Draft new Recommendation ITU-T Y.QKDN_BM

Quantum Key Distribution Networks - Business role-based models

Summary

Draft Recommendation ITU-T Y.QKDN_BM describes business roles, business role-based models, and service scenarios in Quantum Key Distribution Network (QKDN) from different deployment and operation perspectives with existing user networks for supporting secure communications in various application sectors.

This draft Recommendation can be used as a guideline for applying QKDN from business point of views as well as for deployment and operation of QKDN from telecom operators' point of views.

(TBD)

Keywords

QKDN, business roles, business role-based models, service scenarios.

Table of Contents

1 Scope 4
2 References 4
3 Definitions 4
3.1 Terms defined elsewhere 4
3.2 Terms defined in this Recommendation 5
4 Abbreviations and acronyms 5
5 Conventions 5
6 Business roles in QKDN for security application services 5
7 Business role-based models and service scenarios 8
8 Security Considerations 20
Annex A <Annex Title> 21
Appendix I Implementation description of QKDN business model 22
Bibliography 24
~~1 Scope ..... 5~~
~~2 References ..... 5~~
~~3 Definitions ..... 5~~
~~3.1 Terms defined elsewhere ..... 5~~
~~3.2 Terms defined in this Recommendation ..... 6~~
~~4 Abbreviations and acronyms ..... 6~~
~~5 Conventions ..... 6~~
~~6 Business roles in QKDN for security application services ..... 6~~
~~7 Business role-based models and service scenarios ..... 9~~
~~7.1 Business role-based models and service scenarios for secure communication in general ..... 9~~
~~7.2 Business role-based models and service scenarios for secure communication in financial sector ..... 11~~
~~7.3 Business role-based models and service scenarios for secure communication in telecom sector ..... 15~~
~~7.4 Business role-based models and service scenarios for secure communication in power sector ..... 15~~

~~8 Security Considerations ..... 16~~

~~Annex A <Annex Title> ..... 17~~

~~Appendix I <Appendix Title> ..... 18~~

~~Bibliography ..... 19~~

Draft new Recommendation ITU-T Y.QKDN_BM

Quantum Key Distribution Networks - Business role-based models

1 Scope

This draft Recommendation describes business roles, business role-based models, and service scenarios in Quantum Key Distribution Network (QKDN) from different deployment and operation perspectives. Especially, this draft Recommendation identifies various business models that require secure communications with QKDN and exiting user networks as follows:

– general QKDN applications;

– financial sector;

– healthcare sector;

– transportation sector;

– etc.

(Editors' Note: the above items should be changed by the contents of this draft Recommendation. TBD.)

This draft Recommendation can be used as a guideline for the specification of service scenarios that utilize QKDN from business point of views as well as for deployment and operation of QKDN from telecom operators' point of views.

NOTE – This draft Recommendation does not identify, in an exhaustive manner, all business roles, business role-based models, and service scenarios of QKDN.

(TBD)

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.3800 (2019), *Overview on Networks supporting Quantum Key Distribution*

(TBD)

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 quantum key distribution (QKD) [b-ETSI GS QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.2 quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links and optionally KM links for sharing and/or relaying keys between QKD nodes.

3.1.3 user network [ITU-T Y.3800]**:** A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

3.1.4 Business role [ITU-T X.1257]: A collection of tasks (with or without permissions) that a user can be entitled to perform.

3.1.5 key manager (KM) [ITU-T Y.3800]**:** A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.6 service level agreement [ITU-T Y.1401]: A negotiated agreement between an end user and the service provider. Its significance varies depending on the service offerings. The service level agreement (SLA) may include a number of attributes such as, but not limited to, traffic contract, availability, performance, encryption, authentication, pricing and billing mechanism, etc.

(TBD)

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 <Term 3>: <definition>.

(TBD)

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

<abbr>	<expansion>
KM	Key Manager
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
SLA	Service Level Agreement

(TBD)

5 Conventions

(TBD)

6 Business roles in QKDN for security application services

(Editors' Note: The alignment issue between business interfaces in this document and other interfaces in other architecture documents will be discussed later.)

Players are involved in security application service related business activities with QKDN environment. Each player plays at least one business role. In some cases, however, one player can play more than one business role at the same time. The identified security application service related business roles are shown in Figure 6-1, and the business interfaces are described in Table 6-1.

