TTC標準
Standard

JT-Y3801

量子鍵配送ネットワークの機能要求条件

Functional requirements for quantum key distribution networks

第 1.0 版

2020 年 11 月 12 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

＜参考＞

1. 国際勧告などとの関連

本標準は量子鍵配送ネットワークの機能要求条件について規定しており、2020 年 3 月に ITU-T SG13 において発行された ITU-T 勧告 Y.3801 に準拠している。

2. 上記勧告などに対する追加項目など

2.1 オプション選択項目

なし

2.2 ナショナルマター決定項目

なし

2.3 その他

なし

2.4 原勧告との章立て構成比較表

章立てに変更なし

3. 改版の履歴

版数	発行日	改版内容
第 1 版	2020 年 11 月 12 日	制定

4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

5. その他

(1) 参照している勧告、標準など

TTC 標準	JT-Y3800
ITU-T 勧告	X.800, Q.1743
ISO/IEC 標準	ISO/IEC 18033-3

6. 標準作成部門

ネットワークビジョン専門委員会

1. 規定範囲

本標準は、以下の量子鍵配送ネットワーク(QKDN)の機能要求条件を定める。

- 量子レイヤの機能要求条件
- 鍵管理レイヤの機能要求条件
- QKDN 制御レイヤの機能要求条件
- QKDN 管理レイヤの機能要求条件

2. 参考文献

以下に列挙するITU-T勧告およびその他の参考文献は、この本文中の参照を通して、本標準を構成する規定を含む。発行時点では、示された版は有効であった。すべての勧告及び他の参考文献は改訂の対象である。したがって、本標準の利用者は、以下に列挙する勧告及び他の参考文献の最新版を適用する可能性を調査することが推奨される。現在有効なITU-T勧告のリストは定期的に発行されている。本標準が文献を参照することは、その文献がそれ単体で勧告となる地位をその文献に与えるものではない。

[ITU-T Y.3800]　　ITU-T Y.3800(2019)、量子鍵配送ネットワークの概要

3. 定義

3.1. 本標準以外で定義されている用語

本標準は、本標準以外で定義された次の用語を使用する。

3.1.1. アクセス制御 [b-ITU-T X.800]: 無許可の方法でのリソースの使用の防止を含む、リソースの無許可の使用の防止。

3.1.2. 古典チャネル [ETSI GR QKD007]：破壊することなく読み取り可能で、完全に再生される形式で符号化されたデータを交換するために 2 つの通信当事者が使用する通信チャネル。

3.1.3. 情報理論的安全性 (IT セキュア) [ITU-T Y.3800]：無制限の計算資源による解読攻撃に対する安全性。

3.1.4. 鍵ライフサイクル[ITU-T Y.3800]：鍵マネージャ (KM) の鍵受信から、暗号アプリケーションでの鍵利用と鍵管理ポリシーによる削除または保存までの一連の処理。

3.1.5. 鍵管理[ITU-T Y.3800]：量子レイヤからの受信、格納、フォーマッティング、リレー、同期、認証、暗号アプリケーションへの供給、鍵管理ポリシーによる削除または保存まで、鍵ライフサイクルで実行されるすべての動作。

3.1.6. 鍵マネージャ (KM) [ITU-T Y.3800]：鍵管理レイヤ内で鍵管理を実行する機能モジュールで、QKD ノード内に配置される。

3.1.7. 鍵マネージャ(KM) リンク[ITU-T Y.3800]：鍵マネージャ(KM) を接続し、鍵管理を行う通信リンク。

3.1.8. 鍵リレー[ITU-T Y.3800]：中間 QKD ノードを経由し任意の QKD ノード間で鍵を共有する方法。

3.1.9. 鍵供給[ITU-T Y.3800]：鍵を暗号アプリケーションに提供する機能

3.1.10. 量子チャネル [ETSI GR QKD007]：量子信号を送信する通信チャネル。

3.1.11. 量子鍵配送 (QKD)[ETSI GR QKD007]：量子情報理論に基づく情報理論的セキュリティを用いて対称暗号鍵を生成および配送する手順または方法。

3.1.12. QKD リンク[ITU-T Y.3800]：QKD を動作させるための 2 つの QKD モジュール間の通信リンク。

注：QKD リンクは、量子信号を送受信する量子チャネルと、同期と鍵蒸留のために情報を交換する古典チャネルから構成される。

3.1.13. QKD モジュール[ITU-T Y.3800]：暗号機能と、QKD プロトコル、同期、鍵生成のための蒸留などの量子光プロセスを実装するハードウェアおよびソフトウェアコンポーネントのセット。定められた暗号境界内に含まれる。

注： QKD モジュールは、QKD リンクに接続され、鍵を生成するエンドポイントモジュールとして動作する。QKD モジュールには 2 つのタイプ、すなわち送信器 (QKD-Tx) および受信器 (QKD- Rx) がある。

