TTC標準
Standard

JT-Q4160

量子鍵配送ネットワーク - プロトコルフレームワーク

Quantum key distribution networks – Protocol framework

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.4160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-X1710, JT-X1712, JT-Y3800, JT-Y3801, JT-Y3802, JT-Y3803, JT-Y.3804

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)の信号フレームワークを規定する。

- QKDN の信号とプロトコルの概要
- QKDN のプロトコルスイートおよびスタック

注-QKD リンクを介して一対の QKD モジュール間で実行される QKD プロトコルは、本標準の範囲外である。

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 X.1710] ITU-T X.1710(2020)、量子鍵配送ネットワークのセキュリティフレームワーク

[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

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

[ITU-T Y.3801] ITU-T Y.3801 (2020)、量子鍵配送ネットワークの機能要求条件

[ITU-T Y.3802] ITU-T Y.3802 (2020)、量子鍵配送ネットワーク - 機能アーキテクチャ

[ITU-T Y.3803] ITU-T Y.3803 (2020)、量子鍵配送ネットワーク - 鍵管理

[ITU-T Y.3804] ITU-T Y.3804 (2020)、量子鍵配送ネットワーク - 制御と管理

3. 用語定義

3.1. 他の標準等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. 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。

3.1.2. 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。

3.1.3. 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。

3.1.4. 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。

3.1.5. 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。

3.1.6. 鍵供給エージェント(KSA)[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。

3.1.7. 鍵供給エージェント鍵(KSA-鍵)[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。

3.1.8. 鍵管理エージェント(KMA)[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。

3.1.9. 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。

3.1.10. 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。

3.1.11. 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。

3.1.12. 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。

3.1.13. 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。

3.1.14. 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。

3.1.15. 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。

3.2. 本標準で定義する用語

無し。

4. 略語

本標準は、以下の略語を使用する。

CNCF	クラウドネイティブコンピューティングファウンデーション (Cloud Native Computing Foundation)
IT-secure	情報理論的安全性 (Information Theoretically-secure)
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）
RPC	リモートプロシージャコール (Remote Procedure Call)

5. 表記法

無し。

6. 概要

QKDN の基本機能とレイヤ構造は[ITU-T Y.3800]で定義されている。機能要件とアーキテクチャはそれぞれ[ITU-T Y.3801]と[ITU-T Y.3802]で規定されている。QKDN のセキュリティフレームワークは[ITU-T X.1710]で規定されており、QKDN に対するセキュリティ脅威に対処し、QKDN の一般的なセキュリティ要求条件とセキュリティ対策を導出している。代表的な信号手順と対応するメッセージパラメータは、[b-ITU-T FG-QIT4N D2.3-Part2]でいくつかの QKDN 参照点のプロトコル例として提供されている。

本標準は、QKDN のための信号要求条件とプロトコルのフレームワークについて説明する。QKDN では、様々な種類のプロトコルを使用することができる。本標準は、鍵管理レイヤ、QKDN 制御レイヤ、および QKDN 管理レイヤのための信号要求条件とプロトコルのフレームワークを規定する。2 つの QKD モジュール間で実行される量子レイヤのためのプロトコルは、本標準の範囲外である。

