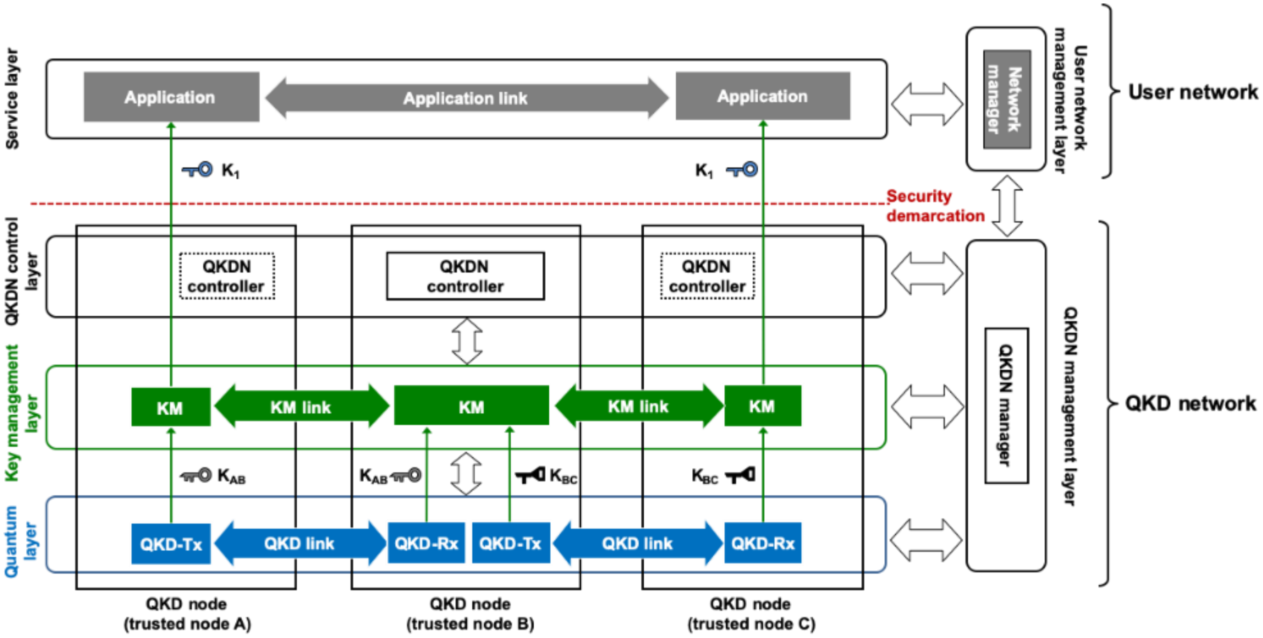


Illustration of the conceptual structures of a QKDN and a user network

Y.3800 Corrigendum

Y.3800が定義する責任分界点(Security demarcation boundary)と情報理論的安全(ITS)の記述がSG17で議論となった。

SG間の整合を図るため、NICTよりSG13とSG17のJoint会合での議論を提案。審議の結果、以下の条文修正を行うことを合意。

Y.3800 corrigendumとして2020年3月SG13会合で承認された。

修正前 **3.2.15 security demarcation boundary**: A security boundary to demarcate quantum key distribution network's responsibility on keys to be supplied from the user network’s responsibility on keys for use.

修正後 **3.2.15 security demarcation boundary**: A boundary to demarcate one layer's responsibility on the keys to be supplied from another layer’s responsibility on the use of keys.

その他、QKDプロトコルはITSだが、QKDNのセキュリティは実装に依存することを明記。

Y.3801: Functional requirements for quantum key distribution network

Y.3800をベースに、QKDNの各レイヤが満たすべき要求条件を規定。

Y.3800承認時に削除したテキストをベースにしたため、比較的短期間(約6ヶ月)で完成。

Functional requirements for quantum layer

To generate keys in a QKDN, QKD protocols should meet the following requirements. (Req_Q.1~Q.7)

Req_Q.1: The QKD protocols are required to be provably secure and allow IT-secure key establishment.
Req_Q.2: The QKD module is required to implement functions that are necessary to execute one or more QKD protocols with a corresponding QKD module connected by a QKD link.
Req_Q.3: The QKD module is required to be contained within a defined cryptographic boundary.

Functional requirements for key management layer

To manage keys in a QKDN securely, reliably and efficiently, a KM should meet the following requirements. (Req_KM.1~KM.11)

Req_KM.1: The KM is recommended to be compatible with various kinds of QKD modules which implement different protocols.
Req_KM.2: The KM is required to receive keys from a QKD module(s) via an appropriate interface, and to store them securely when storage is necessary.
Req_KM.3: The KM is recommended to format keys where necessary for internal purposes or for key supply or key relay, including combining or splitting where lengths are not appropriate.