3.1.14. QKD ネットワーク (QKDN) [ITU-T Y.3800]： QKD リンクを介して接続された 2 以上の QKD ノードから構成するネットワーク。

注： QKD ネットワーク (QKDN) では、QKD リンクで直接接続されていない QKD ノード間でも、鍵リレーによって鍵を共有できる。

3.1.15. QKDN コントローラ[ITU-T Y.3800]：QKDN を制御するために QKDN 制御レイヤに位置する機能モジュール。

3.1.16. QKDN マネージャ[ITU-T Y.3800]：QKDN を監視および管理するために QKDN 管理レイヤに位置する機能モジュール。

3.1.17. QKD ノード[ITU-T Y.3800]：許可されていない当事者による侵入および攻撃から保護されている 1 つ以上の QKD モジュールを含むノード。

注：QKD ノードは、鍵マネージャ(KM)を含むことができる。

3.1.18. Quality of Service(QoS)[b ITU T Q.1743]：サービスのユーザの満足度を決定するサービスパフォーマンスの総合的な効果。この機能は、次のようなすべてのサービスに適用されるパフォーマンス要素の組み合わせによって特徴付けられる。

- サービスの操作性パフォーマンス；
- サービスのアクセス性パフォーマンス；
- サービスの保持性パフォーマンス；
- サービスの完全性パフォーマンス；
- および各サービスに固有のその他の要因。

3.1.19. ユーザネットワーク[ITU-T Y.3800]： QKDN によって供給される鍵を暗号アプリケーションが利用するネットワーク。

3.2. 本標準で定義する用語

無し。

4. 略語及び頭字語

本標準では、次の略語及び頭字語を使用する。

AES	Advanced Encryption Standard
IT-secure	Information Theoretically secure
KM	Key Manager
OTP	One-Time Pad
QKD	Quantum Key Distribution
QKDN	QKD Network
QoS	Quality of Service

5. 表記法

本標準ではキーワード「が要求される」は、厳密に従わなければならず、この文書への適合性が主張される場合にはそこから逸脱することは許されない要求条件を示す。
キーワード「推奨される」は、推奨されるが絶対に必要ではない要求条件を示す。従って、この要求条件は、適合性を主張するために存在する必要はない。

本標準のいくつかの要求条件は、制御及び/又は管理目的のためにQKDN内の主体によって提供される情報(すなわち、鍵管理、状態、障害、性能、課金、構成、セキュリティ関連情報)を参照する。要求条件に基づいて提供される情報は、ユースケースおよび/または実装に依存する。標準に含まれる情報を特定する方法は、本標準の範囲外であり、実装においてなされる選択は、本標準への適合性の主張を妨げない。
本標準において、「鍵」は、QKDNによって生成された「対称ランダムビット列」を意味する。

6. はじめに

以下の章では、[ITU-T Y.3800]におけるQKDNのQKDN能力とレイヤ構造を満たすために、QKDNの機能要求条件を規定する。

本標準の範囲は、ネットワークの側面から機能要求条件を規定することであり、いくつかのセキュリティ要求条件は、それが鍵のセキュリティに直接関係する場合に言及されている。

QKDN全体の一般的なセキュリティ管理と、各レイヤとトラステッドノードにおける詳細なセキュリティ問題は、本標準の範囲外である。

7. 量子レイヤの機能要求条件

QKDNで鍵を生成するために、QKDプロトコルは次の要求条件を満たす。

Req_Q 1. QKD プロトコルは、安全性が証明可能であり、IT セキュアな鍵の確立を可能とすることが要求される。

QKDNで鍵を生成するには、QKDモジュールは次の要求条件を満たす。

Req_Q 2. QKD モジュールは、QKD リンクで接続された対応する QKD モジュールと、1 つ以上の QKD プロトコルを実行するために必要な機能を実装することが要求される。

注 1 - QKD モジュールの機能には、乱数生成、量子通信、鍵生成のための蒸留、および量子チャネル同期が含まれる。

注 2 - QKD モジュールは、鍵を生成するエンドポイントモジュールとして機能する。

注 3 - QKD リンクは、[ITU-T Y.3800]に記載されているように、QKD の距離を延長するために 1 つ以上の量子中継点を含むことができる。

Req_Q 3. QKD モジュールは、定義された暗号境界内に含まれていることが要求される。

Req_Q 4. QKD リンクによって接続された一対の QKD モジュールは、適切なインタフェースを経由して対応する KM に鍵を転送することが要求される。

Req_Q 5. QKD モジュールは、QKD モジュールのステータス情報およびオプションで QKD リンクのステータス情報を KM へ提供することが推奨される。

