TTC標準
Standard

# JT-Q4161

## 量子鍵配送ネットワークのAkインタフェースのプロトコル

## Protocols for Ak 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.4161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 Ak 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. 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. 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。

3.1.3. 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。

3.1.4. 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。

3.1.5. 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。

3.1.6. 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。

3.1.7. 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。

3.1.8. 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。

3.1.9. 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。

3.1.10. 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。

3.1.11. 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） |
| 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. Akインタフェース

参照点 Ak は、暗号アプリケーションと KSA 内の鍵供給機能を接続する。Ak は、暗号アプリケーションから KSA に鍵要求を送信し、暗号アプリケーションと KSA の間で認証を実行し、KSA から暗号アプリケーションに鍵を供給する役割を果たす。

## 7. 信号手順

Ak インタ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) 要求時鍵供給モード：送信元と送信先の両方のKMは、対応する**暗号アプリケーション**から鍵要求を受信した後に、鍵供給を開始する。

2) プロアクティブ鍵供給モード：送信元のKMは、要求に応じて鍵供給を開始し、次に送信先のKMに対して、プロアクティブに鍵を供給するように指示する。

注：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できる。

[ITU-T Q.4160]の付属資料 I では、QKDN 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. 要求時鍵供給モード信号手順

#### 7.1.1. 送信元の鍵要求

暗号アプリケーションが暗号化のために鍵を必要とする場合、鍵要求を KM に送信し、KM が鍵を提供する。KM に十分な数の鍵が格納されていない場合、KM は必要な数を共有するために鍵生成または鍵リレーを開始し、生成またはリレーが完了したときにそれらを暗号アプリケーションに提供する。

図 1 は、送信元の Ak インタフェースでの鍵要求の信号手順を示している。

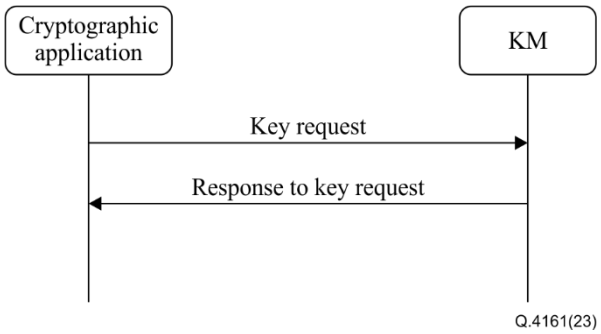



**図1　送信元のAkインタフェースの鍵要求の信号手順**

#### 7.1.2. 送信先の識別子を伴う鍵要求

送信先の暗号アプリケーションは、接続先の KM から鍵を要求する。送信先の暗号アプリケーションは、鍵を指定するために、送信元の暗号アプリケーションから受信した鍵識別子(ID)を使用して要求を送信する。

図 2 は送信先の Ak インタフェースで ID を含む鍵要求の信号手順を示す。

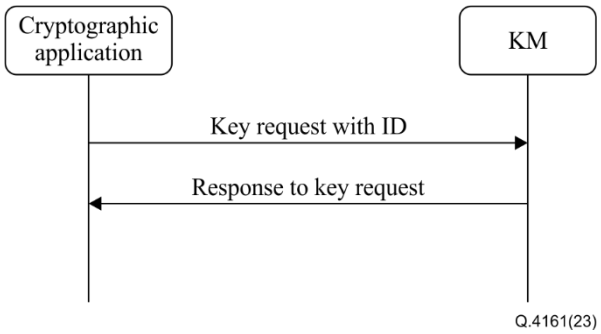



**図2　送信先のAkインタフェースのIDを伴う鍵要求信号手順**

### 7.2. プロアクティブ鍵供給モード信号手順

#### 7.2.1. 送信元のセッション生成

暗号アプリケーションが暗号化用の鍵を必要とする場合、まず、送信元 KM にセッション生成要求を送信する。次に、送信元 KM は、セッションを生成するように送信先 KM に通知し、セッションが正常に生成されると、送信元の暗