図 1 は、[ITU-T Y.3802]で定義されている QKDN の機能アーキテクチャを示している。

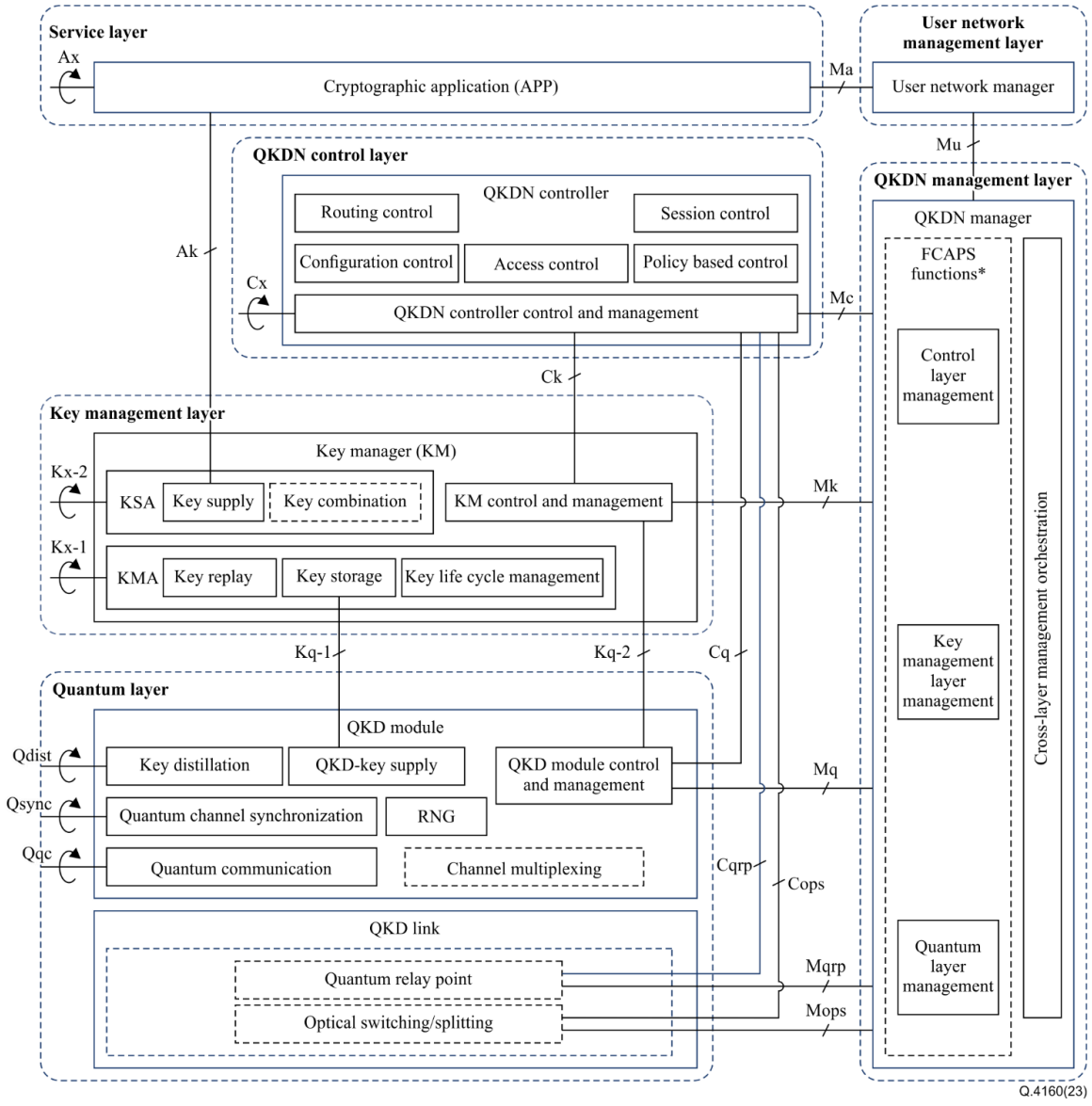


図 1　　[ITU-T Y.3802]で定義されたQKDNの機能アーキテクチャモデル

次の参照点は、[ITU-T Y.3802]で定義されている。

- QKD モジュールの参照点:Qqc、Qsync、Qdist
- KM の参照点:Kq-1、Kq-2、Kx-1、Kx-2
- QKDN コントローラの参照点:Ck、Cq、Cops、Cqrp、Cx
- QKDN マネージャの参照点:Mq、Mops、Mqrp、Mk、Mc、Mu、Mx
- ユーザネットワークマネージャの参照点:Ma
- 暗号アプリケーションの参照点:Ak、Ax

図 1 の機能アーキテクチャモデルと、[ITUT Y.3802]で定義された上記の参照点は、この標準の参照である。

量子レイヤにおける Qqc、Qsync、Qdist の参照点、およびユーザネットワークにおける Ma、Ax の参照点は、この標準の範囲外である。

7. プロトコルスイートとスタック

この章は、各参照点のプロトコルスイートとスタックを規定する。鍵ファイルの形式とメタデータは[ITU-T Y.3803]で定義されている。制御および管理情報は[ITU-T Y.3804]で説明されている。鍵データ、メタデータ、制御および管理情報に関するセキュリティ要求条件と対策は[ITU-T X.1712]で規定されている。

表 1 は、各参照点で伝達される情報をまとめたものである。

表1　参照点における転送情報

参照点	転送情報			注記
	鍵データ	メタデータ	制御および管理情報	
Kq-1	✓	✓	✓	
Kq-2		✓	✓	
Kx-1	✓	✓	✓	OTPなどの鍵リレーのための情報理論的に安全な(ITセキュアな）暗号化が強く推奨される。
Kx-2		✓	✓	
Ck		✓	✓	
Cq		✓	✓	
Cops			✓	
Cqrp			✓	
Cx		✓	✓	
M interfaces			✓	Mインタフェースには、Mq、Mops、Mqrp、Mk、Mc、Mu、およびMxが含まれる。
Ak	✓	✓		

各参照点およびネットワークインタフェースに対して適切なプロトコルを選択することができる。

表 2 は、各参照点において適用可能なプロトコルのリストを含む。

表2　プロトコルスイート

		参考文献	注記
High layer protocols	Remote procedure call (RPC) gRPC HTTP/HTTPS	*RFC 5531[b-IETF RFC 5531]* Cloud native computing foundation (CNCF) gRPC [b-CNCF gRPC] *RFC 9110[b-IETF RFC 9110]*	
L4 protocols	TLS	*RFC 5246[b-IETF RFC 5246]*	

	TCP UDP	*RFC 9293[b-IETF RFC 9293]* *RFC 768[b-IETF RFC 768]*	
L3 protocols	IPv4 IPv6	*RFC 791[b-IETF RFC 791]* *RFC 8200[b-IETF RFC 8200]*	
L2 protocols	Ethernet	*IEEE 802.3[b-IEEE 802.3]*	

