TTC標準
Standard

JT-Q4164

量子鍵配送ネットワークのCkインタフェースのプロトコル

Protocols for Ck 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.4164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 Ck インタ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-key)[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。

3.1.7　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。

3.1.8　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。

3.1.9　鍵供給エージェント(KSA)リンク[b-ITU-T Y.3802]：鍵供給エージェント(KSA)を接続して鍵同期と完全性検証を実行する通信リンク。

3.1.10　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。

3.1.11　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）
RPC	リモートプロシージャコール (Remote Procedure Call)
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.　Ckインタフェース

Ck インタフェースは、QKDN コントローラと鍵マネージャ(KM)の両者の制御機能と管理機能を接続する参照点である。Ck インタフェースは、QKDN コントローラが制御情報を鍵管理エージェント(KMA)および鍵供給エージェント(KSA)と通信するための手段を提供する。

7.　信号手順

QKDN における鍵要求、鍵リレー及び鍵供給のための信号手順の例は、[ITU-T Q.4160]の付属資料 I に記述されている。信号に適用されるプロトコルスイートは、[ITU-T Q.4160]の 7 章に規定されている。鍵リレー制御のための 2 種類の信号手順は、QKDN のネットワークアーキテクチャが分散型か集中型かによって区別することができる。

7.1.　分散型QKDNにおける鍵リレー要求のための信号手順

分散型 QKDN は、KM 間で送信先 KM への一連のホップを使用して鍵リレーを実行する。分散型 QKDN の Ck インタフェースでは、KM が QKDN コントローラに対して、鍵リレーの次ホップの隣接 KM に関する情報を要求する。次に、KM は、コントローラの応答に基づいて鍵を次の KM にリレーする。次の KM は、コントローラからの次ホップを要求する。この要求とホップの手順は、送信先で鍵リレーが完了するまで繰り返される。

図 1 は、分散型 QKDN における鍵リレー要求の信号手順を示す。

KM は、鍵リレー時ホップ要求を QKDN コントローラに送信して、次ホップの KM 識別子(ID)を取得する。QKDN コントローラは、次の KM にホップするために、可能な KM ID で応答する。

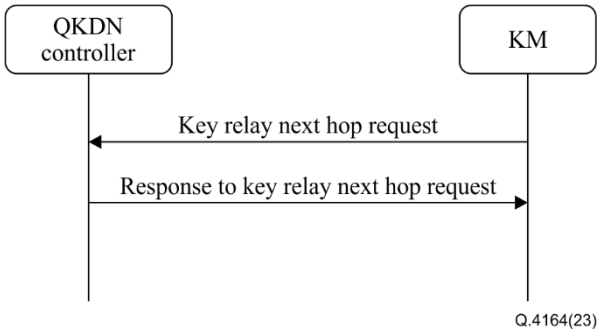


図 1　分散型QKDNの鍵リレーのための典型的な信号手順

7.2.　集中型QKDNにおける鍵リレー要求のための信号手順

集中型 QKDN では、暗号アプリケーションから鍵要求を受信した後に鍵リレーが必要になった場合、KM は QKDN コントローラに鍵リレールートを要求でき、QKDN コントローラは送信先 KM へのルート全体（受け取る KM のリスト）を返す。すべての鍵リレーが完了すると、送信元 KM はその旨の通知を返す。

図 2 は、集中型 QKDN における鍵リレー要求のための信号手順を示す。

暗号化アプリケーションが KM に鍵要求を送信した後、鍵リレーが必要で利用可能なものがない場合、KM は通知とともに QKDN コントローラに鍵リレーを要求する。QKDN コントローラは、送信先 KM への鍵リレーの全ルートを指定し、鍵リレー要求によって要求元 KM に中継 KM のリストを通知する。送信元 KM は、中継 KM のリストに従って鍵リレーを開始する。送信先の暗号化アプリケーションが接続されている KM で鍵リレーが完了すると、送信元 KM は鍵リレー要求への応答によって QKDN コントローラに完了を通知する。