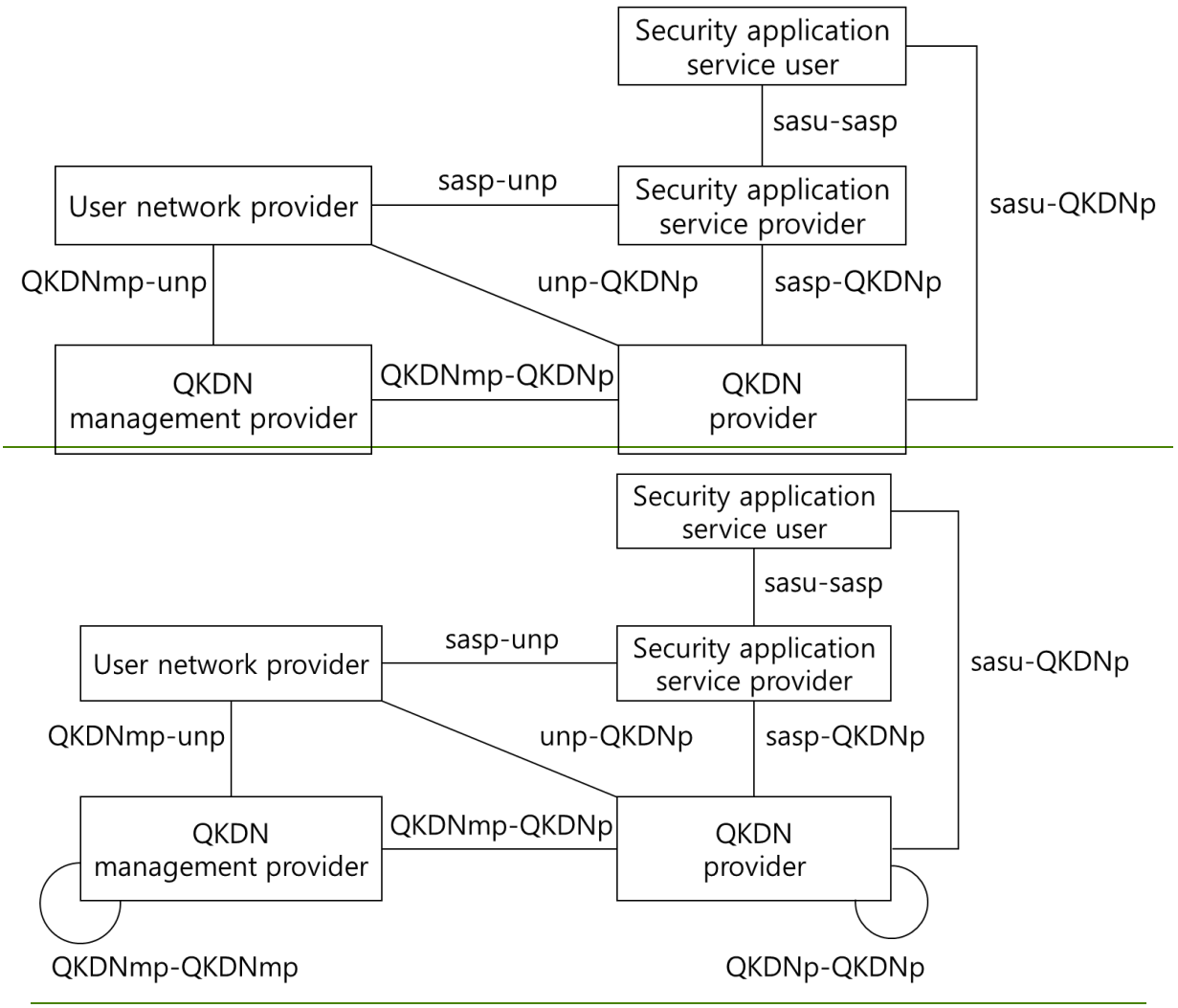


Figure 6-1 – The owners of business roles in QKDN

6.1.1 security application service user

The security application service user uses the application(s) provided by the security application service provider.

6.1.2 security application service provider

The security application service provider is the consumer of the keys provided by QKDN key managers (KM). Furthermore, the security application service provider is responsible for providing secure services to security application service users. These services are running on network services provided by the user network provider.

6.1.3 QKDN provider

The QKDN provider provides key distribution including managing lifecycle of keys and providing these keys.

6.1.4 QKDN management provider

The QKDN management provider is responsible to manage QKDN resources.

6.1.5 User network provider

The user network provider is the owner of the user network.

Table 6-1 – Business interfaces for QKDN

Business interface	Business roles	Interactions via the business interface
sasu-sasp	Security application service user and security application service provider	The security application service user interacts with the security application service provider to protect its data using security application based on corresponding service level agreements, providing corresponding payment when necessary.
sasp-QKDNp	Security application service provider and QKDN provider	The security application service provider interacts with the QKDN provider to consume keys for performing security services based on corresponding service level agreements, providing corresponding payment when necessary.
QKDNmp-QKDNp	QKDN management provider and QKDN provider	The QKDN management provider interacts with the QKDN provider to monitor and manage QKDN infrastructures based on corresponding service level agreements, providing corresponding payment when necessary.
QKDNmp-unp	QKDN management provider and user network provider	The QKDN management provider interacts with the user network provider to orchestrate the consumption of quantum key based on corresponding service level agreements, providing corresponding payment when necessary.
sasp-unp	Security application service provider and user network provider	The security application service provider interacts with the user network provider to access user network for exchanging secure messages based on corresponding service level agreements, providing corresponding payment when necessary.
unp-QKDNp	User network provider and QKDN provider	The user network provider directly requests quantum key for its own purpose (e.g., enhancing network level security, etc.) based on corresponding service level agreements, providing corresponding payment when necessary.

sasu-QKDNp	Security application service user and QKDN provider	The security application service user directly requests quantum key for satisfying its security requirements based on corresponding service level agreements, providing corresponding payment when necessary.
QKDNmp-QKDNmp	QKDN management providers	QKDN management providers exchange information for jointly managing QKDN such as quantum, key, and control layer management, including FCAPS, QoS, pricing, etc.
QKDNp-QKDNp	QKDN providers	QKDN providers exchange information for properly handling quantum keys.

NOTE – A service level agreement can also be established between the providers.

(Editors' Note: Table should be modified considering the content of SLA definition, such as availability, performance/QoS, pricing, etc. Further contributions are invited.)

7 Business role-based models and service scenarios

7.1 Model 1

In this model, there is one player in addition to the security application service user.

Player A plays four roles: Security application service provider, User network provider, QKDN provider, and QKDN management provider.

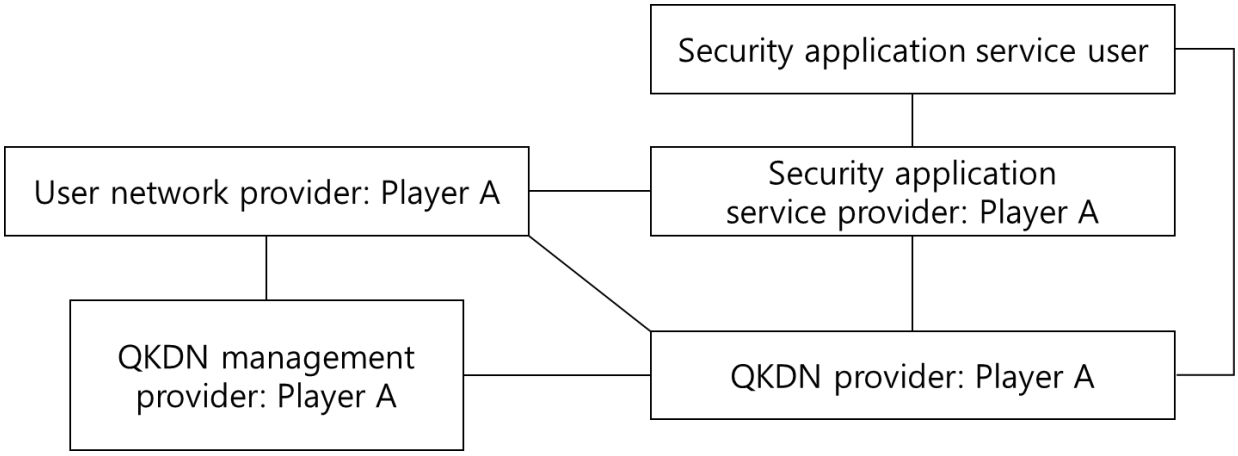


Figure 7-1 – Model 1 for QKDN based security application services

1) Service scenario 1 for model 1

Player A is a security application service provider. The player A also provides a telecom network service as well as a QKDN infrastructure providing quantum key management and distribution. In this use case, player A provides a security application service to users by using quantum key cryptography provided by the same player. The quantum key is transferred through a QKDN of player

A provided by the same player. Data for the security application service are transferred through telecommunication network which is also provided by player A.

(TBD)

7.2 Model 2

In this model, there are two players in addition to the security application service user.

Player A plays the role of security application service provider.

Player B plays three roles: User network provider, QKDN provider, and QKDN management provider.