図 2 は、QKDN の Ak、Ck、Kx、および Cx インタフェースのプロトコルスタックを示している。

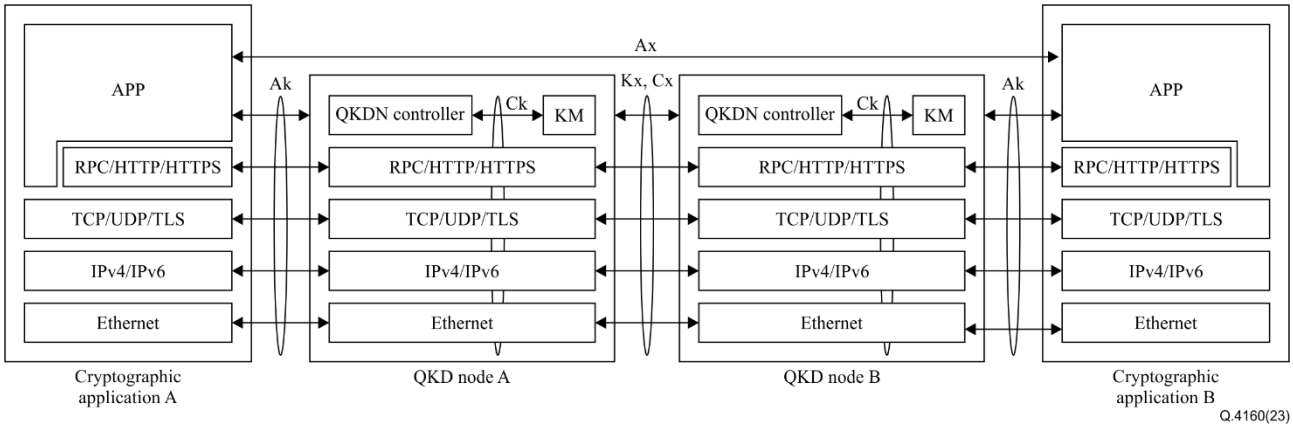


図2　QKDNのAk、Ck、Kx、およびCxインタフェースのプロトコルスタック

図 3 は、QKDN の M インタフェースのプロトコルスタックを示している。

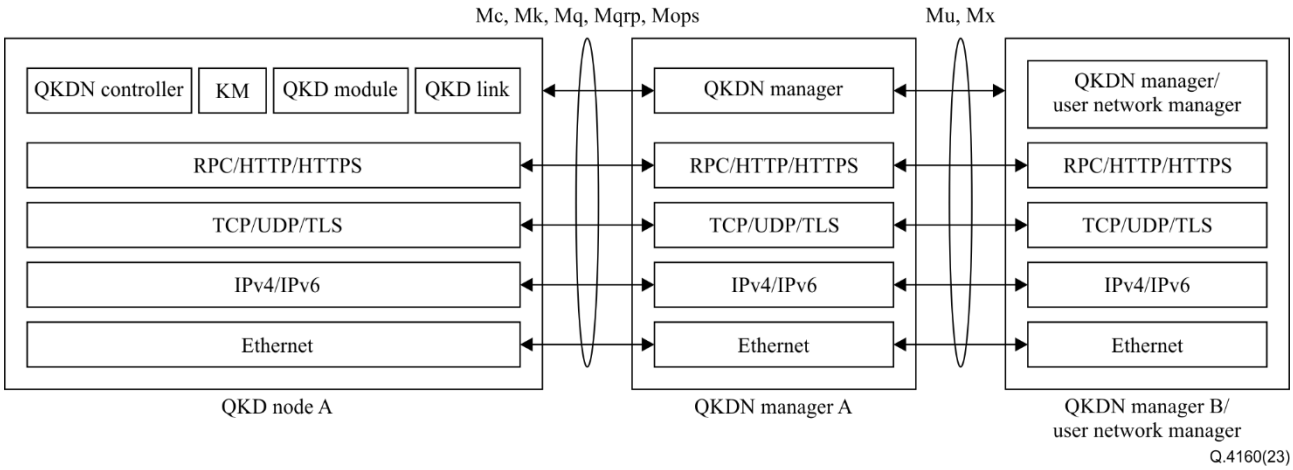


図4　QKDNのMインタフェースのプロトコルスタック

付属資料I

信号手順

（この付属資料は、この標準の不可欠な部分を構成するものではない。）

I.1　要求時鍵供給モード

図 I.1 は、2 つの QKD ノードによって実装された要求時鍵供給モード (Key supply upon request mode)の典型的な信号手順を示す。

図 I.1 に示す典型的な信号手順を以下に簡単に説明する。

1) 送信元の暗号アプリケーションは、送信元QKDノードの送信元KMに鍵要求 (key request)メッセージを送信する。

2) 送信元KMは、要求された鍵および対応する鍵IDを含む鍵要求に対する応答 (response to key request)メッセージを送信元の暗号アプリケーションに応答する。

3) 送信元の暗号アプリケーションは、鍵IDを含む鍵ID通知 (key ID notification)メッセージを送信先の暗号アプリケーションに送信する。

4) 送信先の暗号アプリケーションは、受信した鍵IDを含むID付き鍵要求 (key request with ID)メッセージを、送信先のQKDノードの送信先KMに送信する。

5) 送信先KMは、要求された鍵を含む鍵要求に対する応答 (response to key request)メッセージを送信先の暗号アプリケーションに応答する。

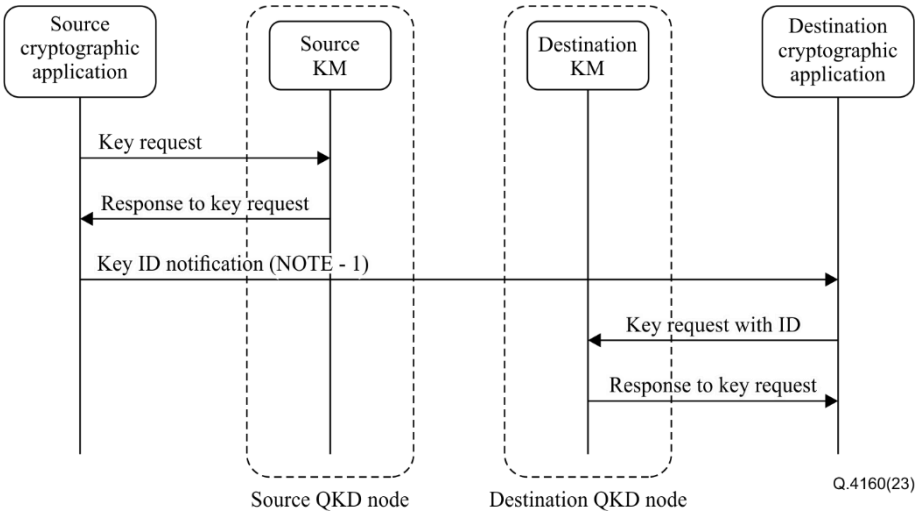


図 I.1　2つのQKDノードによって実装される要求モード鍵供給信号手順

注：鍵ID通知メッセージは、2つの暗号アプリケーション間のAx参照点を通して送信される。この信号メッセージは、この標準の範囲外である。

I.2　プロアクティブ鍵供給モード

I.1 章で説明した要求時鍵供給モード(Key supply upon request mode)の手順に加えて、Ak インタフェースには、事前に鍵を供給するための別のモードがある。このモードでは、送信元 QKD ノードの KM が要求時に鍵供給を開始し、次に送信先 QKD ノードの KM にプロアクティブに鍵供給を行うように指示する。プロアクティブ鍵供給モードは、送信元と送信先の両方の暗号アプリケーションが KSA-鍵を持つ前に直接通信を行わないように制限されているシナリオで採用することができる。