号アプリケーションにセッション ID で応答する。生成されたセッションに基づいて、送信元の暗号アプリケーションは、送信元 KM から鍵を要求できる。

図 3 は、送信元の Ak インタフェースでセッションを生成するための信号手順を示す。

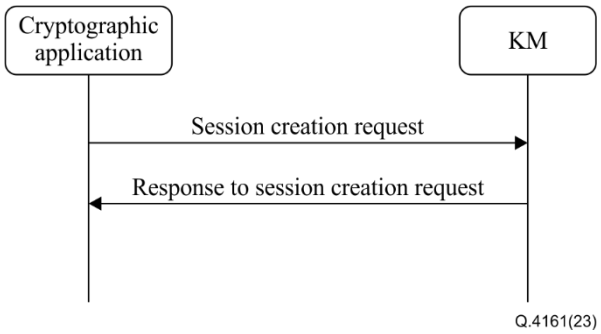



**図3**　送信元のAkインタフェースのセッション生成信号手順

### 7.2.2.　送信先のセッション生成

暗号アプリケーションは、接続先の KM からセッション生成通知を受信する。送信先 KM は、セッションを指定するために、送信元 KM から受信したセッション ID を使用して通知を送信する。

図 4 は、送信先の Ak インタフェースでセッションを生成するための信号手順を示す。

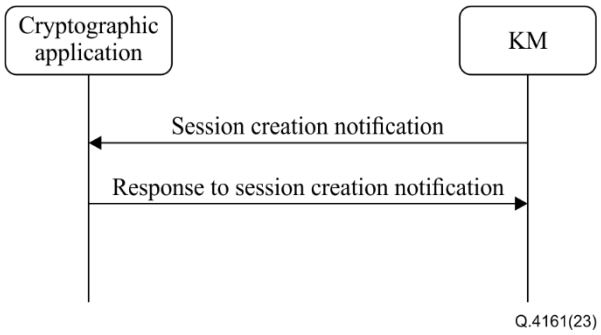



**図4**　送信先のAkインタフェースのセッション生成信号手順

### 7.2.3.　送信先のセッション識別子を含む鍵要求

セッションが生成されると、送信元 KM は、送信元の暗号アプリケーションからの要求に応じて KSA-鍵を提供する。

図 5 は、送信元の Ak インタフェースでのセッション ID を含む鍵要求の信号手順を示す。

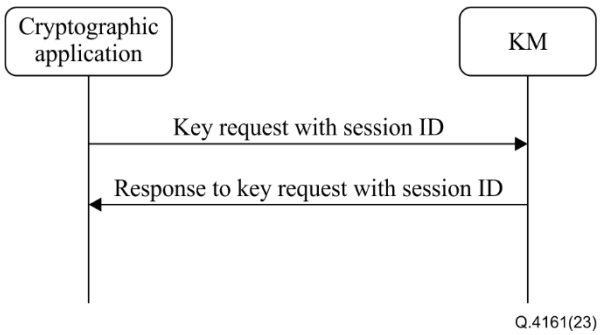



**図5**　送信先のAkインタフェースのセッションIDを含む鍵要求信号手順

### 7.2.4. 送信先のプロアクティブ鍵供給

送信先 KM は、それが接続されている送信先の暗号アプリケーションに KSA-鍵をプロアクティブに供給する。この方式は、送信元の暗号アプリケーションからの鍵要求を送信元 KM が受信した場合に適用でき、送信元 KM は、送信先 KM に対してプロアクティブに鍵を供給するように指示する。

図 6 は、Ak インタフェースでのプロアクティブ鍵供給の信号手順を示す。

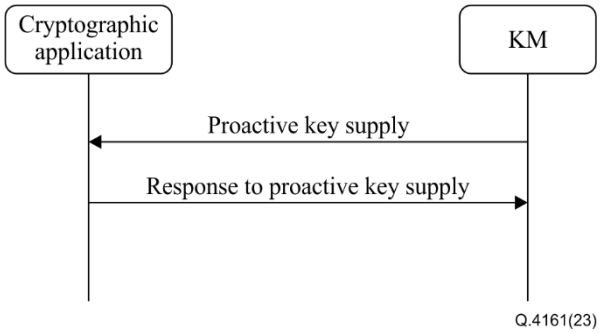



**図6** 送信先のAkインタフェースのプロアクティブ鍵供給信号手順

## 8. 信号メッセージおよびパラメータ

この節は、Ak 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 11 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 11 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 11 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. 要求時鍵供給モードのメッセージとパラメータ