Functional Requirements for QKDN control layer

To control a QKDN for secure, stable, efficient, and robust operations and services, a QKDN controller should meet the following requirements. (Req_C.1~C.7)

Req_C.1: The QKDN controller is required to provide routing control of key relay if the key relay function is supported by a QKDN.
Req_C.2: The QKDN controller is recommended to provide configuration control of QKD modules, QKD links, KMs and KM links.
Req_C.3: The QKDN controller is recommended to provide charging policy control.

Functional requirements of QKDN management layer

To support monitoring, and management of a QKDN as a whole, and to support user network, management, a QKD manager should meet the following requirements. (Req_M.1~M.11)

Req_M.1: The QKDN manager is required to provide fault management to support:

- collecting/receiving status information provided by the quantum, key management, and control layers;
- analysing the status information collected/received for fault indicators.

Req_M.2: The QKDN manager is recommended to provide fault management to support:

- root-cause analysis capability;
- diagnosis capability;
- management of failure resolving policies, and interactions with relevant functional components for healing actions.

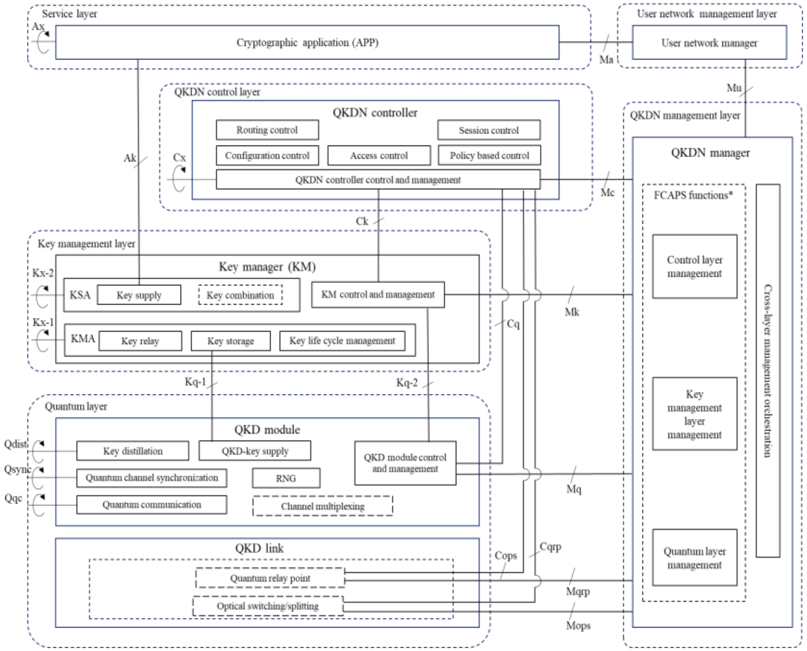
Y.3802 Functional architecture of the QKDN