図 I.2 は、2 つの QKD ノードによって実装されたプロアクティブ鍵供給モード (proactive key supply mode)のための典型的な信号手順を示す。

図 I.2 に示す典型的な信号手順を以下に簡単に説明する。

1) 送信元の暗号アプリケーションは、送信元 QKD ノードで送信元 KM にセッション生成要求 (session creation request) メッセージを送信する。

2) 送信元 KM は、セッション生成要求 (session creation request)メッセージを対応する QKDN コントローラに送信する。

3) QKD コントローラは、セッション ID を生成し、そのセッション ID を含むセッション生成通知 (session creation notification)メッセージを、送信先 QKD ノードの送信先 KM に送信する。分散型 QKD コントローラがある場合、セッション生成通知 (session creation notification)メッセージは、送信元 QKD ノードの QKDN コントローラから送信先 QKD ノードの QKDN コントローラに送信され、その後、送信先 KM にリレーされる。

4) 送信先 KM は、受信したセッション ID を含むセッション生成通知 (session creation notification)メッセージを送信先の暗号アプリケーションに送信する。

5) 送信先の暗号アプリケーションは、セッション生成通知に対する応答 (response to session creation notification)メッセージを、セッション生成結果とともに送信先 KM に応答する。

6) 送信先 KM は、受信したセッション生成結果を用いて、対応する QKDN コントローラにセッション生成応答通知 (response to session creation notification)メッセージを応答する。分散型 QKDN コントローラがある場合、セッション生成応答通知 (response to session creation notification)メッセージは、送信先 KM から送信先 QKD ノードの QKDN コントローラに送信され、送信元 QKD ノードの QKDN コントローラにリレーされる。

7) セッションが正常に生成されると、QKDN コントローラは、送信元の QKD ノード内のセッション ID を使用して、セッション生成要求に対する応答 (response to session creation request)メッセージを送信元 KM に応答する。

8) 送信元 KM は、受信したセッション ID を含むセッション生成要求に対する応答 (response to session creation request) メッセージを送信元の暗号アプリケーションに応答する。

9) 送信元の暗号アプリケーションは、送信元 QKD ノード内の送信元 KM に、受信したセッション ID を含むセッション ID 付き鍵要求 (key request with session ID)メッセージを送信する。

10) 送信元 QKD ノードの送信元 KM は、供給される数の鍵を含む鍵供給通知 (key supply notification)メッセージを送信先 QKD ノードの送信先 KM に送信する。

11) 送信先 KM は、通知された数の鍵を含むプロアクティブ鍵供給 (proactive key supply)メッセージを送信先の暗号アプリケーションに送信する。

12) 送信先の暗号アプリケーションは、受信した鍵の鍵 ID を含むプロアクティブ鍵供給に対する応答 (response to proactive key supply)メッセージを KM に応答する。

13) 送信先 KM は、受信した鍵 ID を含む鍵供給通知応答 (response to key supply notification)メッセージを送信元 KM に応答する。

14) 送信元 KM は、受信した鍵 ID に対応する鍵を含むセッション ID 付き鍵要求に対する応答 (response to key request with session ID)メッセージを送信元の暗号アプリケーションに応答する。