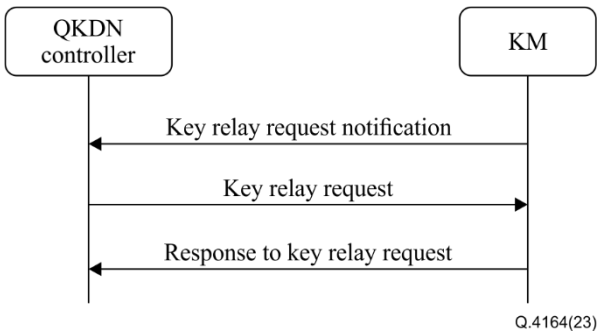


図2　集中型QKDNのための鍵リレーのための典型的な信号手順

7.3.　セッション生成要求の信号手順

送信元、送信先の両方の暗号アプリケーションと KM との間の鍵供給を促進するために、送信元 KM は、対応する QKDN コントローラにセッション生成要求を送信することができ、QKDN コントローラは、セッション ID を生成し、セッションを生成するためのセッション ID を送信先 KM に通知する。QKDN コントローラは、セッション生成結果を受信した後、セッション ID を送信元 KM に応答する。

図 3 は、セッション生成要求の信号手順を示す。

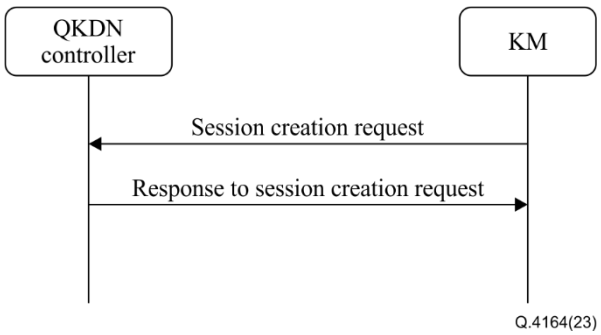


図3　セッション生成要求の信号手順

7.4.　セッション生成通知のための信号手順

対応する QKDN コントローラは、セッション ID を含むセッション生成通知を送信先 KM に送信することができ、送信先 KM は、送信先の暗号アプリケーションに通知する。暗号アプリケーションからセッション生成結果を受信した後、送信先 KM は、対応する QKDN コントローラにセッション ID とともに応答する。

図 4 は、セッション生成通知の信号手順を示しています。

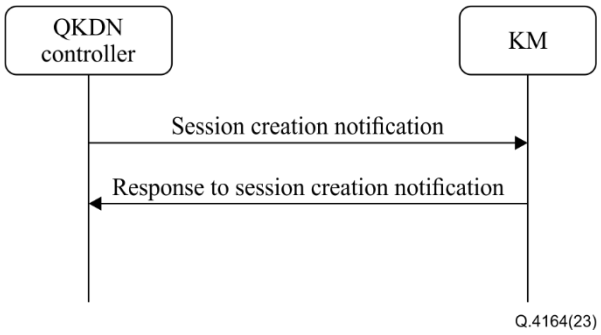


図4　セッション生成通知の信号手順

7.5.　鍵予約要求のための信号手順

QKDN コントローラは、送信先 KM にリレーされる鍵を予約するために、KMA ID を使用して鍵予約要求を KM に送信できる。鍵予約要求を受信した後、KM は対応する QKDN コントローラに対して、予約された KMA 鍵 ID と結果コードとともに鍵予約要求への応答する。

図 5 は、鍵予約要求のための信号手順を示す。

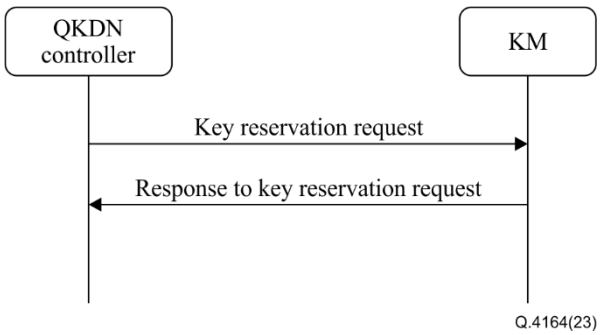


図5　鍵予約要求の信号手順

7.6. 鍵割当要求のための信号手順

対応する QKDN コントローラは、予約された鍵リソースを割り当てるために、KMA ID、KMA-鍵 ID を含む鍵割り当て要求を送信できる。鍵割り当て要求を受信した後、KM は対応する QKDN コントローラに結果コードとともに応答する。