Req_Q 6. QKD モジュールは、QKD モジュールおよびオプションで QKD リンクのステータス情報を QKDN コントローラへ提供することが要求される。

Req_Q 7. QKD モジュールは、QKD モジュールの障害およびパフォーマンス情報を QKDN マネージャに提供することが要求される。

8. 鍵管理レイヤの機能要求条件

QKDN内の鍵を安全、確実かつ効率的に管理するために、KMは以下の要求条件を満たす。

Req_KM 1. KM は、異なるプロトコルを実装するさまざまな種類の QKD モジュールと互換性があることが推奨される。

Req_KM 2. KM は、適切なインタフェースを介して QKD モジュールから鍵を受信し、格納が必要な場合は安全に格納することが要求される。

Req_KM 3. KM は、内部目的または鍵供給または鍵リレーのために必要な場合、鍵をフォーマット(長さが適切でない場合の結合または分割を含む)することが推奨される。

Req_KM 4.　　KM は、量子レイヤの QKD モジュールから QKD モジュールおよび QKD リンクのステータス情報を受信することが推奨される。

注 1 - KM はステータス情報を QKDN コントローラに転送できる。

Req_KM 5.　　KM は以下を提供することが要求される。

- QKDN コントローラに対し、QKDN 制御機能のための鍵管理に関する情報。
- QKDN マネージャに対し、QKDN 管理機能のための鍵管理に関する情報。
- QKDN マネージャに対し、KM および KM リンクの障害およびパフォーマンス情報。

注 2 - 鍵管理に関する情報には、鍵がどの QKD モジュールから来たか、鍵がどのノードにリレーされたか、タイムスタンプ、鍵が供給された暗号アプリケーション、KM リンクの共有鍵量、鍵消費率、KM リンク状態、課金および障害発生時のアラームなどの情報を含めることができる。

Req_KM 6.　　KM は、3 以上のノードを持つ QKDN に接続された任意の 2 つのリモート KM 間で鍵を確立するために、トラステッドノードを介して高度に安全な暗号化(例:OTP[b- Shannon 1949])を使用する鍵リレーをサポートすることが推奨される。

Req_KM 7.　　KM は、鍵管理ポリシーに従って、鍵リレーのための別の適切な方法(例えば、AES[b-ISO/IEC18033 3]、[b-FIPS PUB197])をサポートすることが推奨される。

Req_KM 8.　　鍵リレーの信頼性と安全性を高めるために、KM および KM リンクは、鍵同期、エンティティ認証、およびメッセージ認証の能力を持つことが推奨される。

Req_KM 9.　　鍵リレーを効率的にするために、KM は QKDN コントローラの制御下で互いに協力することが推奨される。

Req_KM 10.　　QKD ノードが設計または構成によってユーザネットワークに鍵を提供する場合、次の要求条件が適用される。

- KM は、認可された暗号アプリケーションから鍵供給インタフェースを介して鍵要求を受信することが要求される。

注 3 – KM は、KM リンクを介して鍵要求を受信する場合がある。

- KM は、十分な鍵が利用可能である場合、鍵管理ポリシーに従うことを条件として、鍵供給インタフェースを介して、ユーザネットワークのサービスレイヤ内の暗号アプリケーションに、要求された量の鍵を供給することが要求される。
- KM は、セキュリティ能力を備えた鍵供給インタフェースを介して、ユーザネットワークのサービスレイヤにある暗号アプリケーションに、鍵を供給することが要求される。
- KM は、ユーザネットワークのサービスレイヤにおける様々な暗号アプリケーションが利用できる鍵供給インタフェースを提供することが推奨される。

注 4 - 暗号アプリケーションには様々な要求条件があり、様々な環境で動作する。鍵供給インタフェースの設計目標には、現在および将来のアプリケーションに対する幅広い操作性と柔軟な拡張性が含まれる。