#### 8.1.1. 鍵要求メッセージ (Key request message)

暗号アプリケーションから送信元 KM にメッセージが送信され、鍵が要求される。

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

表1 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 |
|---|---|---|---|---|
| Application source ID | 送信元の暗号アプリケーション(つまり、このメッセージを送信するアプリケーション)のID | String | O | |
| Application destination ID | 送信先のアプリケーション(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 | |
| Application name | 暗号アプリケーションの名前 | 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。 |
| Size of key | 要求された各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 | |

### 8.1.2. ID付き鍵要求メッセージ(Key request with identifier message)

KSA 鍵を受信すると、送信元の暗号アプリケーションは、対応する鍵 ID を暗号アプリケーションに送信する。送信先の暗号アプリケーションは、鍵 ID を使用して送信先 KM に要求を送信する。次に、送信先の暗号アプリケーションは、送信元 KM と送信先 KM の間で共有されている鍵を受信する。

表 2 に、ID 付き鍵要求メッセージ(Key request with identifier message)のパラメータを示す。

表2　ID付き鍵要求メッセージ(Key request with identifier 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のID | String | M | |
| Application destination ID | 送信先の暗号アプリケーション(つまり、このメッセージを送信するアプリケーション)のID | String | O | |
| Application name | 暗号アプリケーションの名前 | String | O | |
| Key IDs | 要求されたKSA-鍵のID | Array of objects | M | これらのIDは、送信元の暗号アプリケーションから通知される。 |
| Key ID | 要求されたKSA-鍵のID | String | M | |
| Key ID extension | Key ID拡張子 | Object | O | |
| Extension | 拡張パラメータの配列 | Array of objects | O | |

### 8.1.3. 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は、暗号アプリケーションからの鍵要求または ID 付きの鍵要求に応答して、KM から暗号アプリケーションに送信される。KM は、要求された KSA-鍵を暗号アプリケーションに提供する。鍵要求に対する応答については、送信元と送信先で違いはない。

表 3 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3　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 | 説明 | 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KSA-鍵データ | String | M | |
| Key ID | 提供されたKSA-鍵のID | String | M | |
| Key extension | 鍵ファイルの拡張子 | Object | O | ハッシュ値など |
| 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 | |

## 8.2. 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

### 8.2.1. 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、暗号アプリケーションから送信元の KM に送信される。セッションは、送信元と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にするために生成される。

表 4 に、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4　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 | 説明 | 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(つまり、このメッセージを送信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 | |
| Application name | 送信元の暗号アプリケーション名 | 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。<br>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 | |

### 8.2.2. 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)

セッション生成要求メッセージに対する応答メッセージ(Response to session creation request message)は、送信元の KM から暗号アプリケーションに送信される。セッション生成要求を受信した送信元 KM は、セッションを生成するように送信先 KM に通知し、セッションが正常に生成されたときにセッション ID を使用して送信元の暗号アプリケーションに応答する。

表 5 に、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5　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 | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|
| Session ID | 生成されたセッションのID | String | M | |
| Response | セッション生成の結果 | String | M | 成功、失敗の理由、または鍵供給の状態テーブル |
| 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 | |

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

セッション生成通知メッセージ(Session creation notification message)は、送信先の KM から暗号アプリケーションに送信される。送信先 KM は、セッション ID を送信先の暗号アプリケーションに事前に送信し、通信を要求している送信元の暗号アプリケーションの ID とともに通知する。

表 6 に、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6　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 | 説明 | 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(つまり、このメッセージを受信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 | |
| Application name | 送信元の暗号アプリケーションの名前 | String | O | |
| Session ID | 生成されたセッションの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。<br>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 | |