Y.3801が規定する要求条件を実現するための機能とインタフェースを規定。
様々な実装を想定する論理構成（図左）といくつかの実装モデル（図右）を示す。

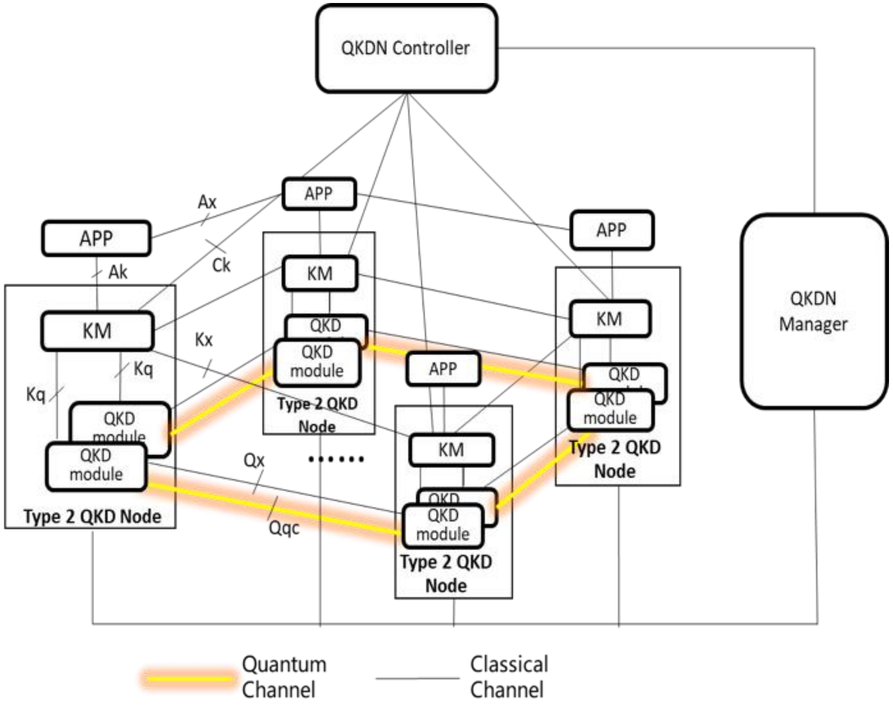
❑ Scope

This Recommendation specifies functional architectures of the Quantum Key Distribution (QKD) network. In particular, the scope of this draft Recommendation includes:

- Functional architecture model
- Functional elements and reference points
- Architectural configurations
- Overall operational procedures



Functional architecture model of QKDN



QKDN Configuration of a centralized QKDN controller

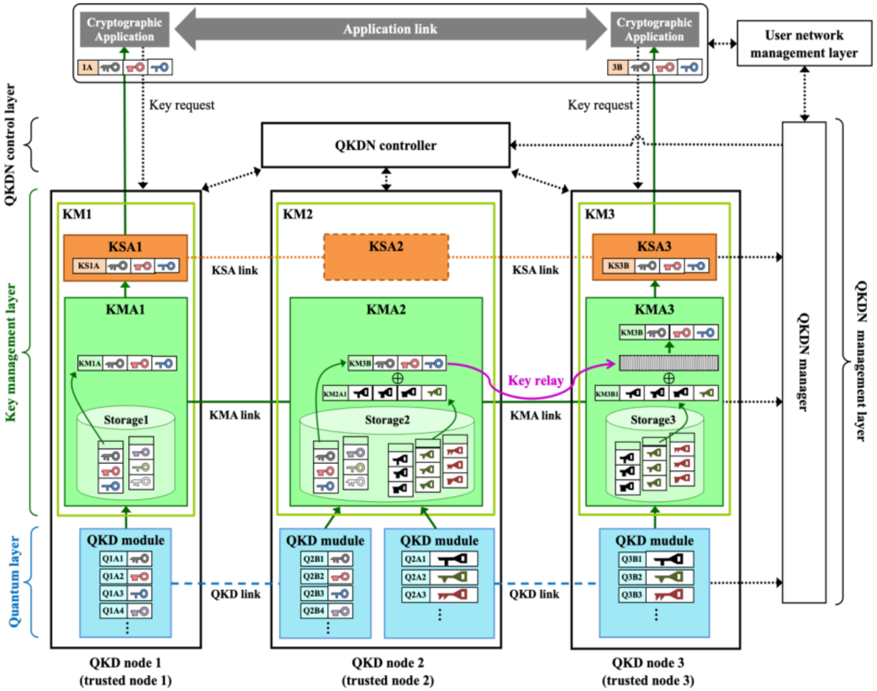
Y.3803 Key management for QKDN

QKDNのコアとなる鍵管理機能（鍵生成から鍵供給まで）の一連の動作を規定。

❑ Scope

This Recommendation describes key management for Quantum Key Distribution (QKD) network which addresses technical specifications to help the implementation and operation. In particular, the scope of this draft Recommendation includes:

- Requirements of key management
- Functional elements of key management
- Procedures of key management
- Key formats (key data and meta-data)



Functional elements and procedure of key management.

Meta-data information

Meta-data	Description	M/O
(1) QKD-key		
QKD-key ID	ID of the QKD-key.	M
Key size	Key size of the QKD-key	M
QKD device ID	ID of the QKD device (Alice or Bob) that generates the QKD-key	M
Generation time stamp	Time stamp of QKD-key generation at the pair of QKD devices	O
Hash value	Hash value of the QKD-key data. (There are several options for hash function, which should be discussed in other Recommendations.)	M
(2) KMA-key		
KMA-key ID	ID of the KMA-key, which should be the same for the pair of keys for Alice and Bob, and unique in a QKD network. A part of the bits of the hash value generated from the names of the pair of QKD devices is often used for this ID.	M
Key size	Key size of the KMA-key	M
Key type	Index to specify whether encrypting key or decrypting key	O
KMA ID	ID of the KMA that stores the KMA-key	M
Generation time stamp	Time stamp of the KMA-key generation at the KMA	O
QKD device ID	ID to identify the QKD device which generates the KMA-key data	O
Matching QKD device ID	ID to identify the matching QKD device which constitutes the pair of Alice and Bob	O

