A.1 justification for proposed draft new ITU-T Y.QKD-TLS, “Quantum Key Distribution integration with Transport Layer Security 1.3”

Question:	Q16/13	**Proposed new ITU-T Recommendation**	Geneva, 23 Oct - 3 Nov 2023	
Reference and title:	ITU-T Y.QKD-TLS, “Quantum Key Distribution integration with Transport Layer Security 1.3”			
Base text:	TD412/WP3		**Timing:**	2024Q3
Editor(s):	Jeongyun Kim; ETRI; Taesang Choi, ETRI; Hyeongsoo Kim, KT;		**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Draft Recommendation specifies use cases, high-level requirements and reference models for quantum key distribution (QKD) integration with transport layer security 1.3 (TLS 1.3), the scope of this Recommendation is as follows:

- Overview of QKD integration with TLS 1.3.
- Use cases of QKD integration with TLS 1.3.
- High-level requirements of QKD integration with TLS 1.3.
- Reference models of QKD integration with TLS 1.3.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

This Draft Recommendation specifies use cases, high-level requirements and reference models for quantum key distribution (QKD) integration with transport layer security 1.3 (TLS 1.3).

Relations to ITU-T Recommendations or to other standards (approved or under development)**:**

ITU-T TR-QKDN-nq “ITU-T’s Views for Quantum-Enabled Future Networks”

Technical Report ITU-T FG QIT4N D2.2 “Quantum information technology for networks use cases: Quantum key distribution network.”

ITU-T TR-XSTR-HYB-QKD “Overview of hybrid approaches for key exchange with quantum key distribution”

IETF RFC8446 "The Transport Layer Security (TLS) Protocol Version 1.3".

Liaisons with other study groups or with other standards bodies:

ITU-T SG11, SG17, ETSI ISG-QKD, IETF, IRTF

Supporting members that are committing to contributing actively to the work item:

Korea (Rep. of), ETRI, KT corp., KAIST, and Korea Univ.

Attachment 2

Draft new Recommendation ITU-T Y.QKD-TLS

Quantum Key Distribution integration with Transport Layer Security 1.3

Summary

This Draft Recommendation specifies use cases, high-level requirements and reference models for quantum key distribution (QKD) integration with transport layer security 1.3 (TLS 1.3).

Keywords

Framework, QKDN, TLS 1.3, integration.

Table of Contents

Draft new Recommendation ITU-T Y.QKD-TLS

Quantum Key Distribution integration with Transport Layer Security 1.3

1 Scope

This Draft Recommendation specifies use cases, high-level requirements and reference models for quantum key distribution (QKD) integration with transport layer security 1.3 (TLS 1.3), the scope of this Recommendation is as follows:

- Overview of QKD integration with TLS 1.3.
- Use cases of QKD integration with TLS 1.3.
- High-level requirements of QKD integration with TLS 1.3.
- Reference models of QKD integration with TLS 1.3.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3800] Recommendation ITU-T Y.3802 (2020), *Overview on networks supporting quantum key distribution.*

[ITU-T TR.QKDN-nq] Draft Technical Report ITU-T TR.QKDN-nq (202x), *Overview for integration of quantum key distribution network with non-quantum cryptographies*.

[ITU-T TR FG QIT4N D2.2] Technical Report ITU-T FG QIT4N D2.2 (2021), *Quantum information technology for networks use cases: Quantum key distribution network.*

[IETF RFC8446] Rescorla, E., *"The Transport Layer Security (TLS) Protocol Version 1.3", RFC8446, August 2018.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

TBD

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

TLS Transport Layer Security

5 Conventions

None.

6 Overview

The quantum key distribution network (QKDN) is expected to be able to provide optimized support for a variety of different quantum key distribution (QKD) services. It is assumed that the coverage of the QKD service is limited since it is delivered between network equipment such as OTN rather than between end-devices for example smart phone and servers.

One of the challenges of the QKDN is to support end-to-end the QKD service and integrating QKD with TLS is one of solutions for this.

In this regard, several issues are identified as follows;

- Whether QKD extension is necessary to integrate with TLS 1.3
- How to integrate QKD with TLS 1.3 (e.g., pre-shared key encryption)

[Editor's note] If any TLS extension is necessary for integration QKD-TLS, the scope of TLS extension would be identified from Q16/13 perspective. IETF would decide whether TLS extension will be done or not.