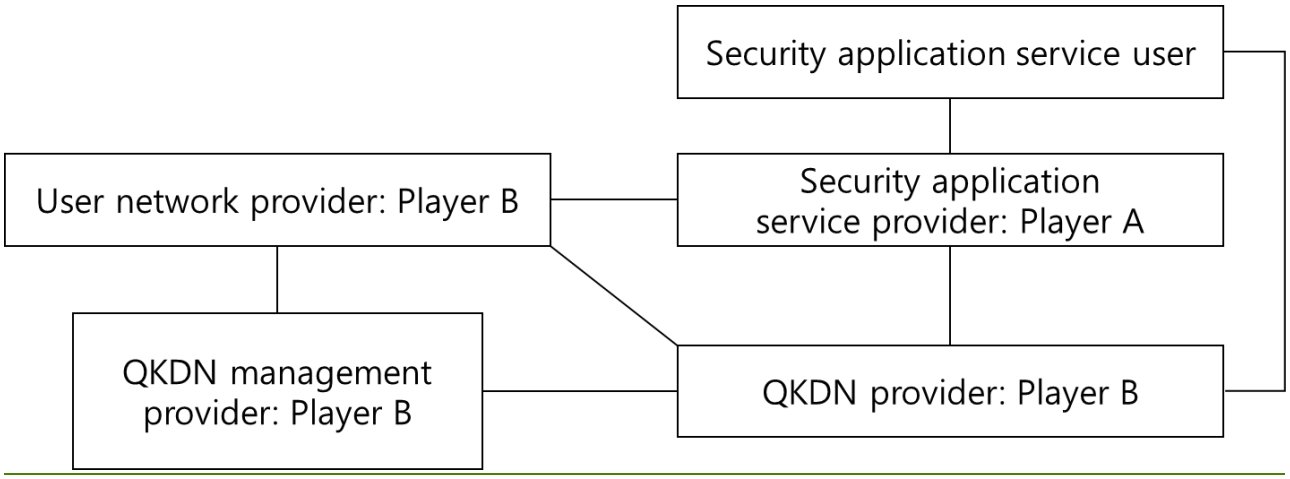


Figure 7-2 – Model 2 for QKDN based security application services

1) Service scenario 1 for model 2

Player A is a security application service provider. Player B is a telecom network operator and a QKDN infrastructure company that provides quantum key management and distribution. In this use case, player A provides a security application service to users by using quantum key cryptography provided by the player B. The quantum key is transferred through a QKDN of player B provided by the same player Data for the security application service are transferred through telecommunication network which is also provided by player B.

(TBD)

7.3 Model 3

In this model, there are three players in addition to the security application service user.

Player A plays the role of security application service provider.

Player B plays the role of user network provider.

Player C plays two roles: QKDN provider and QKDN management provider.

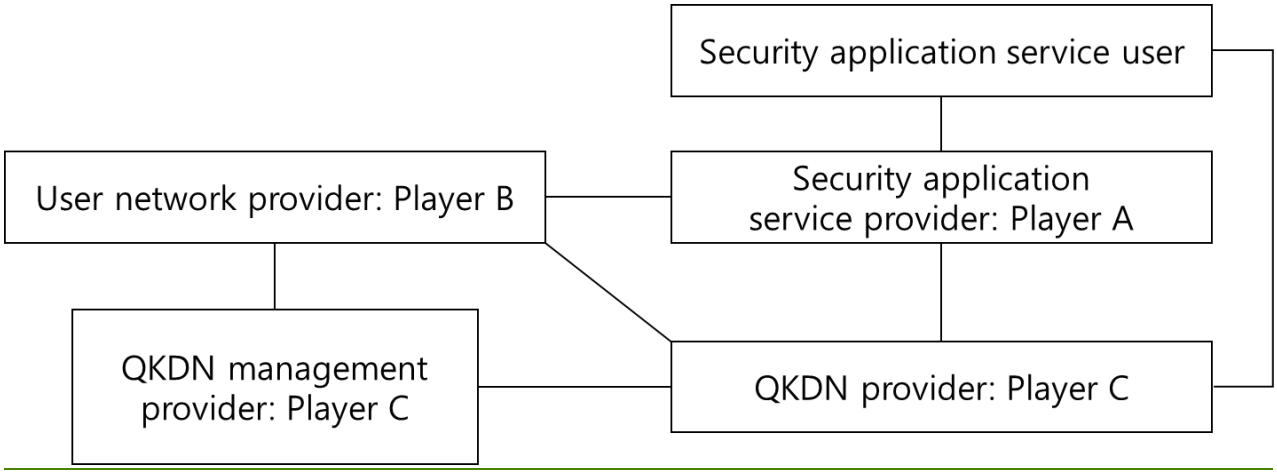


Figure 7-3 – Model 3 for QKDN based security application services

1) Service scenario 1 for model 3

Player A is a security application service provider. Player B is a telecom network operator. Player C is QKDN infrastructure company that provides quantum key management and distribution. In this use case, player A provides a security application service to users by using quantum key cryptography provided by the player C through telecommunication network provided by player B.

(TBD)

7.4 Model 4

In this model, there are four players in addition to the security application service user.

Player A plays the role of security application service provider.

Player B plays the role of user network provider.

Player C plays two roles: QKDN provider and QKDN management provider.

Player D plays the role of QKDN provider.