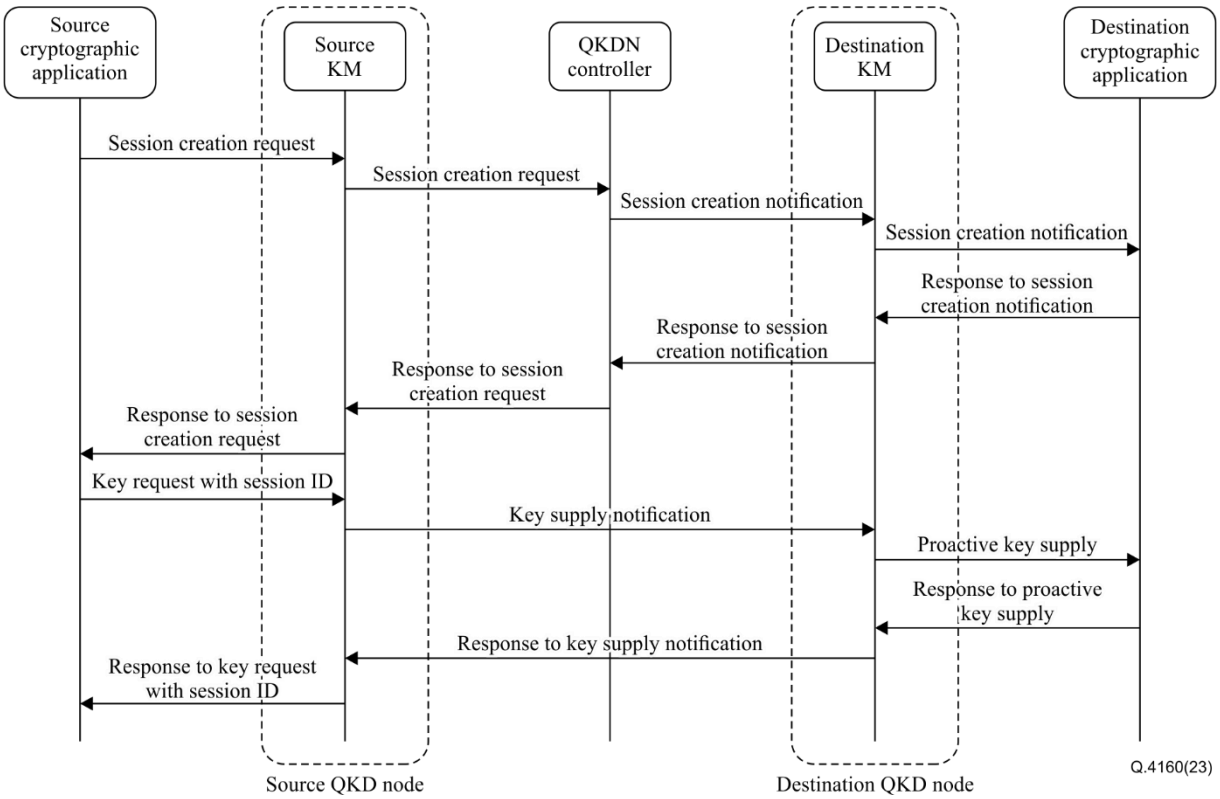


図 I.2　2つのQKDノードによって実装されるプロアクティブモード鍵供給信号手順

I.3　分散型QKDNのための鍵リレー

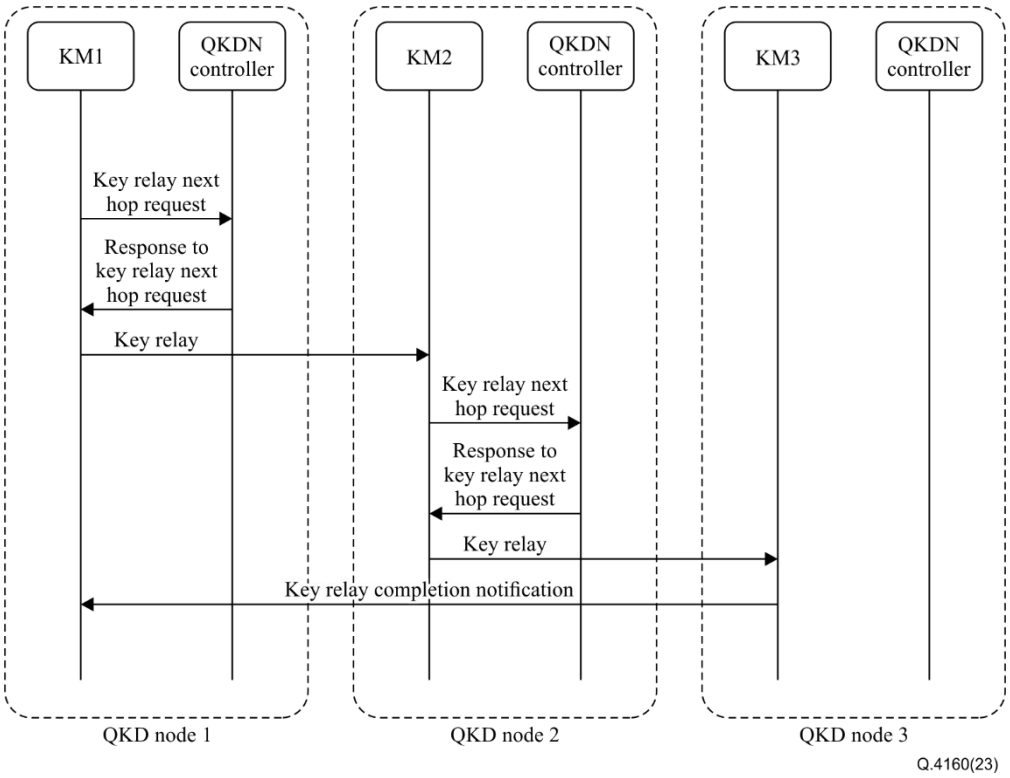
図 I.3 は、[ITU-T Y.3802]で定義されている分散型 QKDN のための鍵リレーのための典型的な信号手順を示す。

1) KM1は、鍵リレー次ホップ要求 (key relay next hop request)メッセージをQKDノード1のQKDコントローラに送信し、QKDコントローラは、鍵リレー次ホップ要求メッセージに対する応答 (response to key relay next hop request)メッセージを鍵リレーの次の送信先とともに応答し、KM1は応答に従い鍵をリレーする。

2) QKDノード2のKM2およびQKDNコントローラは、QKDノード1のKM1と同じ手順を実行する。

3) KM（図中KM3）は、送信先の暗号アプリケーションに最も近いノードである送信先QKDノードに鍵が到達すると、送信元KM（図中KM1）に鍵リレー完了通知 (key relay completion notification)メッセージを送信する。

4) 最も近いKM（図ではKM3として示されている）は、鍵要求に対する応答 (response to key request)メッセージと鍵を応答する。



図I.3　分散型QKDNの鍵リレーのための典型的な信号手順

I.4　集中型QKDNのための鍵リレー

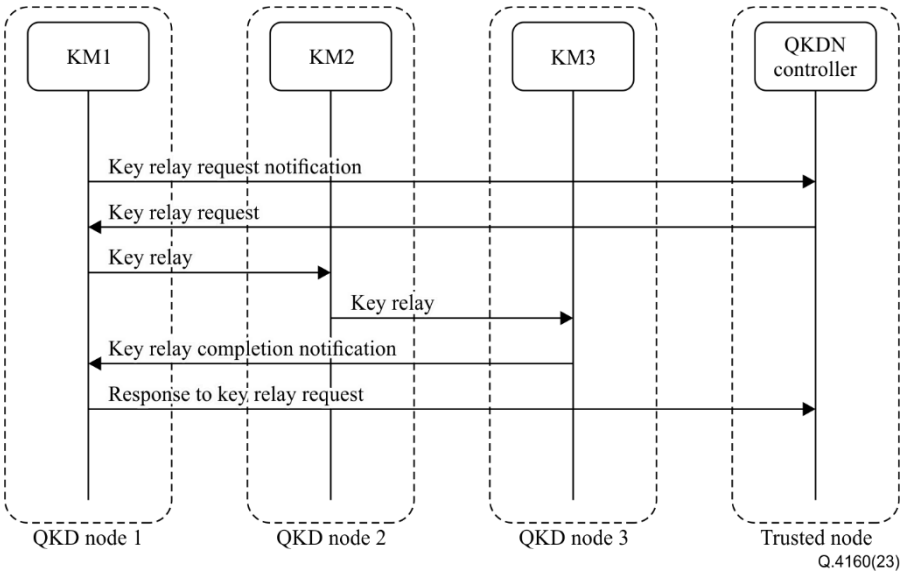
図 I.4a は、[ITU-T Y.3803]で定義された鍵リレースキーム　ケース 2 の下で、[ITU-T Y.3802]で定義されている集中型 QKDN の鍵リレーのための典型的な信号手順を示す。KM1 は、対応する QKDN コントローラへの鍵リレーのための信号手順を開始する。

