TTC標準
Standard

JT-Q4163

量子鍵配送ネットワークのKxインタフェースのプロトコル

Protocols for Kx 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

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.4163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 Kx 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. 鍵管理エージェント(KMA)[b-ITU-T Y.3802]：QKDノード（トラステッドノード）内の１つまたは複数のQKDモジュールによって生成された鍵を管理するための機能要素。

注 - KMAは、1つまたは複数のQKDモジュールから鍵を取得し、同期、サイズ変更、フォーマット、および格納を行う。また、鍵管理エージェント(KMA)リンクを介して鍵のリレーを行う。

3.1.3. 鍵管理エージェント鍵(KMA-鍵)[b-ITU-T Y.3803]：鍵管理エージェント(KMA)で格納され処理される鍵データ。任意のKMAと組みとなるKMAの間で安全に共有される。

3.1.4. 鍵管理エージェント(KMA)リンク[b-ITU-T Y.3802]：鍵管理エージェント(KMA)を接続して鍵リレーと鍵管理のための通信の実行する通信リンク。

3.1.5. 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。

3.1.6. 鍵マネージャ(KM)リンク[b-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。

3.1.7. 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。

3.1.8. 鍵供給エージェント(KSA)[b-ITU-T Y.3802]：鍵管理エージェント(KMA)と暗号アプリケーションの中間に位置し、暗号アプリケーションに鍵を供給する機能要素。

注 - 暗号アプリケーション用のアプリケーションインターフェースは、KSAに実装される。KSAは鍵を同期し、暗号アプリケーションに鍵を供給する前にKSAリンクを介してその完全性を検証する。

3.1.9. 鍵供給エージェント鍵(KSA-鍵)[b-ITU-T Y.3803]：鍵供給エージェント(KSA)で格納され処理される鍵データ。任意のKSAと組みとなるKSAの間で安全に共有される。

3.1.10. 量子鍵配送(QKD)[b-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。

3.1.11. 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。

3.1.12. 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。

3.1.13. 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。

3.1.14. 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。

3.1.15. 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。

ID	識別子（Identifier）
KM	鍵マネージャ（Key Manager）
KMA	鍵管理エージェント(Key Management Agent)
KSA	鍵供給エージェント(Key Supply Agent)
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. Kxインターフェース

Kx インターフェースは、KM リンクを介して各 QKD ノード内の 2 つの KM を接続する参照点である。Kx インターフェースは、KM 間の鍵リレー、鍵同期、および認証に必要な情報と操作を交換する手段を提供する。

7. 信号手順

[ITU-T Q.4160]の付属資料 I では、QKD における鍵要求、鍵リレー、鍵供給の信号手順の例が記述されている。信号に適用されるプロトコルスイートは、[ITU-T Q.4160]の 7 章で規定されている。

7.1. 鍵リレーの信号手順

鍵は、Kx インターフェースを介して送信元から送信先にリレーされる。KM は、QKD コントローラからのメッセージで指定された KM に鍵を送信する。

図 1 は、Kx インターフェースでの鍵リレーの信号手順を示している。

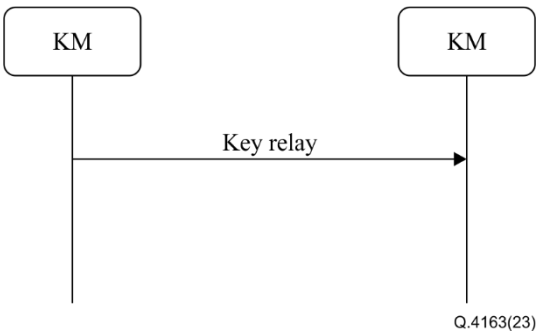


図1　Kxインターフェースでの鍵リレーの信号手順

鍵を受信すると、送信先 KM は、鍵リレーの完了を送信元 KM に通知する。この通知は、完了した鍵リレーにリンクされているトランザクションを指定する情報とともに送信する。

図 2 は、Kx インターフェースでの鍵リレー完了通知の信号手順を示している。

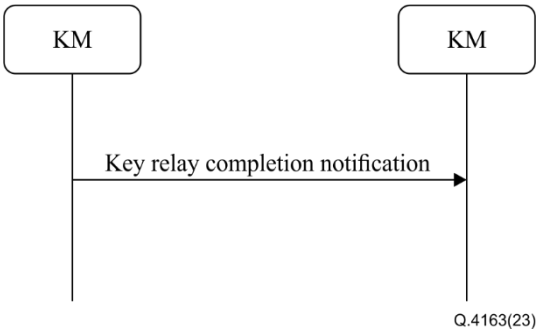


図2　Kxインターフェースでの鍵リレー完了通知の信号手順

7.2.　鍵供給通知のための信号手順

送信元 KM は、送信元の暗号アプリケーションからの鍵要求を受信すると、送信先 KM に鍵をプロアクティブに提供するよう通知することができる。送信先 KM は、プロアクティブに KSA-鍵を送信先の暗号アプリケーションに提供し、提供された KSA-鍵の鍵 ID を送信元 KM に応答する。

