TTC標準草案
(Draft TTC Standards)

Network Vision専門委員会

2021年3月4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.3802、Y.3803、Y.3804は、Y.3800が規定するQKDNの基本構成をベースとし、QKDNの機能アーキテクチャ、鍵管理、制御と管理の詳細仕様について規定する。 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～Y.3804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-3802	1	量子鍵配送ネットワーク- 機能アーキテクチャ
2	新規	JT-3803	1	量子鍵配送ネットワーク - 鍵管理
3	新規	JT-3804	1	量子鍵配送ネットワーク - 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: QKDネットワーク関連の勧告

- 2020年7月 SG13会合で基本勧告セットが完成。

基本編

Y.3800 Overview　QKDNの概要

Y.3801 Requirements　QKDNの要求条件

Y.3802 Architecture　QKDNのアーキテクチャ

Y.3803 Key manager

Y.3804 Control and managment

QKDN
各レイヤの仕様

Y.380a
Business model

Y.380b
SDNC

Y.380c
QoS

QKDN 個別仕様

Y.380d Y.QKDN_frint

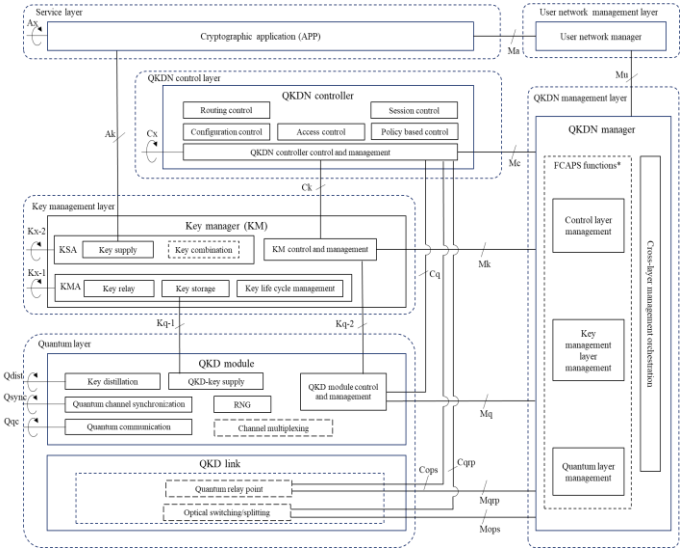
QKDN 実用化仕様

Y.3802:量子鍵配送ネットワーク – 機能アーキテクチャ

Quantum key distribution networks - Functional architecture

- 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、実装モデル(集中/分散/階層)、動作シーケンス例を規定。

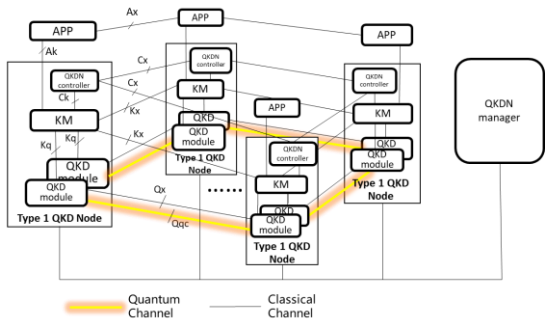
勧告の規定範囲 ・機能アーキテクチャモデル ・機能要素と参照点 ・アーキテクチャ構成 ・基本動作手順



QKDNの機能アーキテクチャ

QKDNのアーキテクチャ構成

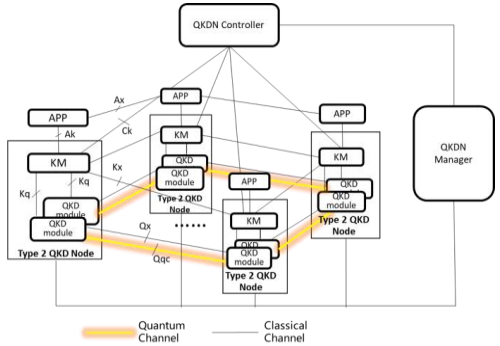
- 構成1:分散型QKDN
- 構成2:集中型QKDN
- 構成3:階層QKDノードを持つ集中型QKDN
- 構成4:集中型鍵リレーを行う集中型QKDN



