TTC標準
Standard

JT-Q4162

量子鍵配送ネットワークの Kq-1 インタフェースのプロトコル

Protocols for Kq-1 interfaces for quantum key distribution networks

第 1 版

2025 年 11 月 6 日制定

一般社団法人
情報通信技術委員会

THE 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概要について規定しており、2023年12月にITU-T SG11において発行されたITU-T勧告Q.4162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	2025年11月6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

JT標準　　JT-Q4160, JT-X1712

6. 標準作成部門

信号制御専門委員会

1. 規定範囲

本標準は、特に次の領域における量子鍵配送ネットワーク(QKDN)の Kq-1 インターフェースのプロトコルを規定する。

- 信号手順
- 信号メッセージおよびパラメータ
- セキュリティに関する考慮事項

2. 参照文献

以下に列挙する ITU-T 勧告およびその他の参照文献は、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照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照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 Q.4160]	ITU-T Q.4160 (2023) 、量子鍵配送ネットワーク - プロトコルフレームワーク
[ITU-T X.1712]	ITU-T X.1712 (2021) 、量子鍵配送ネットワークのセキュリティ要求条件と対策 - 鍵管理

3. 用語定義

3.1. 本標準以外で定義された用語

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. 鍵管理[b-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。

3.1.2. 鍵マネージャ (KM) [b-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。

3.1.3. 鍵リレー[b-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。

3.1.4. 量子鍵配送[b-ETSI GR QKD 007]：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。

3.1.5. QKD-鍵[b-ITU-T Y.3802]：一対のQKDモジュールによって生成される一対の対称ランダムビット列。特に、鍵マネージャでサイズ変更およびフォーマットされる前のランダムビット列を指す。

3.1.6. QKDリンク[b-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。

3.1.7. QKDモジュール[b-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。

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

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。

3.1.9. QKDNコントローラ[b-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。

3.1.10. QKDノード[b-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。

3.2. 本標準で定義された用語定義

無し。

4. 略語

本標準は、以下の略語を使用する。

HTTPS	安全なハイパーテキスト転送プロトコル (Hypertext Transfer Protocol Secure)
ID	識別子（Identifier
KM	鍵マネージャ（Key Manager）
QKD	量子鍵配送（Quantum Key Distribution）
QKDN	量子鍵配送ネットワーク（QKD Network）
Rx	受信器 (Receiver)
TCP	伝送制御プロトコル (Transmission Control Protocol)

TLS　　トランスポートレイヤセキュリティ (Transport Layer Security)

Tx　　送信器 (Transmitter)

5. 表記法

無し。

6. Kq-1インターフェース

参照点 Kq-1 は、KM と QKD モジュールとの間に確立される。Kq-1 インターフェースは、KM 内の鍵保存機能と QKD モジュール内の QKD-鍵供給機能との間の鍵取得に使用される。

7. 信号手順

Kq-1 インターフェースでの鍵要求と鍵供給には、次の 2 つのモードが規定されている。

1) プロアクティブ鍵供給モード：QKDモジュールが、KMへのQKD鍵の供給を開始する。

2) 要求時鍵供給モード：KMが、QKDモジュールにQKD-鍵の供給を要求することによって手順を開始し、QKDモジュールは、要求に応じてKMにQKD-鍵を供給する。

信号に適用されるプロトコルスイートは、[ITU-T Q.4160]の第 7 章に規定されている。

7.1. プロアクティブ鍵供給モード信号手順

この手順は、QKD モジュールで QKD-鍵が生成されたときに開始される。提供される QKD-鍵の数は、主に QKD コントローラからの鍵生成要求に依存する。

図 1 は、送信先の Kq-1 インターフェースでのプロアクティブな鍵供給の信号手順を示す。

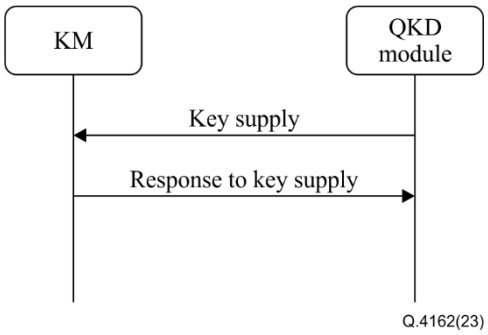


図1　Kq-1インターフェースでのプロアクティブ鍵供給モードの信号手順

7.2. 要求時鍵供給モード信号手順

この手順では、KM が QKD 鍵を必要とするとき、KM が QKD モジュールに鍵要求を送信する。QKD モジュールは、要求に応答して KM に QKD 鍵を供給する。