図 3 は、Kx インターフェースでの鍵供給通知の信号手順を示している。

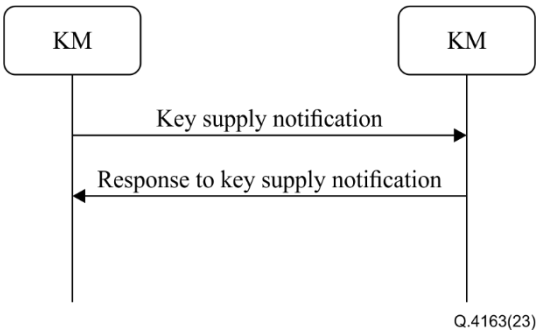


図3　Kxインターフェースにおける鍵供給通知のための信号手順

8.　信号メッセージおよびパラメータ

この章は、Kx 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しており、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タイプは、プロトコルによって異なる可能性がある。

8.1. 鍵リレーメッセージ (Key relay message)

鍵リレーメッセージ (Key relay message)は、送信元 KM から送信先 KM に鍵を伝達する。

表 1 に、鍵リレーメッセージ (Key relay message)のパラメータを示す。

表1　鍵リレーメッセージ (Key relay message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Source KMA ID	鍵リレールート全体の送信元KMAのID	String	M	
Destination KMA ID	鍵リレールート全体の送信先KMAのID	String	M	
Transit KMA IDs	鍵リレールートの中継ノードのKMAのIDのリスト	String	O	
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 ID	リレーされたKMA鍵のID	String	M	
Key	リレーされたKMA鍵データ	String	M	
Key extension	鍵 ファイルの拡張子	Object	O	ハッシュ値など
Key relay request ID	鍵リレー要求のID	String	O	
Extension	拡張パラメータの配列	Array of objects	O	

8.2. 鍵リレー完了通知メッセージ (Key relay completion notification message)

鍵が送信先 KM に到達すると、KM は送信元 KM に鍵リレーの完了を通知する。この通知は、完了した鍵リレーにリンクされているトランザクションを指定する情報とともに送信される。

表 2 は、鍵リレー完了通知メッセージ (Key relay completion notification message)のパラメータを示す。

表2　鍵リレー完了通知メッセージ (Key relay completion notification message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Response	鍵リレーの結果	String	M	成功または失敗の理由
Key relay request ID	鍵リレー要求のID	String	O	
Extension	拡張パラメータの配列	Array of objects	O	

8.3. 鍵供給通知メッセージ (Key supply notification message)

送信元の暗号アプリケーションから鍵要求を受信すると、送信元 KM は送信先 KM に鍵を事前に提供するように通知できる。この通知は、鍵提供のために生成されたセッションと、提供される KSA 鍵の数を指定する情報とともに送信される。

表 3 に、鍵供給通知メッセージ (Key supply notification message)のパラメータを示す。

表3　鍵供給通知メッセージ (Key supply notification message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Session ID	鍵供給のために生成されたセッションID	String	M	
Number of keys	提供されるKSA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	供給される各KSA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	

8.4.　鍵供給通知メッセージに対する応答 (Response to key supply notification message)

送信先 KM は、生成されたセッション中に送信先の暗号アプリケーションによって受信された KSA 鍵の鍵 ID を以て、送信元 KM に応答する。

表 4 に、鍵供給通知メッセージに対する応答 (Response to key supply notification message)のパラメータを示す。

表4　鍵供給通知メッセージに対する応答 (Response to key supply notification message)のパラメータ

パラメータ	概要	データタイプ	M/O	備考
Session ID	鍵供給のために生成されたセッションID	String	M	
Key ID	送信先暗号化アプリケーションから受信されたKSA鍵のID	String	M	
Response	鍵供給の結果	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	

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　および管理データは、Kx 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

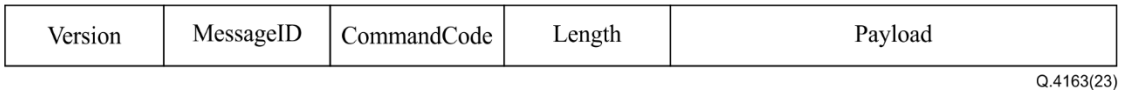
伝送制御プロトコルを使用するプロトコル実装

（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。

KM 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：Kx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)。

Length：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、KM 間で相互認証が実行される。相互認証の後、Kx インターフェースを介してコマンド/応答メッセージを転送し、鍵リレーを行うことができる。

注 3：TLS プロトコルを適用する場合、送信元 KM は、送信先 KM が所有する証明書の有効性を検証し、それに基づいて送信先 KM の ID を確認できる。同様に、送信先 KM は、送信元 KM が所有する証明書の有効性を検証し、それに基づいて送信先の KM 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
0x1101	鍵リレー
0x1102	鍵リレー完了通知
0x1103	鍵供給通知
0x1104	鍵供給通知に対する応答

CommandCode の最初の 2 桁「11」は、対応するメッセージが 1 つの KM から別の KM に送信されることを示す。

参考文献

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

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

[b-ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), Quantum key distribution networks – Key management.

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

[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).