O: Optional, M: Mandatory

Y.3804 Control and management for QKDN

QKDNの制御と管理に関する機能を規定。

❑ Scope

This Recommendation is to specify the control, management, and orchestration for Quantum Key Distribution network.
This recommendation covers:

- Functional architecture of QKDN control, management, and orchestration
- Management information model for QKDN
- Reference points of QKDN control, management, and orchestration
- Procedures of QKDN control, management, and orchestration
- Appendix: Informative procedures of QKDN control, management, and orchestration

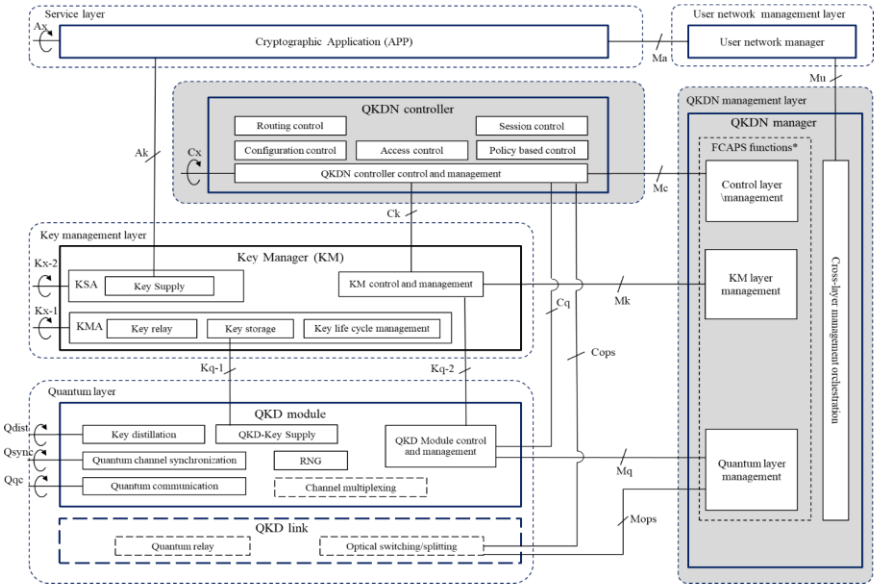


Figure 1. Functional components and reference points relevant to QKDN control and management

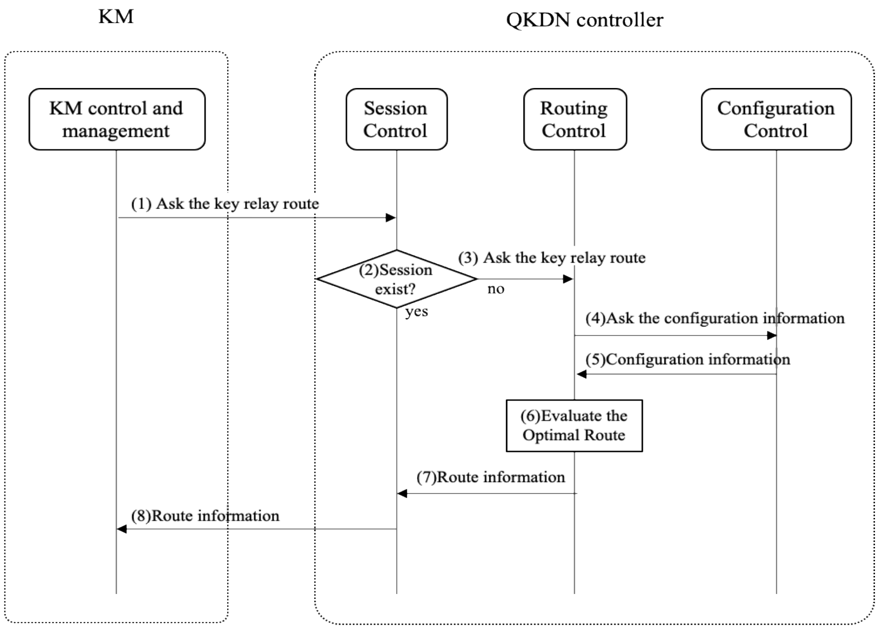

KM
QKDN controller
KM control and management
Session Control
Routing Control
Configuration Control
(1) Ask the key relay route
(2)Session exist?
(3) Ask the key relay route
no
yes
(4)Ask the configuration information
(5)Configuration information
(6)Evaluate the Optimal Route
(7)Route information
(8)Route information

Figure 15. Key relay procedure