図 2 は、Kq-1 インターフェースにおける要求時鍵供給モードの鍵供給のための信号手順を示す。

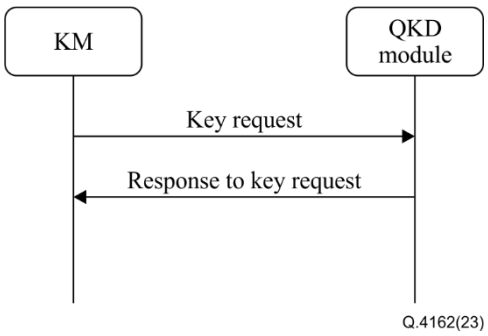


図2　Kq-1インターフェースにおける要求時鍵供給モードの鍵供給のための信号手順

8.　信号メッセージおよびパラメータ

この章は、Kq-1 インターフェースのメッセージとそのパラメータを規定する。

表 1 から表 4 の M/O 欄は、欄 1 のパラメータの信号に関するものであり、M は必須を示し、O は任意を示す。

この章で指定されたメッセージとパラメータは、特定のプロトコルから独立であり、異なる実装を持つことができる。推奨されるプロトコルの実装は、付属資料 I と II で記述されている。

注：表 1 から表 4 に記述されたメッセージパラメータは、必ずしもメッセージペイロードのフィールドにマップされず、特定のプロトコルの制御パラメータの一部である可能性がある。表 1 から表 4 の列 3 に列挙されたデータ型は、特定のプロトコルによって異なる可能性がある。

8.1.　プロアクティブ鍵供給モードのメッセージとパラメータ

8.1.1.　鍵供給メッセージ (Key supply message)

鍵供給メッセージ (Key supply message)は、QKD モジュールから同じ QKD ノード内の KM に送信される。QKD モジュールは、一意の QKD-鍵識別子(ID)を持つ QKD-鍵を KM に供給する。

表 1 に、鍵要求メッセージ (Key supply message)のパラメータを示す。

表 1　鍵供給メッセージ (Key supply message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Key	提供されたQKD-鍵データ	String	M	
Key ID	提供されたQKD-鍵データのID	String	M	
QKD module ID	QKD-鍵を供給したQKDモジュール(AliceまたはBob)のID	String	O	
Matching QKD module ID	AliceとBobのペアを構成する、一致するQKDモジュールを識別するためのID	String	O	
Key length	供給された各QKD-鍵の長さ	Integer	O	省略した場合は、デフォルト値が適用される。
Generation time stamp	QKDモジュールのペアにおけるQKD-鍵生成のタイムスタンプ	String	O	
Hash value	QKD-鍵データのハッシュ値。	String	O	
Extension	拡張パラメータの配列	Array of objects	O	将来の使用のため

8.1.2. 鍵供給メッセージに対する応答 (Response to key supply message)

鍵供給メッセージに対する応答 (Response to key supply message は、鍵供給に応答して KM から QKD モジュールに送信され、KM は QKD 鍵の受信結果を QKD モジュールに通知する。

表 2 に、鍵供給メッセージに対する応答 (Response to key supply message)のパラメータを示す。

表2　鍵供給メッセージに対する応答(Response to key supply message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Key ID	受信したQKD-鍵のID	String	M	
QKD module ID	QKD-鍵を供給したQKDモジュール(AliceまたはBob)のID	String	O	
Matching QKD module ID	AliceとBobのペアを構成する、matching QKDモジュールを識別するためのID	String	O	
Response	QKD-鍵の受信の結果	String	M	成功または失敗の理由
Extension	拡張パラメータの配列	Array of objects	O	将来の使用のため