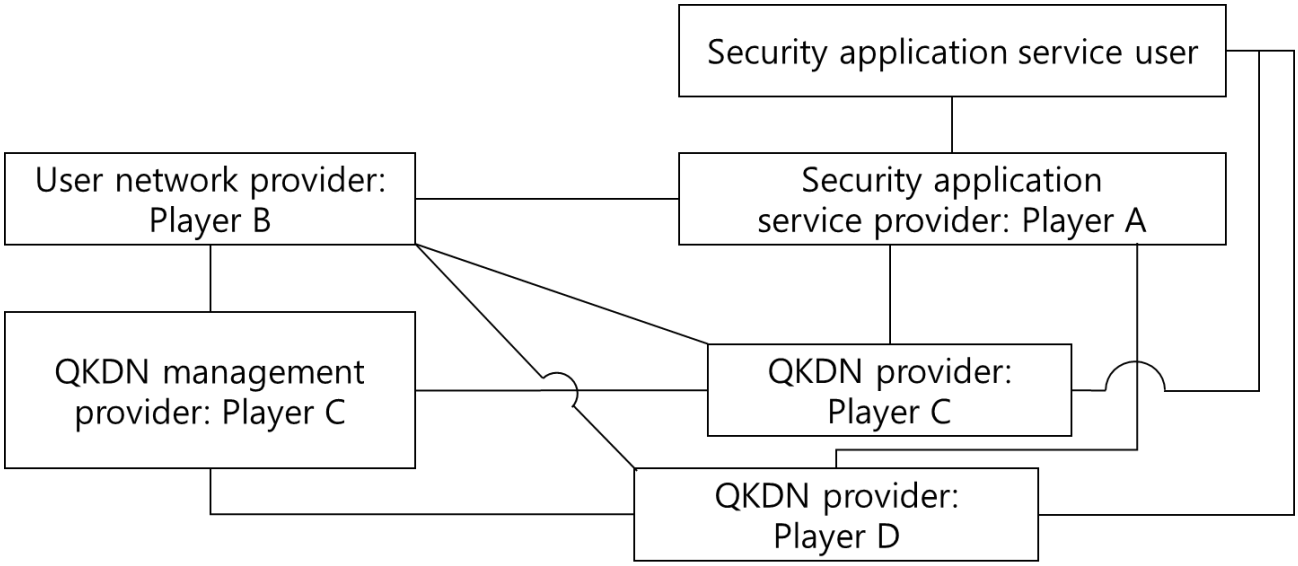


Figure 7-4 – Model 4 for QKDN based security application services

1) Service scenario 1 for Model 4

Player A is a security application service provider. Player B is a telecom network operator. Player C and player D are QKDN infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a security application service to users by using quantum key cryptography provided by the player C. The quantum key is transferred through a QKDN of player C to that of player D. Data for the security application service are transferred through telecommunication network provided by player B.

(TBD)

7.5 Model 5

In this model, there are five players in addition to the security application service user.

Player A plays the role of security application service provider.

Player B plays the role of user network provider.

Player C plays the role of QKDN management provider.

Player D plays the role of QKDN provider.

Player E plays the role of QKDN provider.

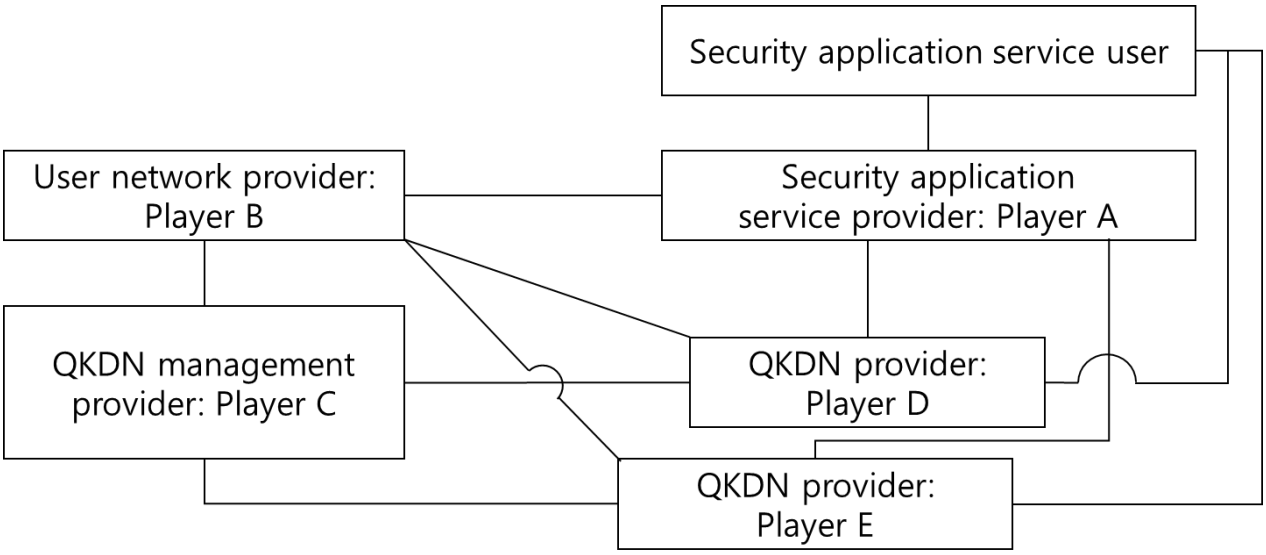


Figure 7-5 – Model 5 for QKDN based security application services

1) Service scenario 1 for Model 5

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C, player D and player E are QKDN infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a cross-domain secure communication service to users (i.e., the SC application user) by using quantum key cryptography provided by the player C. Player C negotiates between player D and player E so that the quantum key is transmitted from the QKDN of player D to the QKDN of player E. Data encrypted messages are transferred through telecommunication network provided by player B.

2) Service scenario 2 for Model 5

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C is the QKDN infrastructure company that provides quantum key management and distribution. Users 1, 2, ..., n is financial application users containing different service requirement attributes, such as service mode (i.e., periodic, long-term, ...), service levels (i.e., high traffic demand, low traffic demand, ...), etc. In this use case, when the service requests come, player A divides users1, ..., n into multiple services according to the users' service requirement attributes, and then provides secure communication services to users (i.e. financial application users) by using the quantum key password provided by player C. Player C controls the quantum key supply to the financial application users according to different service attributes. Data encrypted messages are transferred through telecommunication network provided by player B.

(TBD)

7.6 Consideration points for applying QKDN to industrial sectors

Industrial sectors	Consideration points
Financial	The communication in financial sector involves the financial transactions of corporate and individual users, which have extreme high security requirements, so it is necessary to use QKD to ensure secure communication in the financial sector. In the process of providing keys to the financial sector, good response measures should be taken to deal with real-time unexpected services.
Telecommunication	The communication in telecom sector involves the communications of corporate and individual users, which has extreme high privacy requirements, so it is necessary to use QKD to ensure secure communication in the telecom sector. The telecom sector has a wide range and types of businesses, high demands of quantum key and multi-service in this sector should be taken seriously.
Power	The communication in power sector applies the corporate private network, which is dedicated to provide information interaction control for the national power infrastructure. It has extreme high security requirements. Thus, it is necessary to use QKD to ensure secure communication in power sector. Besides, achieving high reliability and low latency requirements is also needed, the issue of survivability in power sector needs to be taken seriously.

(TBD)

~~7 Business role-based models and service scenarios~~

~~*(Editors' Note: this clause identifies models with business roles (in clause 6) and describes possible service scenarios under various situations.)*~~

(Editors' Note: Specific characteristics for each sector should be described and identified.)

(Editors' Note: One possible approach: General security application service scenarios can be identified, and then sector specific descriptions can be followed such as table, etc.)

7.1 Business role-based models and service scenarios for secure communication in general

7.1.1 Model 1 for general secure communication

In this model, there are three players in addition to the SC application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays two roles: QKD network provider, QKDN management provider.

