International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3809

(02/2022)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Quantum key distribution networks

A role-based model in quantum key distribution networks deployment

Recommendation ITU-T Y.3809

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3809

A role-based model in quantum key distribution networks deployment

Summary

Recommendation ITU-T Y.3809 describes roles, a role-based model and service scenarios in quantum key distribution networks (QKDN) from different deployment and operation perspectives within existing user networks for supporting security applications services.

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

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3809	2022-02-13	13	11.1002/1000/14866

Keywords

QKDN, role-based model, service scenarios.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Roles in QKDN for security application services	2
6.1	Security application service user	2
6.2	Security application service provider	2
6.3	QKDN provider	2
6.4	QKDN management provider	3
6.5	User network provider	3
6.6	International scenarios	3
7	Role-based models and service scenarios	4
7.1	Model 1	4
7.2	Model 2	5
7.3	Model 3	5
7.4	Model 4	6
7.5	Model 5	7
7.6	Model 6	8
7.7	Model 7	8
8	Security considerations	9
Appendix I – Implementation description of QKDN roles		10
I.1	Introduction	10
I.2	Existing structure	10
I.3	Mapping process	10
Bibliography		12

Recommendation ITU-T Y.3809

A role-based model in quantum key distribution networks deployment

1 Scope

This Recommendation describes roles, a role-based model, and service scenarios in quantum key distribution networks (QKDN) from different deployment and operation perspectives. This Recommendation identifies various models that require security application services with QKDN and exiting user networks.

This Recommendation can be used as a guideline for applying service scenarios that globally utilize QKDN from a role point of view as well as for deployment and operation of QKDN from a telecom operators' point of view in an international context.

This Recommendation does not identify, in an exhaustive manner, all roles, a role-based model and service scenarios of QKDN.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 quality of service (QoS) [b-ITU-T P.10]: The totality of characteristics of a telecommunications service that bear on its ability to satisfy the stated and implied needs of the user of the service (see [b-ITU-T E.800]).

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

3.1.4 quantum key distribution network (QKDN) [b-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.

3.1.5 service level agreement [b-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.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FCAPS Fault, Configuration, Accounting, Performance, and Security

ICT Information and Communication Technology

KM Key Manager

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QKDNmp Quantum Key Distribution Network Management Provider

QKDNp Quantum Key Distribution Network Provider

QoS Quality of Service

SASP Security Application Service Provider

SASU Security Application Service User

SLA Service Level Agreement

UNP User Network Provider

5 Conventions

None.

6 Roles in QKDN for security application services

Telecommunication operations, QKDN operators, or other relevant stakeholders in information and communication technology (ICT) environments can act as players in QKDN roles. Players are involved in security application service-related activities with the QKDN environment. Each player plays at least one role. However, in some cases, one player can play more than one role at the same time. The identified roles related to security application services are shown in Figure 6-1, and the interfaces are described in Table 6-1.

6.1 Security application service user

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

6.2 Security application service provider

The security application service provider is the consumer of the keys provided by the 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 (UNP).

6.3 QKDN provider

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

6.4 QKDN management provider

The QKDN management provider is responsible to manage QKDN resources.

6.5 User network provider

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

6.6 International scenarios

The deployment of the above roles in the scenarios that are described in clause 7 shall, in an international implementation, need to conform to national regulatory and legal frameworks in the country where they are deployed.