8.2. 要求時鍵供給モードの鍵供給メッセージとパラメータ

8.2.1. 鍵要求メッセージ (Key request message)

鍵要求メッセージ (Key request message)は、KM から QKD モジュールに送信され、QKD-鍵を要求する。

表 3 に、鍵要求メッセージ (Key request message)のパラメータを示す。

表3　鍵要求メッセージ (Key request message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Number of keys	要求されたQKD-鍵の数	Integer	O	省略した場合は、デフォルト値が適用される。
Size of key	要求された各QKD-鍵の長さ	Integer	O	省略した場合は、デフォルト値が適用される。
Extension	拡張パラメータの配列	Array of objects	O	

8.2.2. 鍵要求メッセージに対する応答 (Response to key request message)

鍵要求メッセージに対する応答 (Response to key request message)は、暗号アプリケーションからの鍵要求に応答して、QKD モジュールから KM に送信される。QKD モジュールは、要求された QKD 鍵を暗号アプリケーションに供給する。

表 4 に、鍵要求メッセージに対する応答 (Response to key request message)のパラメータを示す。

表4　鍵要求メッセージに対する応答(Response to key request message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Keys	鍵ファイルは、鍵データとメタデータで構成される	Array of objects	M	
Key	要求に対して提供されたQKD鍵データ	String	M	
Key ID	提供されたQKD鍵のID	String	M	

Key extension	Key ID拡張子	Object	O	
Response	鍵供給の結果	String	M	
Extension	拡張パラメータの配列	Array of objects	O	

9. セキュリティに関する考慮事項

鍵データおよび関連するメタデータは、Kq-1 参照点を介して転送される。セキュリティ要件およびそれらを保護するための措置は、[ITU-T X.1712]で規定されている。

付属資料I

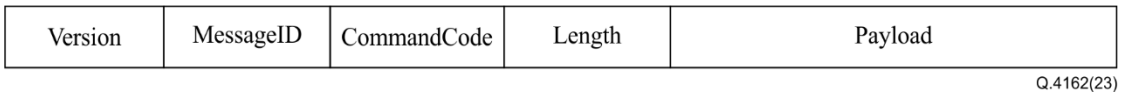
伝送制御プロトコルを使用するプロトコル実装

(この付属資料は、この勧告の不可欠な部分を構成するものではない。)

この付属資料では、8 章に記述されているメッセージとパラメータに対して、伝送制御プロトコル(TCP)を使用する実装について説明する。

注 1：一部のパラメータは、データペイロード内のフィールドにマッピングされるのではなく、プロトコルの制御情報の一部にマッピングされる。

QKD モジュールは、TCP プロトコル[b-IETF RFC 9293]を使用して KM に接続することができる。TCP 上の対応するメッセージフォーマットは、図 I.1 に示されている。



図I. 1　伝送制御プロトコル上のメッセージフォーマット

図I.1において:

Version : 採用されているメッセージフォーマットの現在のバージョン(2バイト)。

MessageID : 各メッセージの固有ID(4バイト)。

CommandCode：Kq-1インターフェースで転送される異なるコマンド/応答メッセージを示す固有のコード(2バイト)。

Lengh：メッセージペイロードの長さ(2バイト)。

Payload：特定のコマンド/応答メッセージのメッセージパラメータ、JavaScriptオブジェクト表記データフォーマット[b-IETF RFC 8259]。

注 2：トランスポートレイヤセキュリティ(TLS)プロトコル[b-IETF RFC 5246]は、セキュリティを強化するために TCP とともに実装することができる。

接続が確立されると、QKD モジュールと KM との間で相互認証が実行される。相互認証の後、Kq-1 インターフェースを介して QKD モジュールから KM に鍵供給のためのコマンド/応答メッセージが転送される。

注 3：TLS プロトコルを適用する場合、QKD モジュールは、KM が所有する証明書の有効性を検証し、それに基づいて接続先の KM の ID を確認できる。同様に、KM は、QKD モジュールが所有する証明書の有効性を検証し、それに基づいて接続先の QKD モジュールの ID を確認できる。