図 6 は、鍵割り当て要求のための信号手順を示す。

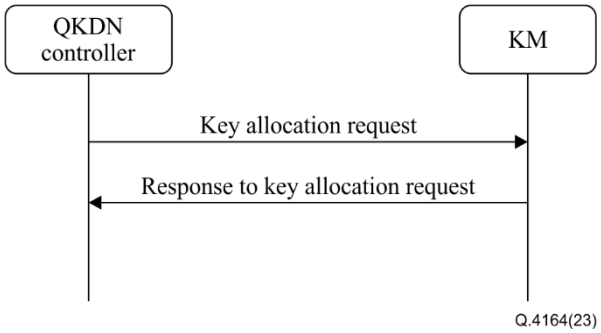


図6　鍵割り当て要求の信号手順

8. 信号メッセージおよびパラメータ

この章は、Ck インタ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 13 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。

この節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 で説明されている。

注：表1から表13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13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. 鍵リレー次ホップ要求メッセージ (Key relay next hop request message)

表 1 は、鍵リレー次ホップ要求メッセージ(Key relay next hop request message)のパラメータを示す。送信先を指定するには、送信先 KMA ID またはアプリケーション送信先 ID のいずれかが必須である。

表1　鍵リレー次ホップ要求メッセージ (Key relay next hop 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
Source KMA ID	鍵リレールート全体の送信元であるKMAのID	String	O	
Destination KMA ID	鍵リレールート全体の送信先であるKMAのID	String	送信先KMA IDまたは送信先アプリケーションIDのいずれかが必須	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	送信先KMA IDまたは送信先アプリケーションIDのいずれかが必須	
Extension	拡張パラメータの配列	Array of objects	O	

8.2. 鍵リレー次ホップ要求に対する応答メッセージ (Response to key relay next hop request message)

表 2 は、鍵リレー次ホップ要求に対する応答メッセージ (Response to key relay next hop request message)のパラメータを示す。分散型 QKDN の場合、QKDN コントローラは、送信先 KMA ID の有無にかかわらず、送信先 KMA に到達する可能性のある KM の ID を返す。

表2　鍵リレー次ホップ要求に対する応答メッセージ (Response to key relay next hop 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
Source KMA ID	鍵リレールート全体の送信元であるKMAのID	String	O	
Destination KMA ID	鍵リレールート全体の送信先であるKMAのID	String	Key relay next hop request messageに送信先アプリケーションIDが含まれている場合は必須	
次のKMA ID	鍵を送信先KMAにリレーするための次のリレーホップとして利用可能なKMAのID	文字列の配列	M	
Extension	拡張パラメータの配列	Array of objects	O	

8.3. 鍵リレー要求通知メッセージ (Key relay request notification message)

鍵リレー要求通知メッセージ (Key relay request notification message)のパラメータを表 3 に示す。集中型 QKDN では、暗号アプリケーションから送信された鍵要求を受信した後、鍵リレーが必要な場合、KM は QKDN コントローラに鍵リレーの全経路を要求することができる。このとき、分散型 QKDN と同様に、鍵リレーの送信先を特定するために、送信先 KMA ID またはアプリケーション送信先 ID のいずれかの情報が必要である。

表3　鍵リレー要求通知メッセージ (Key relay request 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
Source KMA ID	鍵リレールート全体の送信元であるKMAのID	String	O	
Destination KMA ID	鍵リレールート全体の送信先であるKMAのID	String	送信先KMA IDまたは送信先アプリケーションIDのいずれかが必須	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	送信先KMA IDまたは送信先アプリケーションIDのいずれかが必須です	
Extension	拡張パラメータの配列	Array of objects	O	