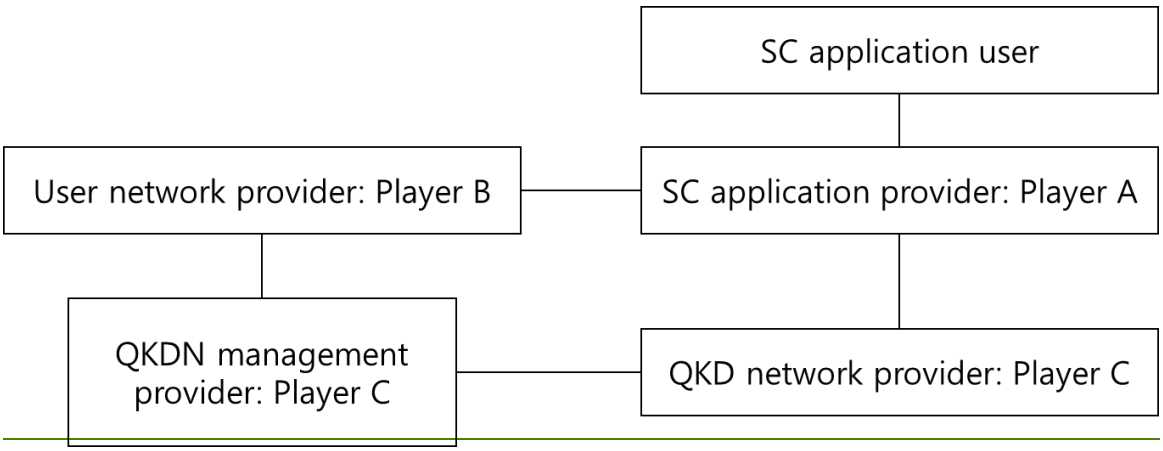


Figure 7-1 – Model 1 for secure communication

7.1.1.1 Service scenario 1 for model 1

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C is QKD network infrastructure company that provides quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the SC application user) by using quantum key cryptography provided by the player C through telecommunication network provided by player B.

7.1.2 Model 2 for secure communication in general

In this model, there are four players in addition to the SC application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays two roles: QKD network provider, QKDN management provider.

Player D plays the role of QKD network provider.

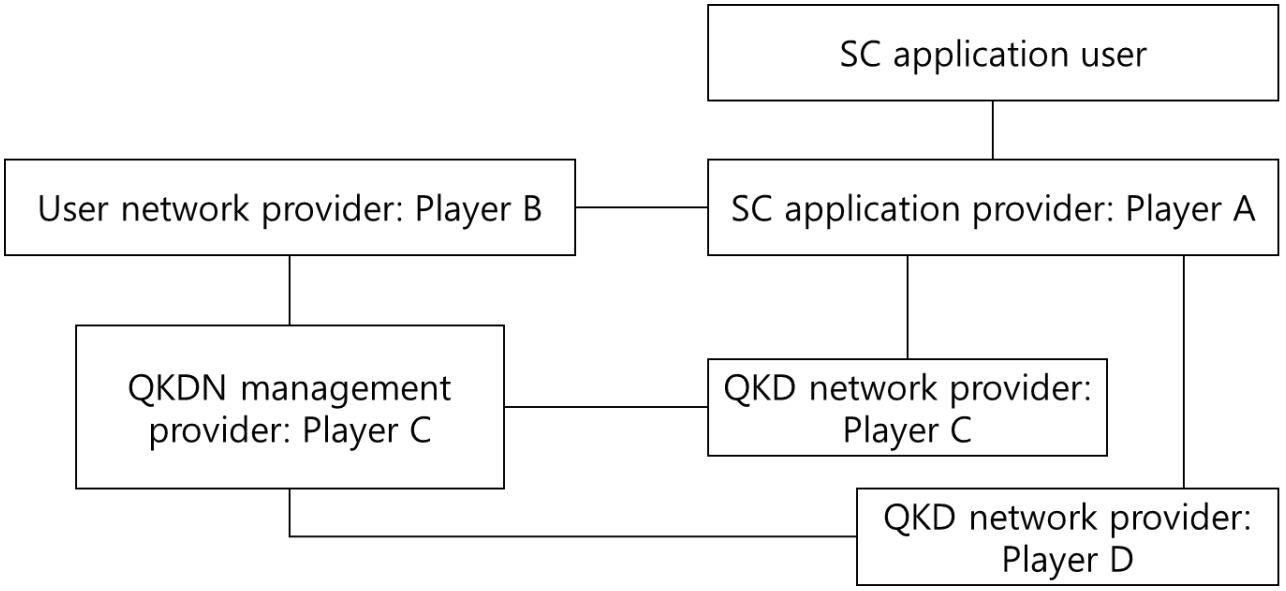


Figure 7-2 – Model 2 for secure communication

7.1.2.1 Service scenario 1 for Model 2

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C and player D are QKD network infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the SC application user) by using quantum key cryptography provided by the player C. The quantum key is transferred through a QKD network of player C to that of player D. Data encrypted messages are transferred through telecommunication network provided by player B.

7.1.3 Model 3 for general secure communication

In this model, there are five players in addition to the SC application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays the role of QKDN management provider.

Player D plays the role of QKD network provider.

Player E plays the role of QKD network provider.