First use cases of QKD-TLS integration are derived and then high-level requirements of QKD-TLS integration are described based on the use cases. The reference models of QKD-TLS integration are specified in order to resolve the issues.

7 Use cases of QKD-TLS integration

Figure 1 shows the QKDN's relation to end-to-end cryptography service. The end-to-end encryption can be realized between the cryptographic applications in the user network by applying QKDN or applying the integration of QKDN and non-quantum cryptographies.

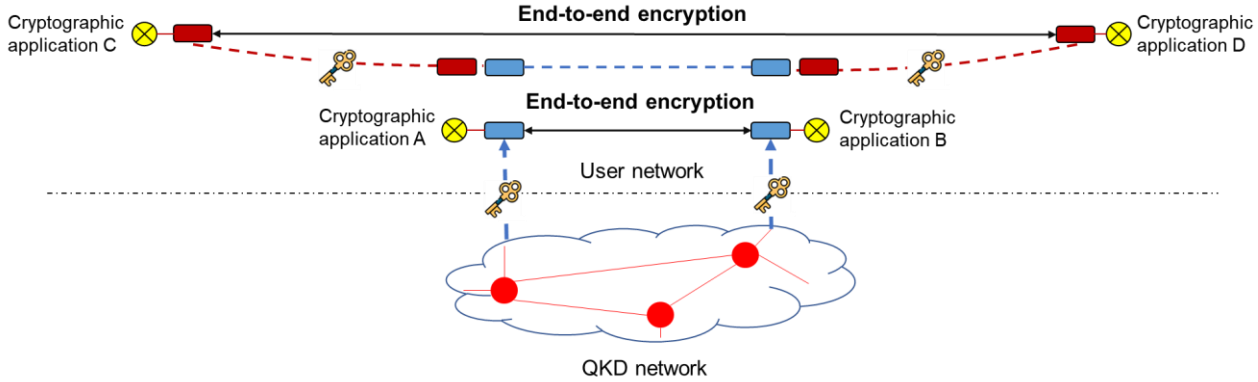

Figure 1. QKDN's relation to end-to-end cryptography service

Furthermore, in a use case of E2E QKD-encrypted model, KSA-keys are delivered to TLS 1.3 (Transport Layer Security 1.3) client and server symmetrically. TLS communication between client and server can be encrypted and decrypted thorough the keys. Therefore, a public-key exchange procedure may not be required, during the initiation process, so called TLS handshake.

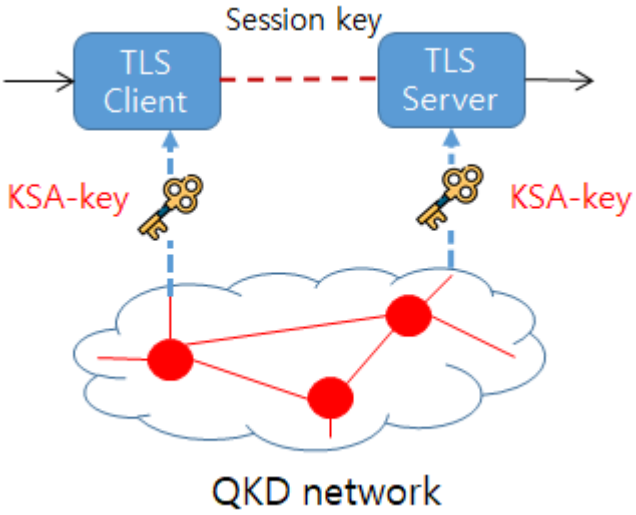

Figure 2. Use case of integration between QKDN and TLS protocol

It is assumed that TLS client/server and QKD module/key manger are located in the same trusted node together. Based on this assumption, the delivery connectivity from QKDN to TLS functions is considered to be IT-secured.

If the TSL client/server and QKD module/Key Manager are not located in the same Trusted Node together, the connectivity from QKD network to TLS functions should be secured. For example, it is required to apply PKI cryptography with PQC algorithm against quantum computing attack.

The use cases are categorized into two; QKD and TLS are co-located in a trusted node and separately located.

8 High-level requirements of QKD-TLS integration

TBD

9 Reference models of QKD-TLS integration

TBD

10 Security considerations

TBD

Bibliography

[b-ITU-T TR-XSTR-HYB-QKD] ITU-T Technical Report “Overview of hybrid approaches for key exchange with quantum key distribution” May 2022.

_____