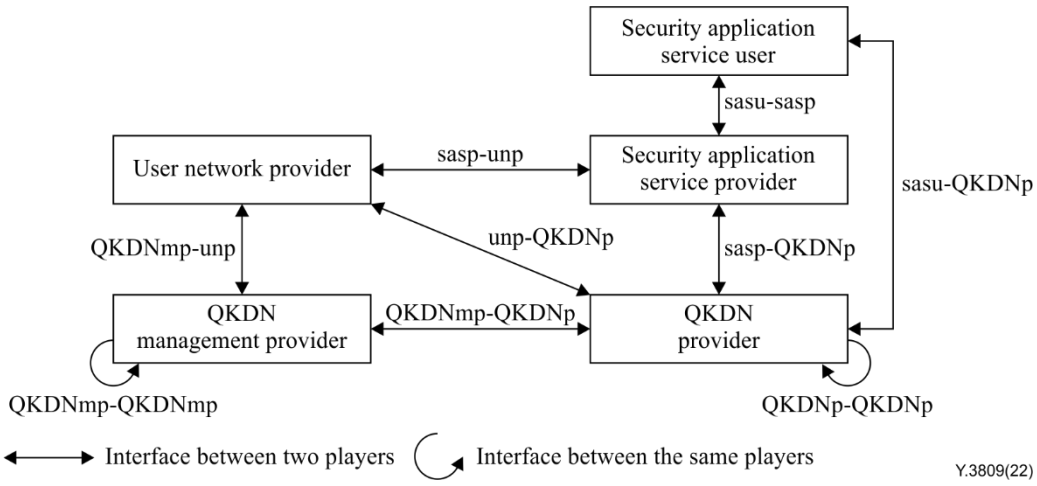

Figure 6-1 – The players of roles in QKDN deployment

Table 6-1 – Interfaces for roles in QKDN deployment

Interface	Roles	Interactions via the 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 the security application based on corresponding service level agreements (SLAs), providing corresponding payments 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 the corresponding SLAs, providing corresponding payments 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 requirements including quality of service (QoS), fault, configuration, accounting, performance, and security (FCAPS), pricing, etc.

Table 6-1 – Interfaces for roles in QKDN deployment

Interface	Roles	Interactions via the interface
QKDNmp-unp	QKDN management provider and user network provider	The QKDN management provider interacts with the user network provider to orchestrate the consumption of keys based on corresponding SLAs, providing corresponding payments 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 the user network for securely transferring data based on corresponding SLAs, providing corresponding payments when necessary.
unp-QKDNp	User network provider and QKDN provider	The user network provider directly requests keys for its own purpose (e.g., enhancing network level security, etc.) based on corresponding SLAs, providing corresponding payments when necessary.
sasu-QKDNp	Security application service user and QKDN provider	The security application service user directly requests keys for satisfying its security requirements based on corresponding SLAs, providing corresponding payments 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 the keys and information for properly handling the keys, including QoS, pricing, etc.

NOTE – An SLA can also be established between the providers.

7 Role-based models and service scenarios

Based on the roles identified in clause 6, this clause provides some service scenarios that utilize QKDN from a role point of view as well as for deployment and operation of QKDN from telecom operators' point of view.

This clause does not identify, in an exhaustive manner, all role-based models and service scenarios of a QKDN.

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.

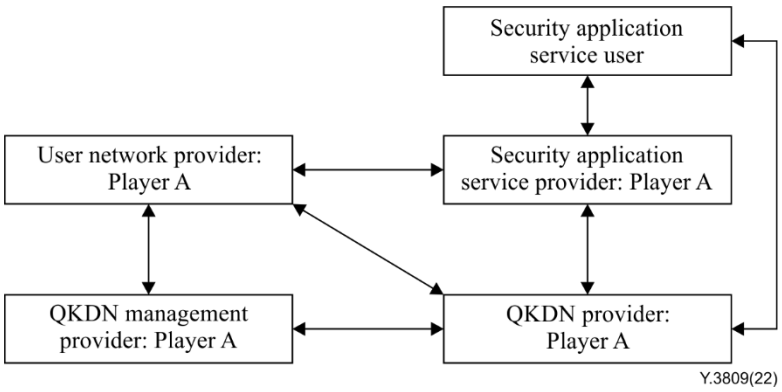

Figure 7-1 – Model 1 for QKDN based security application services

A service scenario for model 1

Player A is a security application service provider. Player A also provides a telecom network service as well as a QKDN infrastructure providing QKDN related key management and distribution. In this scenario, player A provides a security application service to the users (i.e., security application service users) by using the keys provided by the same player. The keys are transferred through a QKDN of player A provided by the same player. Data for the security application service are transferred through a telecommunication network which is also provided by player A.

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 a security application service provider.