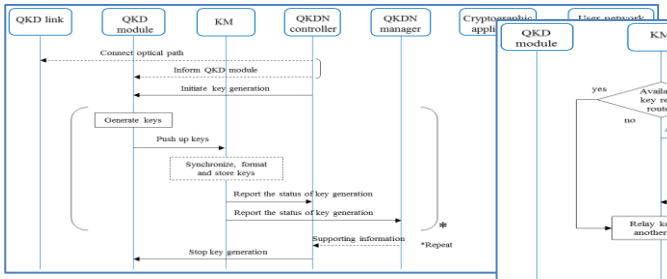
分散型QKDN

QKDN機能の基本動作手順

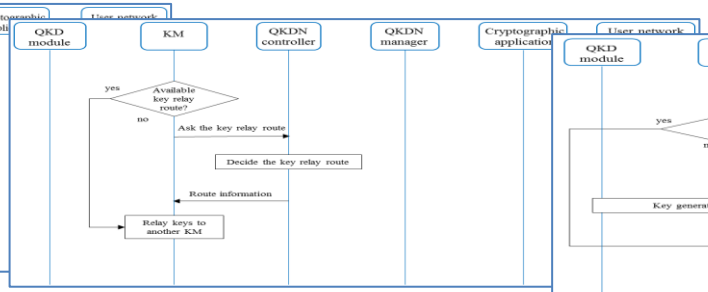
- サービスプロビジョニングとシステム初期化手順
- 鍵生成手順
- 鍵要求と供給手順
- 鍵リレー手順
- 鍵リレー再ルーティング制御手順



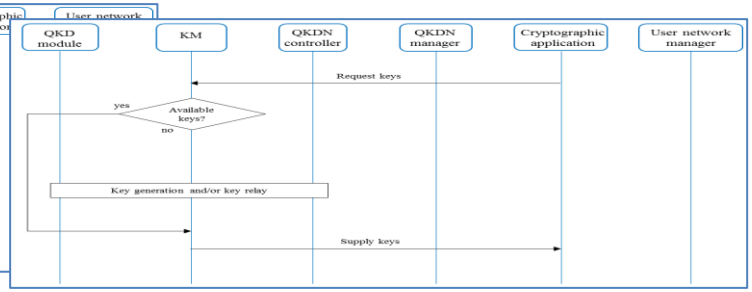
集中型QKDN



鍵生成手順



鍵リレー手順



鍵要求と供給手順

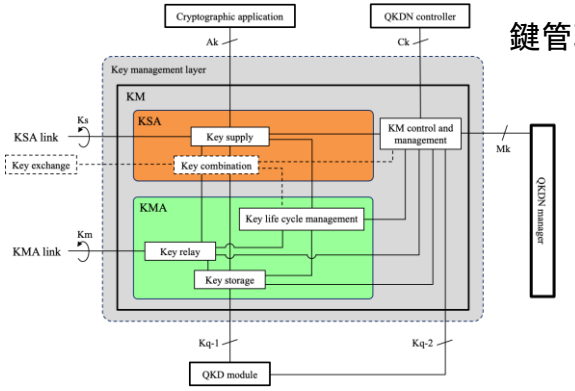
Y.3803:量子鍵配送ネットワーク - 鍵管理

Quantum key distribution networks - Key management

- 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。
- Tokyo QKD networkの実装をベースにしつつ、詳細なノウハウは隠蔽。

勧告の規定範囲

- QKDNの鍵管理の概要
- 鍵管理の機能要素
- 鍵管理の手順
- 鍵のフォーマット(鍵データとメタデータ)