1) QKDノード1のKM1は、鍵リレー要求通知 (key relay request notification)メッセージをトラステッドノードのQKDNコントローラに送信し、QKDNコントローラは、鍵リレー要求 (key relay request)メッセージに対して、送信先ノードへの全ての鍵リレールートとともに応答する。

2) KM1は、鍵リレー経路に従って鍵リレーを開始する。KM1は、鍵リレー (key relay)メッセージをQKDノード2内のKM2に送信する。

3) QKDノード2のKM2は、鍵リレー経路に従って、QKDノード3のKM3に鍵リレーを行う。

4) 送信先の暗号アプリケーションに最も近いノードである送信先QKDノードに鍵が到達すると、KM（図中KM3）は鍵リレー完了通知 (key relay completion notification)メッセージを送信元KM（図中KM1）に送信し、KM1は鍵リレー要求に対する応答 (response to key relay request)メッセージをトラステッドノード内のQKDNコントローラに送信する。



図I.4a　集中型QKDNのための鍵リレーのための典型的な信号手順

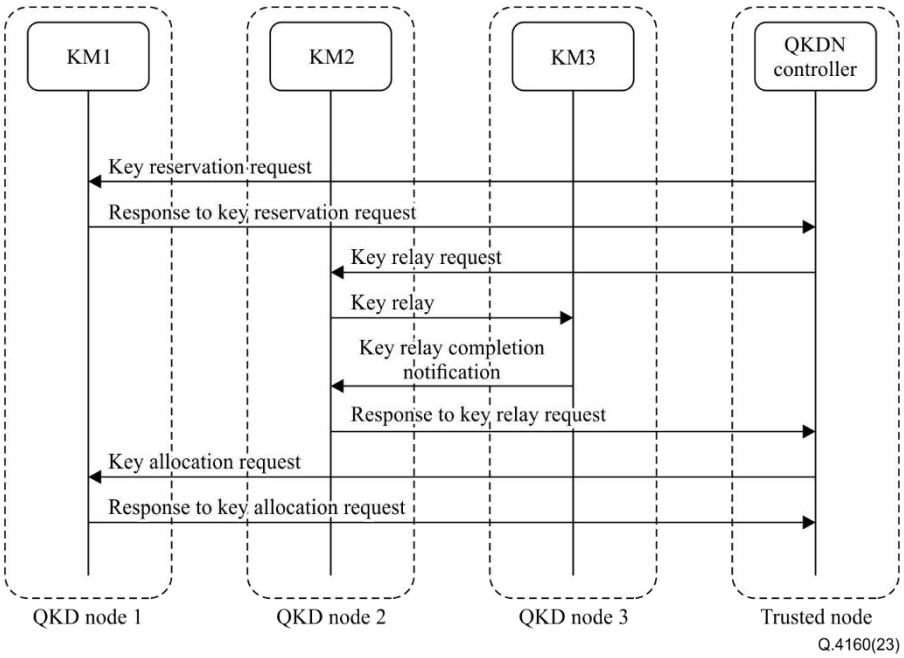
図 I.4b は、[ITU-T Y.3803]の鍵リレースキーム　ケース 1 で、鍵予約を伴う集中型 QKDN のための鍵リレーのための典型的な信号手順を示す。

1) QKDNコントローラは、鍵予約要求 (key reservation request)メッセージをKM1に送信して、送信先KMにリレーされる鍵を予約する。KM1は、鍵予約要求に対する応答 (response to key reservation request)メッセージによってQKDNコントローラに応答を送信する。

2) 次に、対応するQKDコントローラは、送信先ノードへの完全な鍵リレールートを含む鍵リレー要求 (key relay request)メッセージをKM2に送信し、KM2は鍵リレーを開始する。

3) 送信先の暗号アプリケーションに最も近いノードである送信先QKDノードに鍵が到達すると、KM(図中KM3)は鍵リレー完了通知 (key relay completion notification)メッセージを送信元KM(図中KM2)に送信し、KM2は鍵リレー要求に対する応答 (response to key relay request)メッセージを信頼ノードのQKDNコントローラに送信する。

4) QKDNコントローラは、送信先KM3と共有するために予約された鍵を割り当てるために鍵割り当て要求 (key allocation request)を送信し、KM1は、トラステッドノード内の鍵割り当て要求に対する応答 (response to key allocation request)メッセージでQKDNコントローラに応答する。



図I.4b　鍵予約の集中型QKDNの鍵リレーに関する一般的な信号手順

I.5　鍵要求、鍵リレー、および鍵供給

図 I.5a は、[ITU-T Y.3802]で定義されている分散型 QKDN のための鍵要求、鍵リレー、および鍵供給のための典型的な信号手順を示す。

1) 送信元の暗号アプリケーションは、送信元の暗号アプリケーションの最も近いノードであるQKDノード1内のKM1に鍵要求 (key request)メッセージを送信する。

2) KM1は、QKDノード1内のQKDNコントローラに鍵リレー次ホップ要求 (key relay next hop request)メッセージを送信し、QKDNコントローラは、鍵リレーの次ホップ先で鍵リレー次ホップ要求に対する応答 (response to key relay next hop request)メッセージを応答し、KM1は、応答とともに鍵をKM2にリレーする。