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

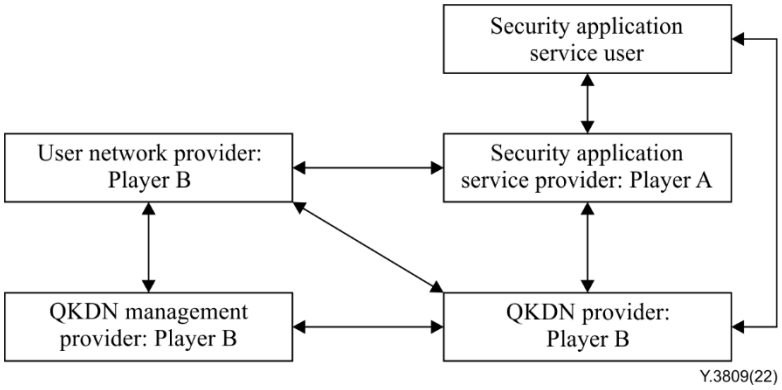

Figure 7-2 – Model 2 for QKDN based security application services

A service scenario 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 QKDN related key management and distribution. In this scenario, player A provides a security application service to the users (i.e., security application service users) by using keys provided by player B. The keys are transferred through a QKDN of player B provided by the same player. Data for the security application service is transferred through the telecommunication network which is also provided by player B.

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 a security application service provider.

Player B plays the role of a user network provider.

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

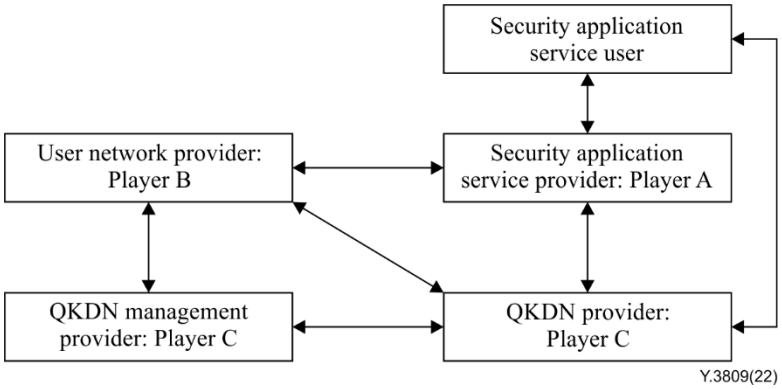

Figure 7-3 – Model 3 for QKDN based security application services

Service scenario 1 for model 3

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

Service scenario 2 for model 3

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

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 a security application service provider.

Player B plays the role of a user network provider.

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

Player D plays the role of a QKDN provider.

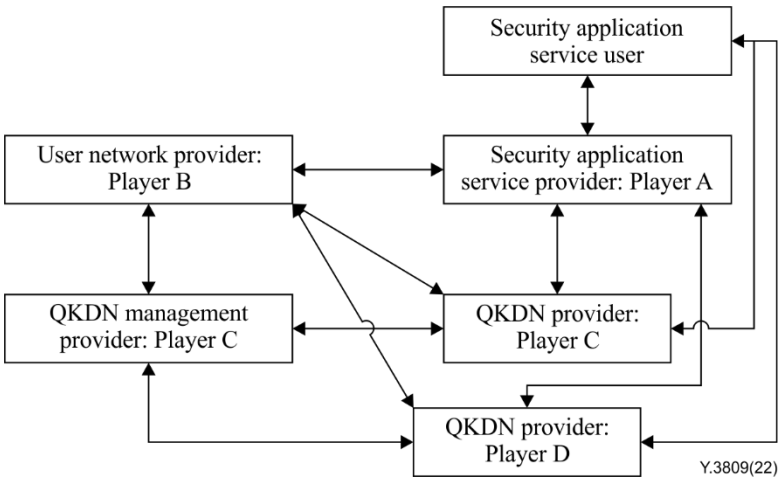

Figure 7-4 – Model 4 for QKDN based security application services

A service scenario 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 QKDN related key management and distribution. In this scenario, player A provides a security application service to the users (i.e., security application service users) by using keys provided by player C and player D. Player C interworks with player D so that the keys are transferred through a QKDN of player C and a QKDN of player D under the management of player C. Data for the security application service are transferred through the telecommunication network provided by player B.