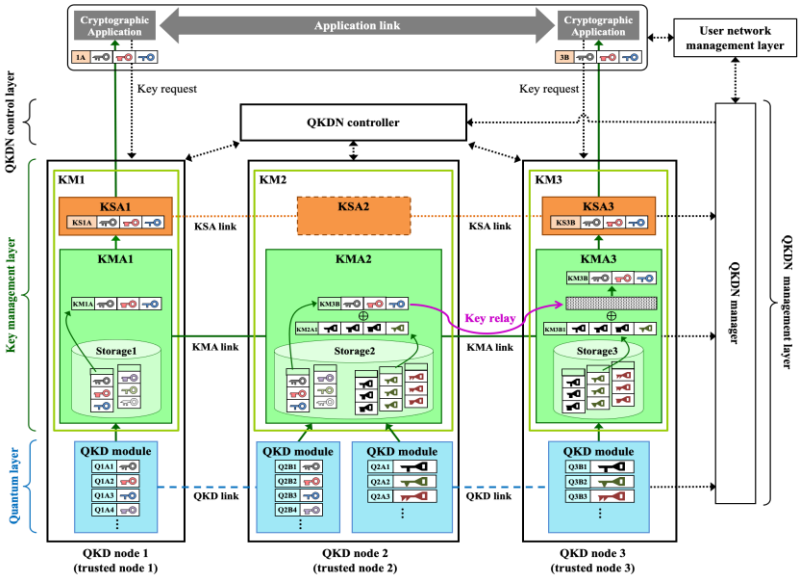


鍵管理レイヤの機能アーキテクチャ

- KM：鍵マネージャ鍵管理を実行する機能モジュール
- KMA：鍵生成、鍵リレー、鍵供給など一連の動作を管理する機能モジュール
- KSA：暗号アプリケーションに鍵を供給する機能モジュール

メタデータ情報(基本情報)

メタデータ	記述	M/O
(1) QKD-鍵		
QKD-鍵ID	QKD-鍵の識別子	M
鍵長	QKD-鍵の長さ	O
QKDモジュール ID	QKD-鍵を生成したQKD モジュール (AliceまたはBob) の識別子	O
組合せQKDモジュールID	AliceとBobの対を構成する組み合わされたQKDモジュールの識別子	O
生成タイムスタンプ	QKDモジュール対でQKD-鍵が生成された時刻のタイムスタンプ	O
ハッシュ値	QKD-鍵データのハッシュ値 (ハッシュ関数にはいくつかのオプションがあり、他の標準で検討される)	O
(2) KMA-鍵		
KMA-鍵 ID	KMA-鍵の識別子。AliceとBob向けの対となる鍵の識別子で、1つのQKDN内で一意である。QKDモジュールの対の名前から生成されたハッシュ値の一部が、しばしばこの識別子に使用される。	M
鍵長	KMA-鍵の長さ	O
鍵タイプ	暗号鍵か復号鍵かを指定する指標	O
KMA ID	KMA-鍵を格納するKMAの識別子	O
組合せKMA ID	組み合わされるKMAの識別子	M
生成タイムスタンプ	KMAでKMA-鍵が生成された時刻のタイムスタンプ	O
QKD モジュールID	KMA-鍵データに対応するQKD-鍵を生成したQKDモジュールの識別子	O
組合せQKD モジュール ID	AliceとBobの対を構成する組み合わされるQKDモジュールの識別子	O
ハッシュ値	KMA-鍵データのハッシュ値（ハッシュ関数にはいくつかのオプションがあり、他の標準で議論される）	O