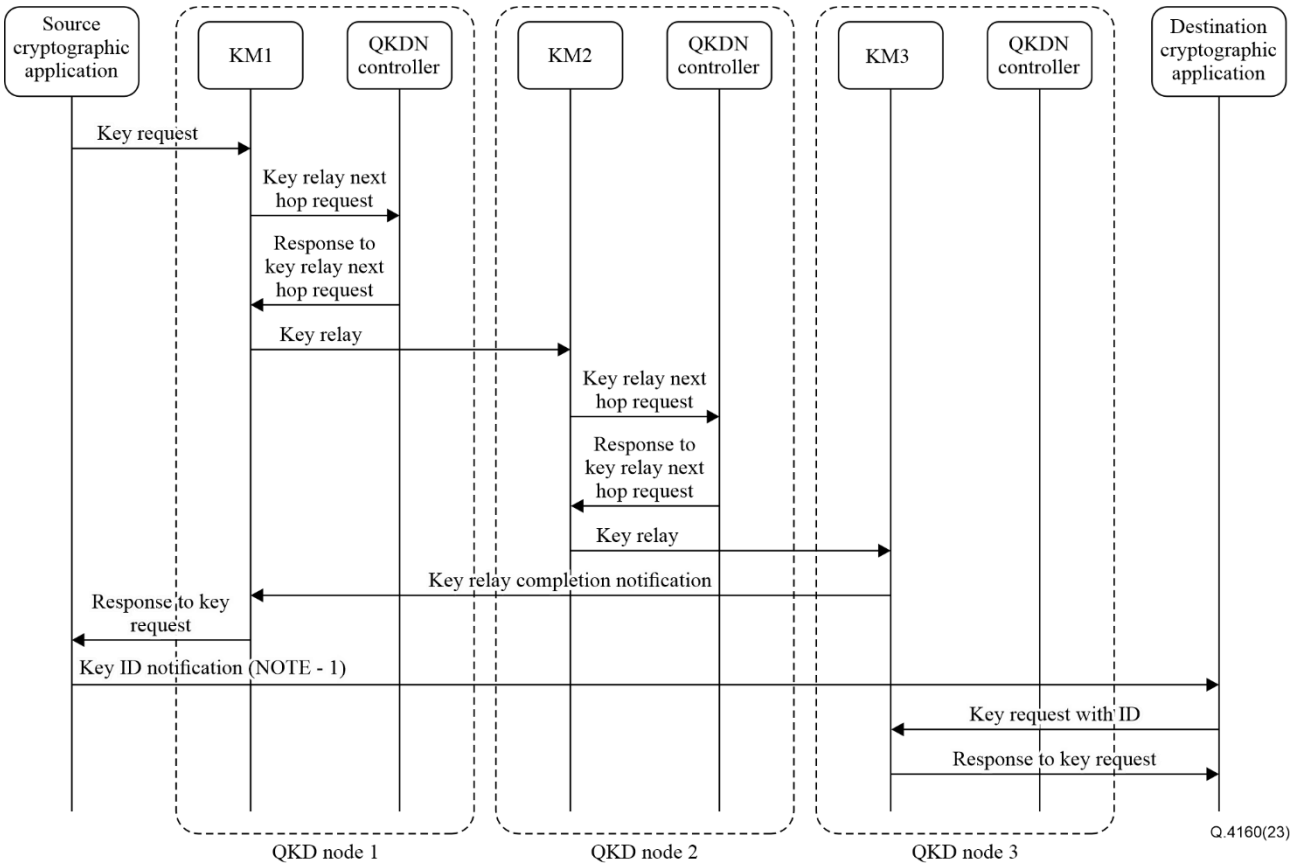
3) QKDノード2のKM2およびQKDNコントローラは、QKDノード1のKM1と同じ手順を実行する。

4) KM（図中KM3）は、送信先の暗号アプリケーションに最も近いノードである送信先QKDノードに鍵が到達すると、鍵リレー完了通知 (key relay completion notification)メッセージを送信元KM（図中KM1）に送信し、KM1は鍵を含む鍵要求応答 (response to key request)メッセージを送信元の暗号アプリケーションを応答する。

5) 送信元暗号アプリケーションは、鍵ID通知 (key ID notification)メッセージを、鍵IDと共に送信先の暗号アプリケーションに送信する。

6) 暗号アプリケーションは、送信元の暗号アプリケーション（ステップ5を参照）から受信した鍵IDを含むID付き鍵要求 (key request with ID)メッセージを、最も近いKM（図ではKM3として示されている）に送信する。

7) 最も近いKM（図ではKM3として示されている）は、鍵を含む鍵要求に対する応答 (response to key request)メッセージに、送信先の暗号アプリケーションへ応答する。



図I.5a　分散型QKDNの鍵要求、鍵リレー、および、鍵供給に関する一般的な信号手順

図 I.5b は、[ITU-T Y.3802]で定義されている集中型 QKDN のための鍵要求、鍵リレー、および鍵供給のための典型的な信号手順を示す。

1) 送信元の暗号アプリケーションは、送信元の暗号アプリケーションの最も近いノードであるQKDノード1内のKM1に鍵要求 (key request)メッセージを送信する。

2) KM1は、鍵リレー要求通知 (key relay request notification)メッセージをトラステッドノードのQKDNコントローラに送信し、QKDNコントローラは、送信先ノードへの完全な鍵リレールートを含む鍵リレー要求 (key relay request)メッセージを応答する。