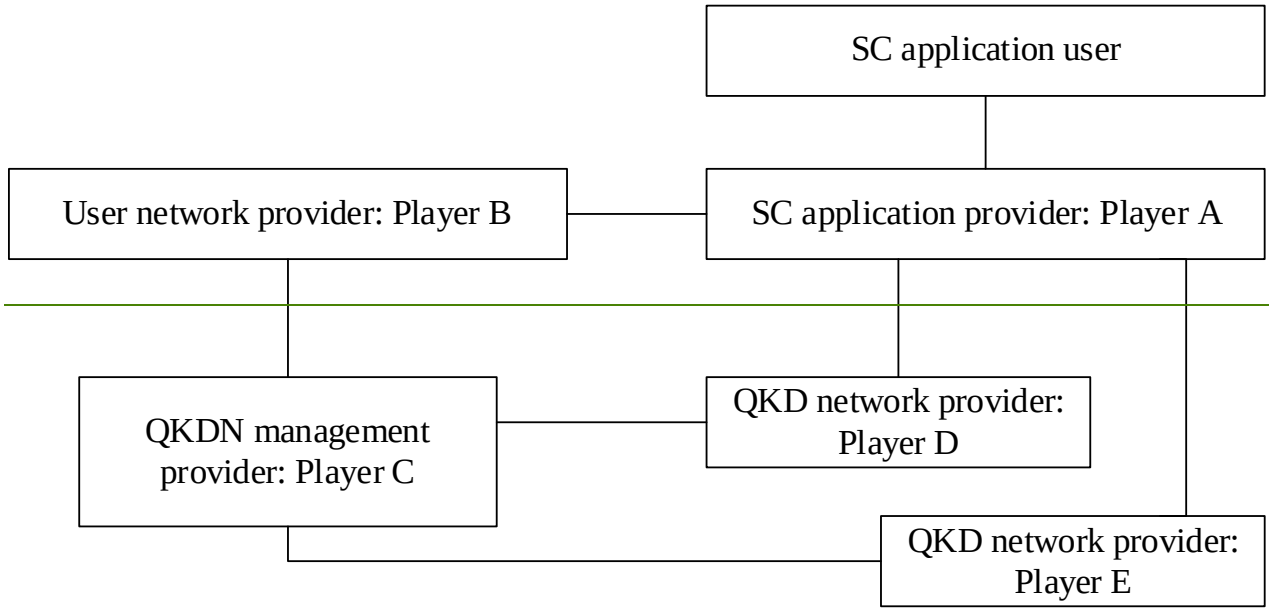


Figure 7-3 – Model 3 for secure communication

7.1.3.1 Service scenario 1 for Model 3

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C, player D and player E are QKD network infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a cross-domain secure communication service to users (i.e., the SC application user) by using quantum key cryptography provided by the player C. Player C negotiates between player D and player E so that the quantum key is transmitted from the QKD network of player D to the QKD network of player E. Data encrypted messages are transferred through telecommunication network provided by player B.

(TBD)

7.2 Business role-based models and service scenarios for secure communication in financial sector

7.2.1 Model 1 for secure communication in financial sector

In this model, there are three players in addition to the financial application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays two roles: QKD network provider, QKDN management provider.

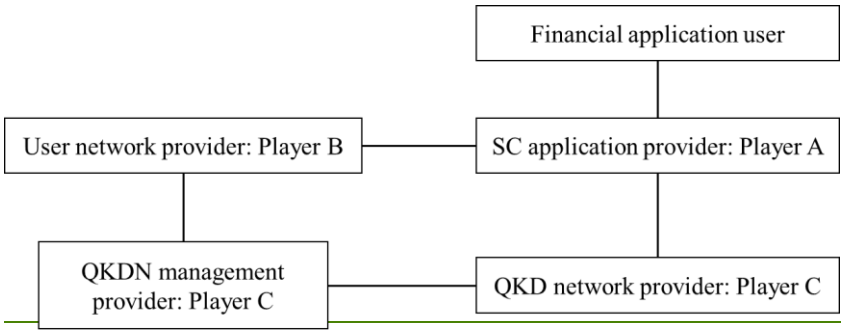


Figure 7-4 – Model 1 for secure communication in Financial sector

7.2.1.1 Service scenario 1 for model 1

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C is QKD network infrastructure company that provides quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the Financial application user) by using quantum key cryptography provided by the player C through telecommunication network provided by player B.

7.2.2 Model 2 for secure communication in financial sector

In this model, there are four players in addition to the financial application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays two roles: QKD network provider, QKDN management provider.

Player D plays the role of QKD network provider.

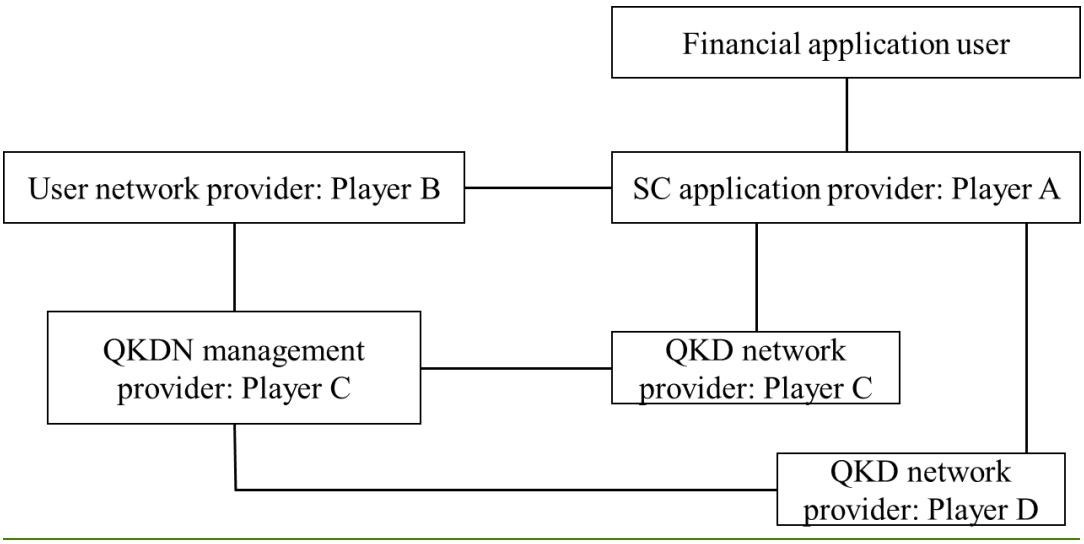


Figure 7-5 – Model 2 for secure communication in financial sector

7.2.2.1 Service scenario 1 for Model 2

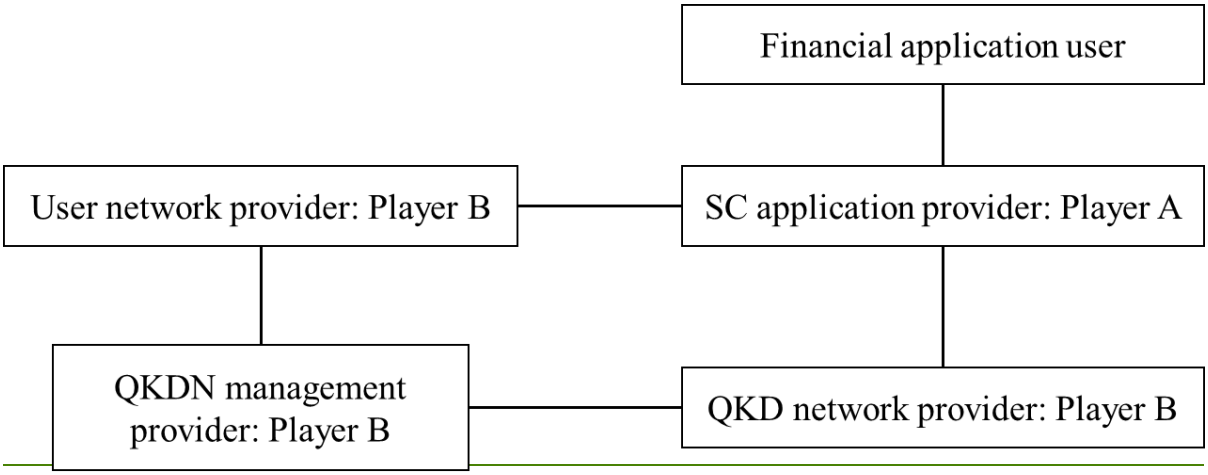
Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C and player D are QKD network infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the Financial application user) by using quantum key cryptography provided by the player C. The quantum key is transferred through a QKD network of player C to that of player D. Data encrypted messages are transferred through telecommunication network provided by player B.