### 8.2.4. 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、暗号アプリケーションから KM に対して、送信先のセッション生成通知に応じて送信され、送信先の暗号アプリケーションは、セッションの生成結果を送信先の KM に通知する。

表 7 に、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7　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 | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|
| Session ID | 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 |
| Extension | 拡張パラメータの配列 | Array of objects | O | |

### 8.2.5. セッションID付き鍵要求メッセージ(Key request with session identifier message)

セッションが生成されると、暗号アプリケーションはセッション ID メッセージを含む鍵要求を送信元の KM に送信する。次に、送信元 KM は、セッション中に要求された KSA-鍵を送信元の暗号アプリケーションに提供する。

表 8 に、セッション ID 付き鍵要求メッセージ(Key request with session identifier message)のパラメータを示す。

表8　セッションID付き鍵要求メッセージ(Key request with session identifier message)のパラメータ

| パラメータ | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Session ID | 生成されたセッションの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。 |
| Size of key | 要求された各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 | |

### 8.2.6. セッションID付き鍵要求に対する応答メッセージ(Response to key request with session identifier message)

セッション ID 付き鍵要求に対する応答メッセージ(Response to key request with session identifier message)が、送信元の KM から暗号アプリケーションに送信される。次に、送信元 KM は、生成されたセッション中に、要求された KSA 鍵を送信元の暗号アプリケーションに提供する。

表 9 に、セッション ID 付き鍵要求に対する応答メッセージ(Response to key request with session identifier message)のパラメータを示す。

表9　セッションID付き鍵要求に対する応答(Response to key request with session identifier message)のパラメータ

| パラメータ | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|
| Session ID | 生成されたセッションのID | String | M | |
| 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KSA-鍵データ | String | M | |
| Key ID | 提供されたKSA-鍵のID | String | M | |
| Key extension | 鍵ファイルの拡張子 | Object | O | ハッシュ値など |
| 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 | |

### 8.2.7. プロアクティブ鍵供給メッセージ(Proactive key supply message)

プロアクティブ鍵供給メッセージ(Proactive key supply message)は、送信先の KM から暗号アプリケーションに送信される。送信先 KM は、生成されたセッション中に、KSA-鍵を送信先の暗号アプリケーションにプロアクティブに供給する。

表 10 に、プロアクティブ鍵供給メッセージ(Proactive key supply message)のパラメータを示す。

表10　プロアクティブ鍵供給メッセージ(Proactive key supply message)のパラメータ

| パラメータ | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|
| Session ID | 生成されたセッションのID | String | M | |
| 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 | 提供されたKSA-鍵データ | String | M | |
| Key ID | 提供されたKSA-鍵のID | String | M | |
| Key extension | 鍵ファイルの拡張子 | Object | O | ハッシュ値など |
| Extension | 拡張パラメータの配列 | Array of objects | O | |

### 8.2.8. プロアクティブ鍵供給に対する応答メッセージ(Response to proactive key supply message)

送信先でのプロアクティブ鍵供給に応答して、暗号アプリケーションから KM にプロアクティブ鍵供給メッセージ(Proactive key supply message)に対する応答が送信される。送信先の暗号アプリケーションは、KSA 鍵の受信を送信先 KM に通知する。

表 11 に、プロアクティブ鍵供給に対する応答メッセージ(Response to proactive key supply message)のパラメータを示す。

表11　プロアクティブ鍵供給に対する応答メッセージ(Response to proactive key supply message)のパラメータ

| パラメータ | 説明 | データタイプ | M/O | 備考 |
|---|---|---|---|---|
| Session ID | 生成されたセッションのID | String | M | |
| Key ID | 受信したKSA-鍵のID | String | M | |
| Response | KSA-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 | |

## 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、Ak 基準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**

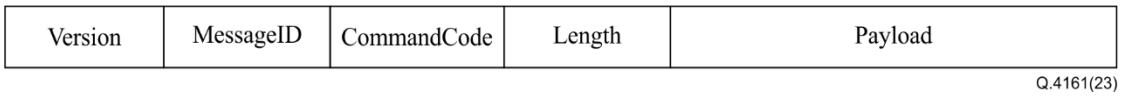
**伝送制御プロトコルを使用するプロトコル実装**

(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。

暗号アプリケーションは、TCP[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 に示す。




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：Ak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一意のコード(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[bIETF 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、暗号アプリケーションと KM との間で相互認証が実行される。相互認証の後、Ak 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、鍵要求と鍵供給を行うことができる。