8.4. 鍵リレー要求メッセージ (Key relay request message)

表 4 は、鍵リレー要求メッセージ (Key relay request message)のパラメータを示す。QKDN コントローラは、送信先 KMA ID の有無にかかわらず、送信先 KMA に到達するためにルート内のすべての KM(中継 KMA ID)を返す。

表4　鍵リレー要求メッセージ (Key relay 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
Source KMA ID	鍵リレールート全体の送信元であるKMAのID	String	O	

Destination KMA ID	鍵リレールート全体の送信先であるKMAのID	String	Key relay request message に送信先アプリケーションIDが含まれている場合は必須。	
Transit KMA IDs	鍵リレールートの中継ノードであるKMAのIDのリスト	String	M	
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	

8.5. 鍵リレー要求に対する応答メッセージ (Response to key relay request message)

表 5 は、鍵リレー要求に対する応答メッセージ (Response to key relay request message)のパラメータを示す。

表5　鍵リレー要求に対する応答メッセージ (Response to key relay 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
Response	Result of key relay	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	

8.6. セッション生成要求メッセージ (Session creation request message)

セッション生成要求メッセージ(Session creation request message)は、送信元の KM から対応する QKDN コントローラに送信される。セッションは、送信元、送信先両者の暗号アプリケーションと KM との間の鍵供給を促進するために生成される。

表 6 は、セッション生成要求メッセージ(Session creation request message)のパラメータを示す。

表6　セッション生成要求メッセージ (Session creation 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
Application source ID	送信元の暗号アプリケーション（すなわち、KSA鍵を受信するために送信元KMに接続するアプリケーション）のID	String	M	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	M	
Number of keys	要求された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。このパラメータは一つのセッションの間に要求されるKSA鍵の最大数として使用することができる。
Extension	拡張パラメータの配列	Array of objects	O	

8.7. セッション生成要求に対する応答メッセージ (Response to session creation request message)

対応する QKDN コントローラから送信元 KM に対して、セッション生成要求メッセージに対する応答が送信される。QKDN コントローラは、セッション生成要求を受信すると、セッション ID を生成し、そのセッション ID を送信先 KM に通知してセッションを生成する。QKDN コントローラは、セッション生成結果を受信すると、そのセッション ID を送信元 KM に応答する。

表 7 は、セッション生成要求に対する応答メッセージ (Response to session creation request message)のパラメータを示す。

表7　セッション生成要求に対する応答メッセージ (Response to session creation 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
Session ID	鍵供給のために生成されたセッションのID	String	M	
Response	セッションの生成の結果	String	M	成功または失敗の理由
Destination KMA ID	送信先KMのID	String	M	
Source KM ID	送信元KMのID	String	O	
Extension	拡張パラメータの配列	Array of objects	O	

8.8. セッション生成通知メッセージ (Session creation notification message)

対応する QKDN コントローラから送信先 KM に対して、セッション生成通知メッセージ(Session creation notification message)が送信される。送信先 KM は、受信したセッション生成ためのセッション ID を送信先の暗号アプリケーションに通知することができる。

表 8 は、セッション生成通知メッセージ(Session creation notification message)のパラメータを示す。

表8　セッション生成通知メッセージ(Session creation 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
Application source ID	送信元の暗号アプリケーション（すなわち、KSA鍵を受信するために送信元KMに接続するアプリケーション）のID	String	M	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	M	
Session ID	鍵供給のために生成されたセッションのID	String	M	
Source KM ID	送信元KMのID	String	M	
Destination KMA ID	KMのID	String	O	
Number of keys	要求された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。 このパラメータは一つのセッションの間に要求されるKSA鍵の最大数として使用することができる。

Extension	拡張パラメータの配列	Array of objects	O	

8.9. セッション生成通知に対する応答メッセージ (Response to session creation notification message)

セッション生成通知に対する応答メッセージ(Response to session creation notification message)は、送信先 KM から対応する QKDN コントローラに送信される。送信先 KM は、セッション生成結果を対応する QKDN コントローラに応答する。