7.2.3 Model 3 for secure communication in financial sector

In this model, there are two players in addition to the financial application user.

~~Player A plays the role of SC application provider.~~

~~Player B plays three roles: User network provider, QKD network provider, QKDN management provider.~~



~~Figure 7-6 – Model 3 for secure communication in Financial sector~~

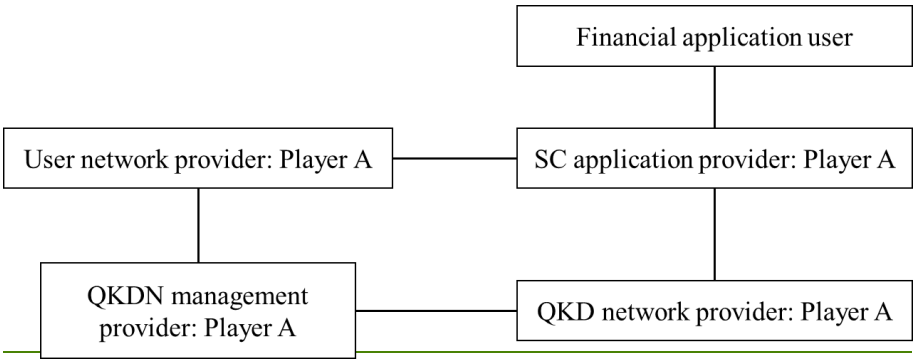
~~7.2.3.1 Service scenario 1 for model 3~~

~~Player A is an application provider with secure communication functionality. Player B is a telecom network operator and a QKD network infrastructure company that provides quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the Financial application user) by using quantum key cryptography provided by the player B. The quantum key is transferred through a QKD network of player B provided by the same player. Data encrypted messages are transferred through telecommunication network which is also provided by player B.~~

~~7.2.4 Model 4 for secure communication in financial sector~~

~~In this model, there are two players in addition to the financial application user.~~

~~Player A plays four roles: SC application provider, User network provider, QKD network provider, QKDN management provider.~~



~~Figure 7-7 – Model 4 for secure communication in Financial sector~~

~~7.2.4.1 Service scenario 1 for model 4~~

Player A is an application provider with secure communication functionality, also providing a telecom network service as well as a QKD network infrastructure providing quantum key management and distribution. In this use case, player A provides a secure communication service to users (i.e., the Financial application user) by using quantum key cryptography provided by the same player. The quantum key is transferred through a QKD network of player A provided by the same player. Data encrypted messages are transferred through telecommunication network which is also provided by player A.

7.2.5 Model 5 for secure communication in financial sector

In this model, there are five players in addition to the financial application user.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays the role of QKDN management provider.

Player D plays the role of QKD network provider.

Player E plays the role of QKD network provider.

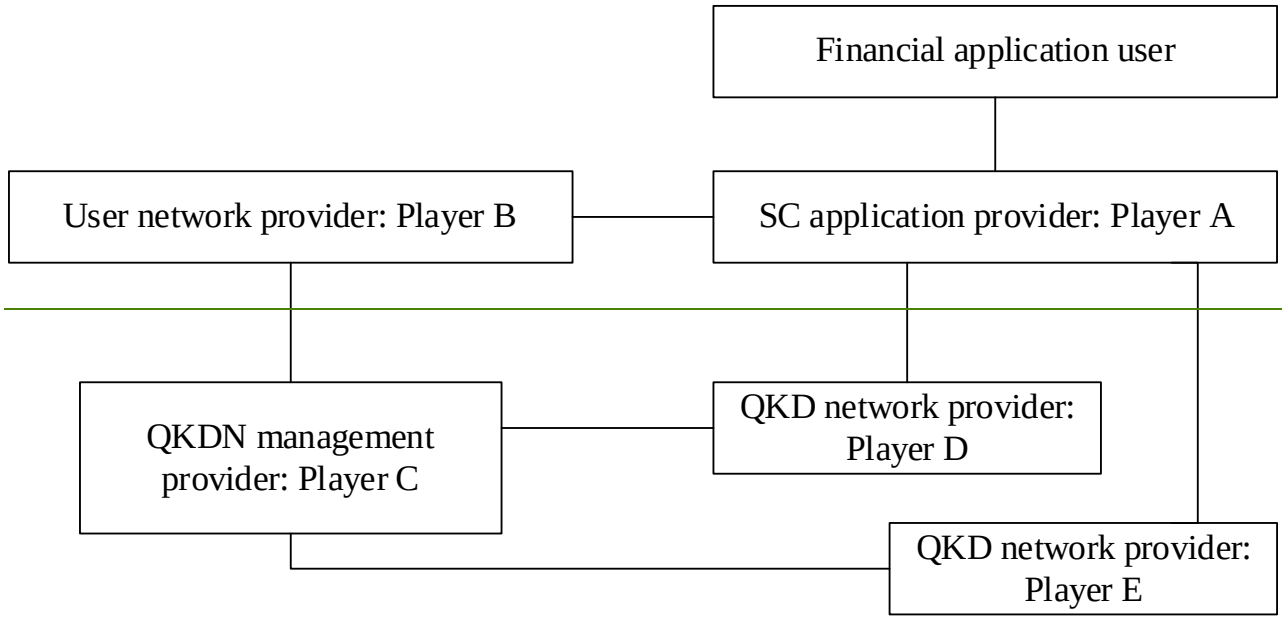


Figure 7-8 – Model 5 for secure communication in financial sector

7.2.5.1 Service scenario 1 for Model 5

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C, player D and player E are QKD network infrastructure companies that provide quantum key management and distribution. In this use case, player A provides a cross-domain secure communication service to users (i.e., the Financial application user) by using quantum key cryptography provided by the player C. Player C negotiates between player D and player E so that the quantum key is transmitted from the QKD network of player D to the QKD network of player E. Data encrypted messages are transferred through telecommunication network provided by player B.

7.2.6 Model 6 for secure communication in financial sector

In this model, there are several financial application users and several players.

Player A plays the role of SC application provider.

Player B plays the role of user network provider.

Player C plays the role of QKDN management provider.

Player D_1, D_2, ⋯D_i, ⋯, D_k plays the role of QKD network provider.

User 1, 2,⋯, n play the role of financial application users.