注 3-TLS プロトコルを適用する場合、暗号アプリケーションは、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、暗号アプリケーション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暗号アプリケーションの 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リストする。

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 |
|---|---|
| 0x2101 | 鍵要求 |
| 0x2102 | ID付き鍵要求 |
| 0x1203 | 鍵要求に対する応答 |
| 0x2104 | セッション生成要求 |
| 0x1205 | セッション生成要求に対する応答 |
| 0x1206 | セッション生成通知 |
| 0x2107 | セッション生成通知に対する応答 |
| 0x2108 | セッションID付き鍵要求 |
| 0x1209 | セッションID付き鍵要求に対する応答 |

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 |
|---|---|
| 0x120A | プロアクティブ鍵供給 |
| 0x210B | プロアクティブ鍵供給に対する応答 |

CommandCode の最初の 2 桁「12」は、対応するメッセージが KM から暗号アプリケーションに送信されることを示し、「21」は、対応するメッセージが暗号アプリケーションから 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。)

8.1 章で規定された要求時鍵供給モード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、8.1 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、暗号アプリケーションと KM 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(SAE)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、8.1.1 章で規定された鍵要求メッセージ(Key request message)は、[b-ETSI GS QKD 014]で規定された 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 要求に対応する。表 II.1 は、鍵要求メッセージ(Key request message)の Get Key メソッドへのマッピングをリストする。

表II. 1　Get Keyメソッドへの鍵要求メッセージのマッピング

| パラメータ | M/O | データタイプ | Get Keyメソッドでの実装 |
|---|---|---|---|
| Application source ID | O | String | なし |
| Application destination ID | M | String | アクセスURLの「{target_SAE_ID}」部分 |
| Application name | O | String | なし |
| Number of keys | O | Integer | 鍵要求データ形式の「番号」項目 |
| Size of key | O | Integer | 鍵要求データ形式のsize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　ID付き鍵要求メッセージ(Key request with identifier message)

この実装では、8.1.2 章で規定された ID 付き鍵要求メッセージ(Key request with identifier message)は、[b-ETSI GS QKD 014]で規定された ID 付き鍵取得方法として実行される HTTPS トランザクションの HTTPS 要求に対応する。表 II.2 は、ID 付き鍵要求メッセージの ID 付き鍵取得方法へのマッピングを示す。

表II.2　Get Key with IDメソッドへの識別子メッセージを伴う鍵要求のマッピング

| パラメータ | M/O | データタイプ | Get Key with IDメソッドの実装 |
|---|---|---|---|
| Application source ID | M | String | アクセスURLの「{initiator_SAE_ID}」部分 |
| Application destination ID | O | String | なし |
| Application name | O | String | なし |
| Key IDs | M | Array of objects | 鍵IDデータ形式のkey_IDs項目 |
| Key ID | M | String | 鍵IDデータ形式のkey_ID項目 |
| Key ID extension | O | Object | 鍵IDデータ形式のkey_ID_extension |
| Extension | O | Array of objects | 鍵IDデータ形式のkey_IDs_extension |

### II.3　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、8.1.3 章で指定された鍵要求メッセージに対する応答(Response to key request message)は、Get Key メソッドまたは Get Key with ID メソッドとして実行された HTTPS トランザクションの HTTPS 応答に対応する。表 II.3 は、鍵要求メッセージに対する応答の Get Key メソッドまたは Get Key with ID メソッドへのマッピングをリストする。

表II.3　Get Key/Get Key with IDメソッドへの鍵要求メッセージに対する応答のマッピング

| パラメータ | M/O | データタイプ | Get Keyまたは<br>Get Key with IDメソッド |
|---|---|---|---|
| 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「鍵」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メソッドまたはGet Key with IDメソッドとして実行された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), 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-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).