表 I.1 は、CommandCode 対コマンド/応答メッセージ名を示す。

表I.1　コマンドコード対コマンド/応答メッセージ名

コマンドコード	コマンド/応答メッセージ名
0x3101	鍵供給
0x1302	鍵供給に対する応答
0x1303	鍵要求
0x3104	鍵要求に対する応答

CommandCode の最初の 2 桁の「13」は、対応するメッセージが KM から QKD モジュールに送信されることを示し、「31」は、対応するメッセージが QKD モジュールから KM に送信されることを示す。

付属資料II

安全なハイパーテキスト転送プロトコルを使用する要求時鍵供給モードのためのプロトコル実装

(この付属資料は、この勧告の不可欠な部分を構成するものではない。)

8.2 章で規定された要求時鍵供給モードでの鍵供給のための信号メッセージとパラメータは、[b-ETSI GS QKD 014]で規定された代表状態転送ベースの鍵配送アプリケーションプログラミングインタフェースのプロトコルとデータフォーマットに従って、安全なハイパーテキスト転送プロトコル(HTTPS)を使用して実装することができる。この付属資料では、8.2 章で指定されたメッセージとパラメータの、[b-ETSI GS QKD 014]で指定された対応するデータフォーマットへのマッピングについて説明する。

注：この実装では、KM と QKD モジュールは、それぞれ[b-ETSI GS QKD 014]で定義されているセキュアアプリケーションエンティティと鍵管理エンティティに対応する。

II.1 **鍵要求メッセージ** (Key request message)

この実装では、8.2.1 章で規定されている鍵要求メッセージ(Key request message)は、[b-ETSI GS QKD 014]で規定されている Get Key メソッドとして実行される HTTPS トランザクションの HTTPS リクエストに対応する。表 II.1 は、鍵要求メッセージ(Key request message)と Get Key メソッドのマッピングを示す。

表II.1　Get Keyメソッドへの鍵要求メッセージ(Key request message)のマッピング

パラメータ	M/O	データタイプ	Get Keyメソッドでの実装
Number of keys	O	Integer	鍵要求データ形式の「number」の項目
Size of key	O	Integer	鍵要求データ形式の「size」の項目
Extension	O	Array of objects	鍵要求データフォーマットの"extension_mandatory"または"extension_optional"項目

II.2 **鍵要求メッセージに対する応答** (Response to key request message)

この実装では、8.2.2 章で規定される鍵要求メッセージへの応答(Response to key request message)は、[b-ETSI GS QKD 014]で規定される Get Key メソッドとして実行される HTTPS トランザクションの HTTPS 応答に対応する。表 II.2 は、鍵要求メッセージへの応答と Get Key メソッドのマッピングを示す。

表II.2　Get Keyメソッドへの鍵要求への応答メッセージ(Response to key request message)のマッピング

パラメータ	M/O	データタイプ	Get Keyメソッドでの実装
Keys	M	Array of objects	鍵コンテナデータフォーマットの「keys」項目
Key	M	String	鍵コンテナデータフォーマットの「keys」項目
Key ID	M	String	鍵コンテナデータフォーマットの「key_ID」項目
Key extension	O	Object	鍵コンテナデータフォーマットの「key_ID_extension」項目
Response	M	String	Get KeyメソッドとしてHTTPSトランザクションのステータスコード
Extension	O	Array of objects	鍵コンテナデータフォーマットの「key_container_extension」項目

参考文献

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Cor.1 (04/2020), Overview on networks supporting quantum key distribution.

[b-ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020)/Cor.1 (04/2021), Quantum key distribution networks – Functional architecture.

[b-ETSI GR QKD 007] ETSI GR QKD 007 V1.1.1 (2018), Quantum key distribution (QKD); Vocabulary.

[b-ETSI GS QKD 014] ETSI GS QKD 014 V1.1.1 (2019), Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API.

[b-IETF RFC 5246] IETF RFC 5246 (2008), The transport layer security (TLS) protocol – Version 1.2.

[b-IETF RFC 8259] IETF RFC 8259 (2017), The JavaScript object notation (JSON) data interchange format.

[b-IETF RFC 9293] IETF RFC 9293 (2022), Transmission control protocol (TCP)