表 9 は、セッション生成通知に対する応答メッセージ(Response to session creation notification message)のパラメータを示す。

表9　セッション生成通知に対する応答メッセージ(Response to session creation 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	
Response	セッション生成の結果	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	

8.10. 鍵予約要求メッセージ (Key reservation request message)

表 10 は、鍵予約要求メッセージ (Key reservation request message)のパラメータを示す。

表10　鍵予約要求メッセージ (Key reservation request)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であるKMAのIdentifier（ID;識別子）	String	M	
Destination KMA ID	鍵リレールート全体の送信先であるKMAのID	String	M	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	O	
Extension	拡張パラメータの配列	Array of objects	O	

8.11. 鍵予約要求に対する応答メッセージ (Response to key reservation request message)

表 11 は、鍵予約要求に対する応答メッセージ (Response to key reservation request)のパラメータを示す。

表11　鍵予約要求に対する応答メッセージ (Response to key reservation request)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のKMAのID	String	O	
Destination KMA ID	鍵リレールート全体の送信先のKMAのID	String	O	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	O	
Key IDs	予約されたKMA-鍵のID	String	M	
Response	鍵予約要求の結果	Integer	M	
Extension	拡張パラメータの配列	Array of objects	O	

8.12. 鍵割当要求メッセージ (Key allocation request message)

表 12 は、鍵割当要求メッセージ (Key allocation request message)のパラメータを示す。

表12　鍵割当要求メッセージ (Key allocation 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
Source KMA ID	鍵リレールート全体の送信元のKMAのID	String	M	
Destination KMA ID	鍵リレールート全体の送信先のKMAのID	String	M	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	O	
Key IDs	予約されたKMA鍵のID	Array of objects	M	
Extension	拡張パラメータの配列	Array of objects	O	

8.13. 鍵割当て要求に対する応答メッセージ (Response to key allocation request message)

表 13 は、鍵割当て要求に対する応答メッセージ (Response to key allocation request message)のパラメータを示す。

表13　鍵割当て要求に対する応答メッセージ (Response to key allocation 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
Source KMA ID	鍵リレールート全体の送信元のKMAのID	String	O	
Destination KMA ID	鍵リレールート全体の送信先のKMAのID	String	O	
Application destination ID	送信先の暗号アプリケーション（すなわち、送信元の暗号アプリケーションが通信することを要求するアプリケーション）のID	String	O	
Key IDs	予約されたKMA-鍵のID	Array of objects	O	
Response	鍵割当要求の結果	Integer	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

制御および管理データは、Ck 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

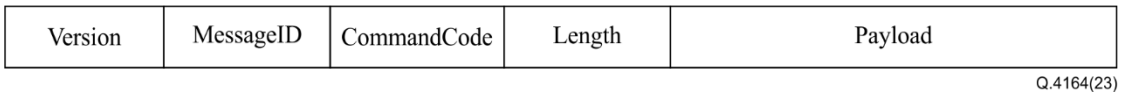
伝送制御プロトコルを使用するプロトコル実装

（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 QKDN コントローラ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：Ckインタ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 と QKDN コントローラ間で相互認証が実行される。相互認証の後、Ck インタフェースを介してコマンド/応答メッセージを転送し、鍵リレー要求を行うことができる。

注3：TLSプロトコルを適用する場合、KMは、QKDNコントローラ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QKDNコントローラのIDを確認できる。同様に、QKDNコントローラは、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。

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
0x1401	鍵リレー次ホップ要求
0x4102	鍵リレー次ホップ要求に対する応答
0x1403	鍵リレー要求通知
0x4104	鍵リレー要求
0x1405	鍵リレー要求に対する応答
0x1406	セッション生成要求
0x4107	セッション生成要求に対する応答
0x4108	セッション生成通知
0x1409	セッション生成通知に対する応答
0x410A	鍵予約要求
0 x 140B	鍵予約要求に対する応答
0x410C	鍵割当要求
0 x 140D	鍵割当要求に対する応答