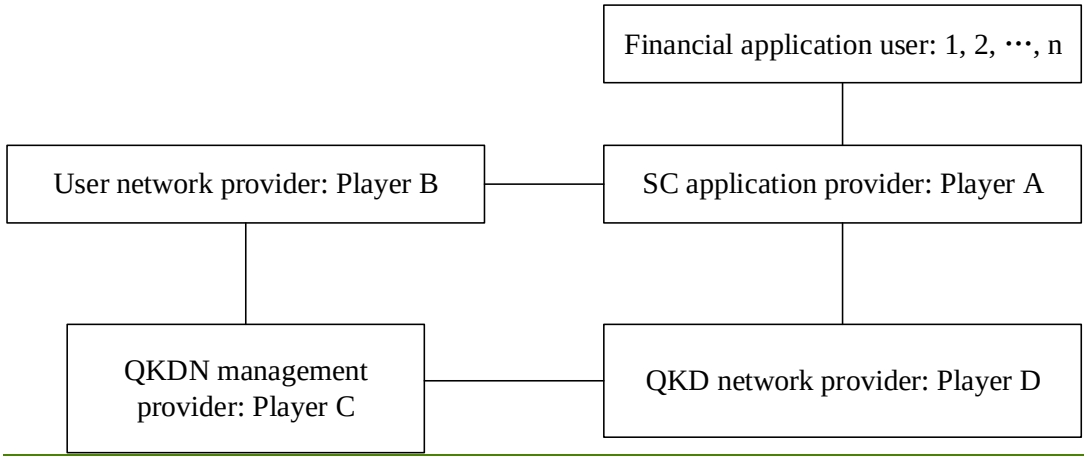


Figure 7-9 – Model 6 for secure communication in financial sector

7.2.6.1 Service scenario 1 for Model 6

Player A is an application provider with secure communication functionality. Player B is a telecom network operator. Player C is the QKD network infrastructure company that provides quantum key management and distribution. Users 1, 2, ..., n is financial application users containing different service requirement attributes, such as service mode (i.e., periodic, long-term, ...), service levels (i.e., high traffic demand, low traffic demand, ...), etc. In this use case, when the service requests come, player A divides users1, ..., n into multiple services according to the users' service requirement attributes, and then provides secure communication services to users (i.e. financial application users) by using the quantum key password provided by player C. Player C controls the quantum key supply to the financial application users according to different service attributes. Data encrypted messages are transferred through telecommunication network provided by player B.

7.3 Business role-based models and service scenarios for secure communication in telecom sector

(*TBD*)

7.4 Business role-based models and service scenarios for secure communication in power sector

(*TBD*)

8 Security Considerations

(TBD)

Annex A

<Annex Title>

(This annex forms an integral part of this Recommendation.)

<Body of annex A>

Appendix I

~~<Appendix Title>~~Implementation description of QKDN business model

(This appendix does not form an integral part of this Recommendation.)

~~<Body of appendix I>~~

This appendix is used to illustrate the engineering implementation of the QKDN business role architecture diagram.

I.1 Introduction

It is important to clarify the relationship between the QKDN business model and the QKDN architecture and explain how the business model maps to the QKDN architecture.

I.2 Existing structure

– Layer structure defined in [ITU-T Y.3800]: quantum layer, key management layer, QKDN control layer, QKDN management layer, service layer, and user network management layer;
– Basic functions and links defined in [ITU-T Y.3800]: QKD module, key manager (KM), QKDN controller, and QKDN manager, QKD link, and KM link in the QKDN; cryptographic application, user network manager, and application link in the user network;

I.3 Mapping process

The mapping process is as shown in the figure I.1.

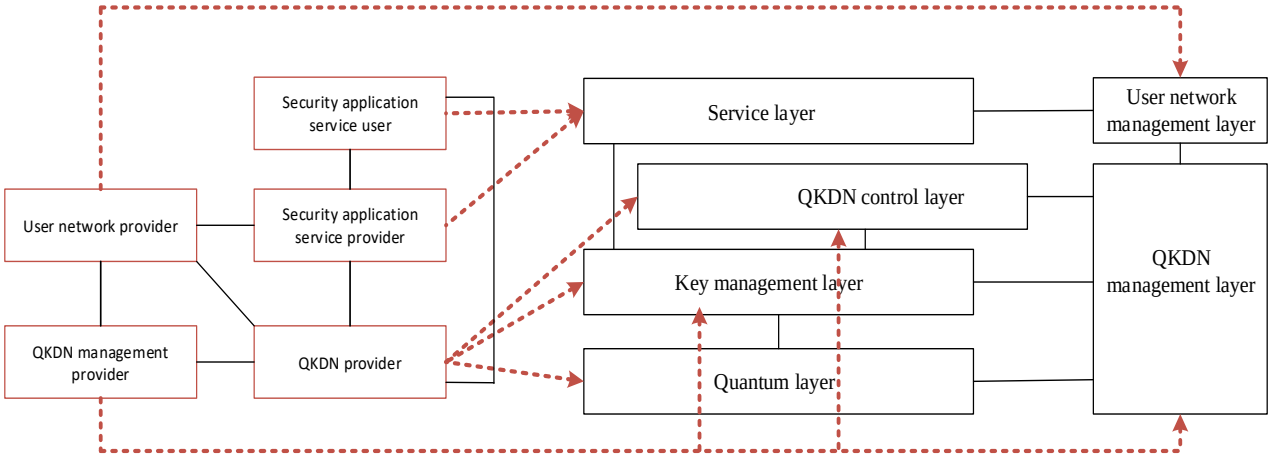


Figure I.1 mapping process

– **The security application service user** uses the application(s) provided by the security application service provider. The **security application service provider** is responsible for providing secure services to security application service users. In a **service layer**, the following functional element exists: cryptographic application function. It consumes the shared key pairs provided by a QKDN and perform secure communication between remote parties. So security application service user and security application service provider are mapped by service layer.
– The **user network provider** is the owner of the user network. In a **user network management layer**, there exists user network manager function: it performs FCAPS management features of

a user network. Therefore, the function of user network provider can be provided by user network management layer.

– The **QKDN management provider** is responsible to manage QKDN resources. In a **QKDN management layer**, a QKDN manager function is to manage fault, configuration, accounting, performance and security (FCAPS) aspects of a QKDN as a whole, and support user network management. In a **key management layer**, a KM function is to receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications. In a **QKDN control layer**, a QKDN controller function is to control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN. Therefore, QKDN management layer, key management layer and QKDN control layer can realize the function of QKDN management provider.

– The **QKDN provider** provides key distribution including managing lifecycle of keys and providing these keys. In a **quantum layer**, quantum key distribution keys (QKD-keys) are generated. In a **key management layer**, a KM function is to receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications. In a **QKDN control layer**, a QKDN controller function is to control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN. Therefore, the function of QKDN provider can be provided by quantum layer, key management layer and QKDN control layer.

Bibliography

(TBD)

_____