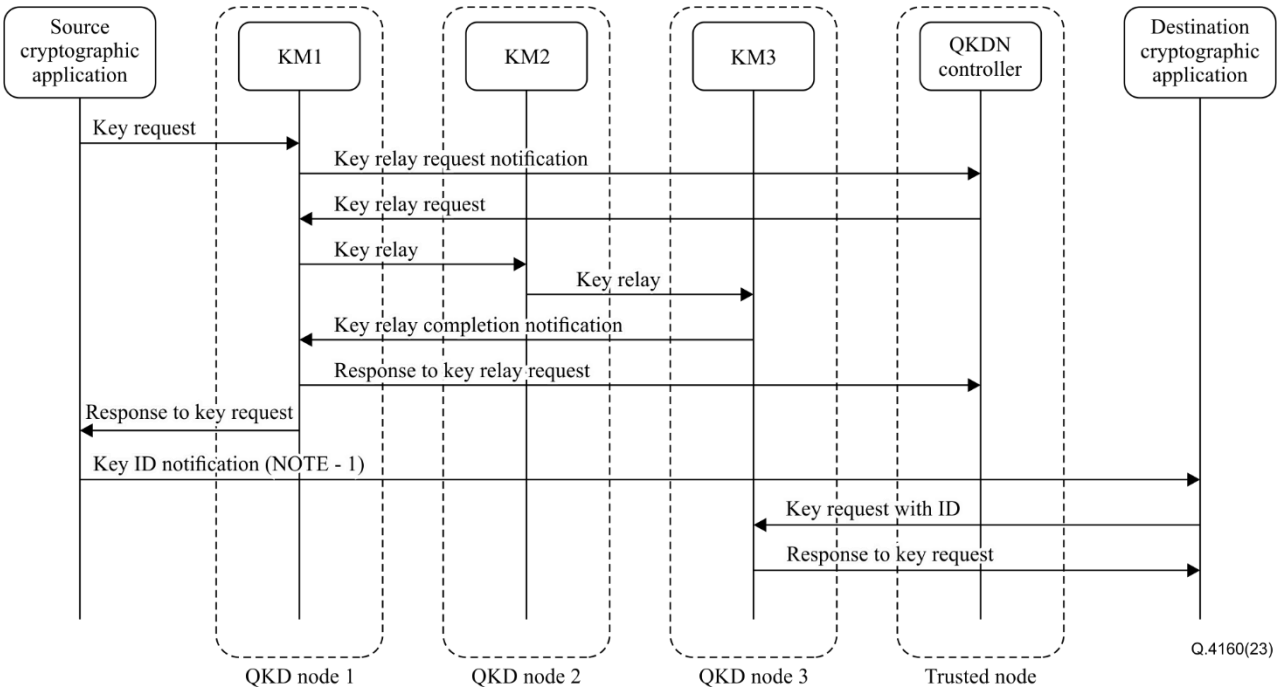
3) KM1は、鍵リレー経路に沿って鍵リレーを開始し、QKDノード2のKM2は、鍵リレー経路に従って鍵リレーを行う。

4) KM（図中KM3）は、送信先の暗号アプリケーションに最も近いノードである送信先QKDノードに鍵が到達すると、鍵リレー完了通知 (key relay completion notification)メッセージを送信元KM（図中KM1）に送信し、次に、KM1は、鍵リレー要求に対する応答 (response to key relay request)メッセージを信頼ノード内のQKDNコントローラに送信するとともに、鍵を含む鍵要求に対する応答 (response to key request)メッセージを送信元暗号アプリケーションに応答する。

5) 送信元暗号アプリケーションは、鍵ID通知 (key ID notification)メッセージを、鍵IDとともに送信先の暗号アプリケーションに送信する。

6) 送信先の暗号アプリケーションは、送信元の暗号アプリケーション（ステップ5を参照）から受信した鍵IDを含むID付き鍵要求 (key request with ID)メッセージを、最も近いKM（図ではKM3として示されている）に送信する。

7) 最も近いKM（図ではKM3として示されている）は、鍵を含む鍵要求に対する応答 (response to key request)メッセージに、送信先の暗号アプリケーションへ応答する。



図I-5b　集中型QKDNの鍵要求、鍵リレー、および　鍵供給に関する一般的な信号手順

注 1：鍵 ID 通知メッセージは、2 つの暗号アプリケーション間の Ax 参照点を介して送信される。この信号メッセージは、この標準の範囲外である。

注 2：図 I.5a および I.5b は、[ITU-T Y.3803]で指定されている鍵リレー方式のケース 2 の信号手順を示している。

参考文献

[b-ITU-T FG-QIT4N D2.3-Part2]	Technical Report ITU-T FG QIT4N D2.3-Part2(2021),Quantum Key Distribution Network Protocols:Key management layer, QKDN Control Layer and QKDN Management Layer.
[b-CNCF gRPC]	gRPC <https://grpc.io/docs/what-is-grpc/> <https://www.cncf.io/projects/grpc/>
[b-ETSI GR QKD 007]	ETSI GR QKD 007 V1.1.1(2018),Quantum Key Distribution(QKD);Vocabulary. <https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01_01_60/gr_QKD007v010101p.pdf>
[b-IEEE 802.3]	IEEE 802.3-2018, IEEE Standard for Ethernet. <https://standards.ieee.org/ieee/802.3/7071/>
[b-IETF RFC 768]	IETF RFC 768 (1980), User Datagram Protocol. <https://datatracker.ietf.org/doc/html/rfc768>
[b-IETF RFC 791]	IETF RFC 791 (1981), Internet Protocol. <https://datatracker.ietf.org/doc/html/rfc791>
[b-IETF RFC 5246]	IETF RFC 5246 (2008), The transport layer security (TLS) protocol − Version 1.2. <https://datatracker.ietf.org/doc/html/rfc5246>
[b-IETF RFC 5531]	IETF RFC 5531 (2009), RPC: Remote Procedure Call Protocol Specification Version 2. <https://datatracker.ietf.org/doc/html/rfc5531>
[b-IETF RFC 8200]	IETF RFC 8200 (2017), Internet Protocol, Version 6 (IPv6) Specification. <https://datatracker.ietf.org/doc/html/rfc8200>
[b-IETF RFC 9110]	IETF RFC 9110(2022),HTTP Semantics. <https://datatracker.ietf.org/doc/rfc9110/>
[b-IETF RFC 9293]	IETF RFC 9293(2022)、Transmission Control Protocol(TCP)<https://datatracker.ietf.org/doc/html/rfc9293>