- KM は、暗号アプリケーションのアクセス制御をサポートすることが推奨される。
- KM は、鍵管理ポリシーを適用することが要求される。

注 5 - 鍵管理ポリシーには、鍵の供給が実行された後に、鍵を削除すること、または鍵ストレージに鍵を保存することが含まれる。

Req_KM 11.　　KM は、鍵ライフサイクル管理の要素を提供することが要求される。

9.　QKDN 制御レイヤの機能要求条件

QKDNを制御し、安全で、安定し、効率的で、堅牢な動作およびサービスを提供するために、QKDNコントローラは、以下の要求条件を満たす。

Req_C 1.　　鍵リレー機能が QKDN によってサポートされている場合、QKDN コントローラは鍵リレーのルーティング制御を提供することが要求される。

Req_C 2.　　QKDN コントローラは、QKD モジュール、QKD リンク、KM、および KM リンクの構成を制御することが推奨される。

Req_C 3.　　QKDN コントローラは、課金ポリシー制御を提供することが推奨される。

Req_C 4.　　QKDN コントローラは、Quality of Service(QoS)ポリシー制御を提供することが推奨される。

Req_C 5.　　QKDN コントローラは、量子レイヤおよび鍵管理レイヤの機能要素のアクセス制御をサポートし保証することが推奨される。

Req_C 6.　　QKDN コントローラは、セッション制御を提供することが推奨される。

注 - セッションとは、エンドツーエンドで鍵を確立したり、ユーザネットワークのサービスレイヤにある暗号アプリケーションに鍵を提供したりするための KM 間の通信である。セッション制御は、セッションを開始、維持、および終了する。

Req_C 7.　　QKDN コントローラは、障害、パフォーマンス、課金、および構成情報を QKDN マネージャに提供することが推奨される。

10.　QKDN 管理レイヤの機能要求条件

QKDN全体の監視と管理をサポートし、ユーザネットワークの管理をサポートするには、QKDマネージャは次の要求条件を満たす。

Req_M 1.　　QKDN マネージャは、以下をサポートするために障害管理を提供することが要求される。

- 量子レイヤ、鍵管理レイヤ、および QKDN 制御レイヤによって提供されるステータス情報を収集/受信する。
- 障害表示のために、収集/受信したステータス情報を分析する。

Req_M 2.　　QKDN マネージャは、以下をサポートするために障害管理を提供することが推奨される。

- 根本原因分析能力。
- 診断能力。
- 障害解決ポリシーの管理、および修復アクションに関連する機能コンポーネントとの連携。

Req_M 3.　　QKDN マネージャは、次の項目をサポートするために構成管理を提供することが要求される。

- リソースプロビジョニングの管理。

Req_M 4.　　QKDN マネージャは、以下をサポートするために構成管理を提供することが推奨される。

- QKDN が鍵リレーをサポートする場合、鍵リレーのルーティングおよび再ルーティング。
- ネットワークトポロジの収集と管理。
- インベントリ管理のためのリソース構成。
- 需要と可用性に基づく管理対象リソースの変更。
- 管理された QKDN での QKD 管理対象リソースのディスカバリー。

Req_M 5. QKDN マネージャは、次の項目をサポートするために課金管理を提供することが推奨される。

- 鍵供給サービスとそのポリシー。

Req_M 6. QKDN マネージャは、次の項目をサポートするためにパフォーマンス管理を提供することが要求される。

- 量子レイヤ、鍵管理レイヤおよび QKDN 制御レイヤから性能情報を収集/受信する。
- 収集/受信した QKDN 性能情報の分析。

Req_M 7. QKDN マネージャは、以下をサポートするためにパフォーマンス管理を提供することが推奨される。

- 鍵供給の QoS。
- 鍵供給サービスポリシーの管理。

Req_M 8. QKDN マネージャは、以下をサポートするためにセキュリティ管理を提供することが要求される。

- QKDN からのセキュリティに関する管理情報の収集/受信。

Req_M 9. QKDN マネージャは、KM の鍵ライフサイクル管理をサポートすることが要求される。

Req_M 10. QKDN マネージャは、以下をサポートするためにセキュリティ管理を提供することが推奨される。

- 認証と認可の管理。

Req_M 11. QKDN マネージャは、クロスレイヤ管理オーケストレーションを実行し、ユーザネットワーク管理からの管理要求をサポートすることが推奨される。

11. セキュリティに関する考慮事項

セキュリティ上の脅威及び潜在的な攻撃を軽減するために、機密性、完全性、真正性、否認防止、可用性及びトレーサビリティの問題に対処する必要があり、QKDN、ユーザネットワーク及び2つのネットワーク間のインタフェースにおいて、適切なセキュリティ及びプライバシー保護スキームを考慮すべきである。
詳細は本標準の範囲外である。

参考文献

[b-ITU-T X.800] Security architecture for Open Systems Interconnection for CCITT applications

[b-ETSI GR QKD 007] Group Specification ETSI GS QKD 007 (2018), Quantum Key Distribution (QKD); Vocabulary.

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-Shannon 1949] Claude Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28, pp. 666–682, 1949.

[b-ISO/IEC 18033-3] ISO/IEC 10833-3:2010 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), Announcing the ADVANCED ENCRYPTION STANDARD (AES)