

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

I. <概要>

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

II. <参考>

1. 国際標準等の関連

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 章立ての相違

なし

2. 4 その他

なし

JT-Q4161

Protocols for Ak interfaces for quantum key distribution networks

I. < Outline >

This standard specifies the protocol for Ak Interface of Quantum Key Distribution Network (QKDN), in particular in the following areas:

- Signal procedure
- Signal message and parameters
- Security considerations

II. < References >

1. Relevance to international standards, etc.

This standard specifies an overview of quantum key distribution networks and conforms to ITU-T Recommendation Q. 4161 issued at ITU-T SG11 in December 2023.

2. Additional items to the above recommendations, etc.

2.1 Optional selectable items

None

2.2 National matter determining items

None

2.3 Difference in chapter structure

None

2.4 Other

None

3. 改版の履歴

版数	制定日	改版内容
1.0	2025 年*月*日	制定

4. その他

4. 1 参照する勧告、標準など

JT 標準 JT-Q4160, JT-X1712

5. 標準策定部門

信号制御専門委員会

III.<目次>

1. 規定範囲
2. 参照文献
3. 用語定義
 - 3.1. 他の標準等で定義されている用語
 - 3.2. 本標準で定義された用語定義
4. 略称
5. 表記法
6. Ak インタフェース
7. 信号手順
 - 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
 - 7.1.2. 送信元の識別子を伴う鍵要求
 - 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

3. Revision History

Number of editions	Date of enactment	Revision Contents
1.0	January *, 2025	Established

4. Other

4.1 Recommendations, standards, etc.

JT Standards JT-Q4160, JT-X1712

5. Standards Development Department

Signal Control Expert Committee

III. <Table of contents>

1. Scope of Regulations
2. References
3. Definition of Terms
 - 3.1. Terms defined in other standards
 - 3.2. Definitions of terms defined in this standard
4. Abbreviation
5. Notation
6. Ak Interface
7. Signal Procedure
 - 7.1. Request key supply mode signaling procedure
 - 7.1.1. Source key request
 - 7.1.2. Key request with source identifier
 - 7.2. Proactive key supply mode signaling procedure
 - 7.2.1. Source session generation

7.2.2.	送信先のセッション生成
7.2.3.	送信先のセッション識別子を含む鍵要求
7.2.4.	送信先のプロアクティブ鍵供給
8.	信号メッセージおよびパラメータ
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
8.1.2.	ID 付き鍵要求メッセージ
8.1.3.	鍵要求メッセージに対する応答
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
8.2.2.	セッション生成要求に対する応答メッセージ
8.2.3.	セッション生成通知メッセージ
8.2.4.	セッション生成通知に対する応答メッセージ
8.2.5.	セッション ID 付き鍵要求メッセージ
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
8.2.7.	プロアクティブ鍵供給メッセージ
8.2.8.	プロアクティブ鍵供給に対する応答メッセージ
9.	セキュリティに関する考慮事項
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	
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	
II.1	鍵要求メッセージ
II.2	ID 付き鍵要求メッセージ
II.3	鍵要求メッセージに対する応答
参考文献	

7.2.2.	Session generation of the destination
7.2.3.	Key request including the session identifier of the destination
7.2.4.	Proactive key supply of the destination
8.	Signal messages and parameters
8.1.	On demand key supply mode messages and parameters
8.1.1.	Key request message
8.1.2.	Key request with identifier message
8.1.3.	Response to Key request message
8.2.	Proactive key supply mode messages and parameters
8.2.1.	Session creation request message
8.2.2.	Response to session creation request message
8.2.3.	Session creation notification message
8.2.4.	Response to session creation notification message
8.2.5.	Key request with session identifier message
8.2.6.	Response to Key request with session identifier message
8.2.7.	Proactive key supply message
8.2.8.	Response to proactive key supply message
9.	Security considerations
Annex I	Protocol implementation using Transmission Control Protocol
Annex II	Protocol implementation for on-demand key supply mode using secure hypertext transfer protocol
II.1	Key request message
II.2	Key request with identifier message
II.3	Response to Key request message
References	