CommandCode の最初の 2 桁の「14」は、対応するメッセージが KM から QKDN コントローラに送信されることを示し、「41」は、対応するメッセージが QKDN コントローラから KM に送信されることを示す。

付属資料II

gRPC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。

II.1　信号メッセージからgRPCメッセージへのマッピング

gRPC は、クロスプラットフォームでオープンソースの高性能リモートプロシージャコール(RPC)フレームワークである。現在、Linux Foundation 傘下の Cloud Native Computing Foundation(CNCF)の下で開発されている。HTTP 2.0 を使用し、複数のプログラミング言語をサポートしている[bCNCF gRPC]。

表II.1-1　gRPCメッセージへの信号メッセージのマッピング例

信号メッセージ	gRPCメッセージ名
Key relay request notification	KeyRelayRequestNotification
Key relay request	KeyRelayRequest
Response to key relay request	KeyRelayResponse
Key reservation request	KeyReservationRequest
Response to key reservation request	KeyReservationResponse
Key allocation request	KeyAllocationRequest
Response to key allocation request	KeyAllocationResponse

II.2　鍵リレー要求通知メッセージ (Key relay request notification message)

表 II.2-1 は、gRPC プロファイルへの鍵リレー要求通知メッセージ **(**Key relay request notification meaage)マッピング例を示す。

表II.2-1　gRPCプロファイルへの鍵リレー要求通知 (Key relay request notification)メッセージマッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Extension	not mapped	

II.3　鍵リレー要求とそれに対する応答メッセージ (Key relay request and response message)

表 II.3-1 は、gRPC プロファイルへの鍵リレー要求メッセージ (Key relay request message)マッピングの例を示す。表 II.3-2 は、応答メッセージマッピングの例を示す。

表II.3-1　gRPCプロファイルへの鍵リレー要求メッセージ (Key relay request message)マッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Transit KMA IDs	gRPC'kma_id'	String
Key relay request ID	gRPC 'keyrelayrequest_id'	String
Extension	not mapped	

表II.3-2　gRPCプロファイルへの鍵リレー要求に対する応答メッセージ (Response to key relay request message)マッピング例

パラメータ	マップ先	データタイプ
Response	gRPC 'result_code'　例) 0:OK、1:NG	Integer
Key relay request ID	gRPC 'keyrelayrequest_id'	String
Extension	gRPC 'error_message'	String

II.4　鍵予約要求とそれに対する応答メッセージ (Key reservation request and response message)

表 II.4-1 は、gRPC プロファイルへの鍵予約要求メッセージ (Key reservation request message)マッピングの例を示す。表 II.42 は、応答メッセージマッピングの例を示す。

表II.4-1　gRPCプロファイルへの鍵予約要求メッセージ (key reservation request message)マッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Extension	not mapped	

表II.4-2　gRPCプロファイルへの鍵予約要求に対する応答メッセージ (response to key reservation request message)マッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Response	gRPC 'result_code'　例) 0:OK、1:NG	Integer
Extension	gRPC 'error_message'	String

II.5　鍵割当要求とそれに対する応答メッセージ (Key allocation request and response message)

表 II.5-1 は、gRPC プロファイルへの鍵割当要求メッセージ (Key allocation request message)マッピングの例を示す。表 II.5-2 は、応答メッセージマッピングの例を示す。

表II.5-1　gRPCプロファイルへの鍵割当要求メッセージ (Key allocation request message)マッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Extension	not mapped	

表II.5-2　gRPCプロファイルへの鍵割当要求メッセージに対する応答メッセージ (Response to key allocation request message)マッピング例

パラメータ	マップ先	データタイプ
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Response	gRPC 'result_code'　例) 0:OK、1:NG	Integer
Extension	gRPC 'error_message'	String

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-CNCF gRPC]	Cloud Native Computing Foundation(2024).What is gRPC?Mountain View, CA:gPRC authors. Available[viewed 2023-03-03]at;https://gRPC.io/docs/what-is-gRPC/See also[viewed 2023-03-03]:https://www.cncf.io/projects/gRPC/
[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).