鍵管理の機能要素と詳細手順

Y.3804:量子鍵配送ネットワーク - 制御と管理

Quantum Key Distribution Networks - Control and Management

• QKDNの制御と管理に関する機能を規定。韓国ETRIがエディターとして主導。

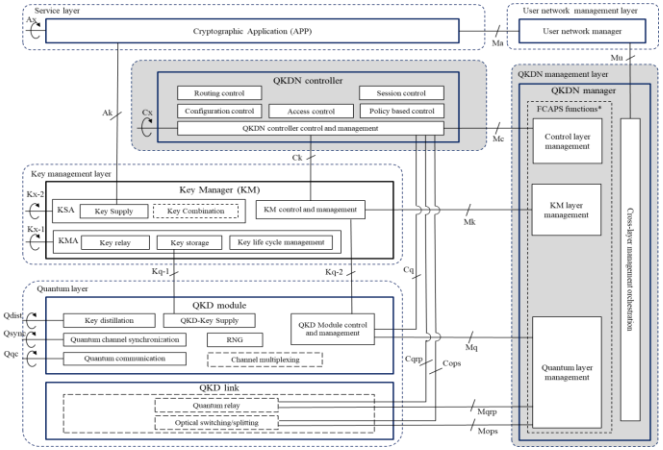
勧告の規定範囲　QKDNの制御、管理及びオーケストレーションの機能要素、機能、手順

QKDN制御レイヤの機能

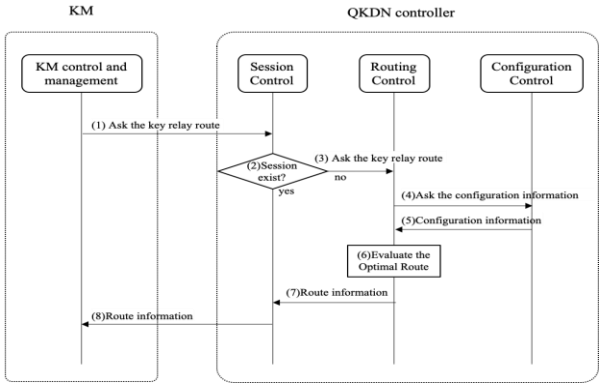
- ルーティング制御機能
- 構成制御機能
- ポリシーベース制御機能
- アクセス制御機能
- セッション制御機能

QKDN管理レイヤの機能

- レイヤ共通管理機能（FCAPS）
- 各レイヤ固有の管理機能
- クロスレイヤ管理機能



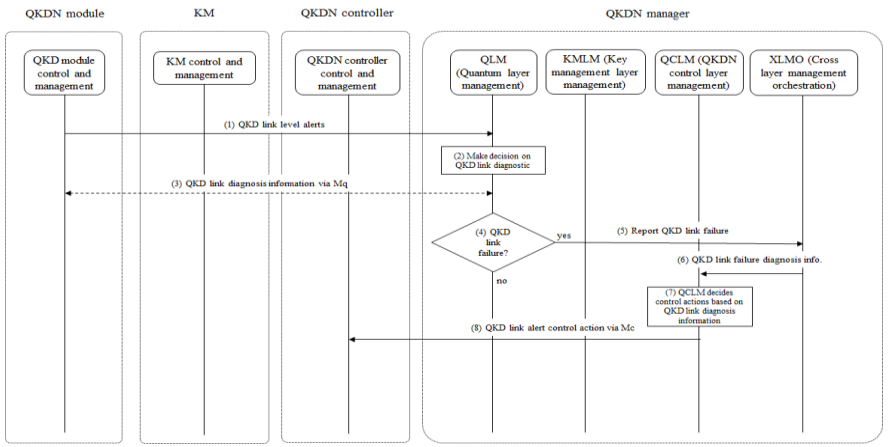
制御と管理に関連する機能要素



鍵リレー手順例

以下の手順を例として記載

- 障害管理手順(QKDリンク障害、KMの鍵リレー障害)
- 課金管理手順
- 構成管理手順
- パフォーマンス管理手順
- セキュリティ管理手順
- 鍵リレー手順
- 鍵リレー再ルーティング手順



QKDリンク障害手順例