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 a security application service provider.

Player B plays the role of a user network provider.

Player C plays the role of a QKDN management provider.

Player D plays the role of a QKDN provider.

Player E plays the role of a QKDN provider.

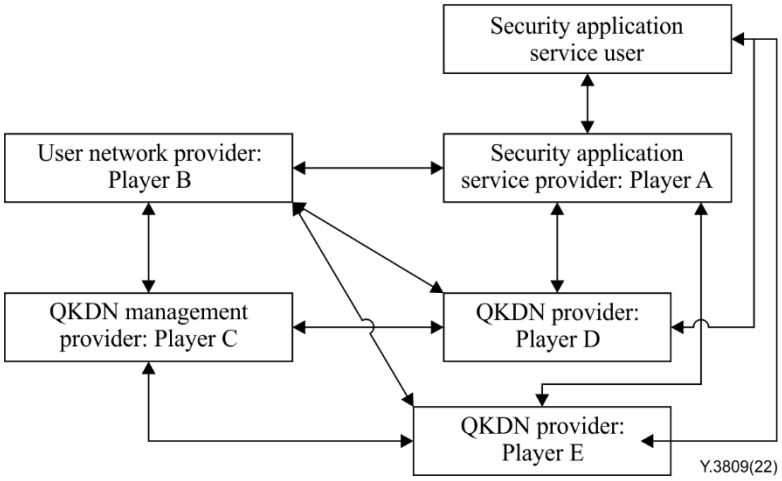

Figure 7-5 – Model 5 for QKDN based security application services

A service scenario for model 5

Player A is an application provider with security functionality. Player B is a telecom network operator. Player C, player D and player E are QKDN infrastructure companies that provide QKDN related key management and distribution. In this scenario, player A provides a cross-domain security application service to the users (i.e., security application service users) by using keys provided by player D and player E. Player C interworks with player D and player E so that the keys are transmitted through a QKDN of player D and a QKDN of player E under the management of player C. Data for security application using keys are transferred through the telecommunication network provided by player B.

7.6 Model 6

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

Player A plays the role of a security application service provider.

Player B plays the role of a user network provider.

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

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

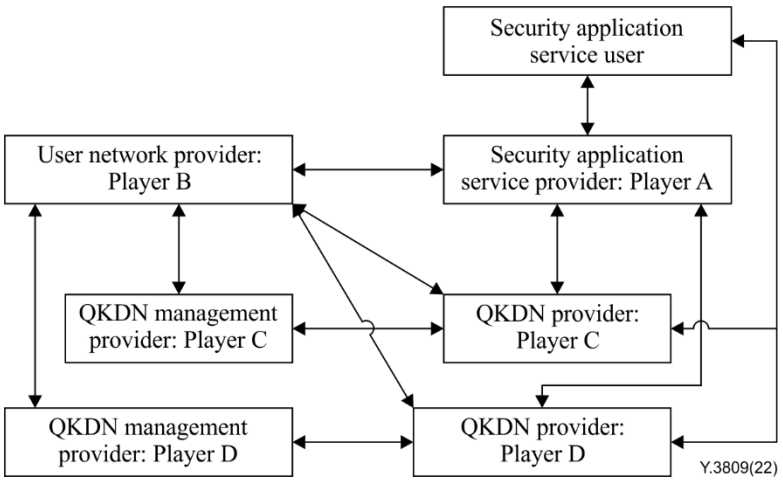

Figure 7-6 – Model 6 for QKDN based security application services

A service scenario for model 6

Player A is an application provider with security functionality. Player B is a telecom network operator. Player C and player D are QKDN infrastructure companies that provide QKDN related key management and distribution. In this scenario, player A provides a cross-domain security application service to the users (i.e., the security application service user), by using interoperable keys provided by player C and player D. Player A consumes multiple interoperable keys from player C and player D for providing security applications. Data for security application using the interoperable keys are transferred through the telecommunication networks provided by player B.

7.7 Model 7

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

Player A plays the role of a security application service provider.

Player B plays the role of a user network provider.

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

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

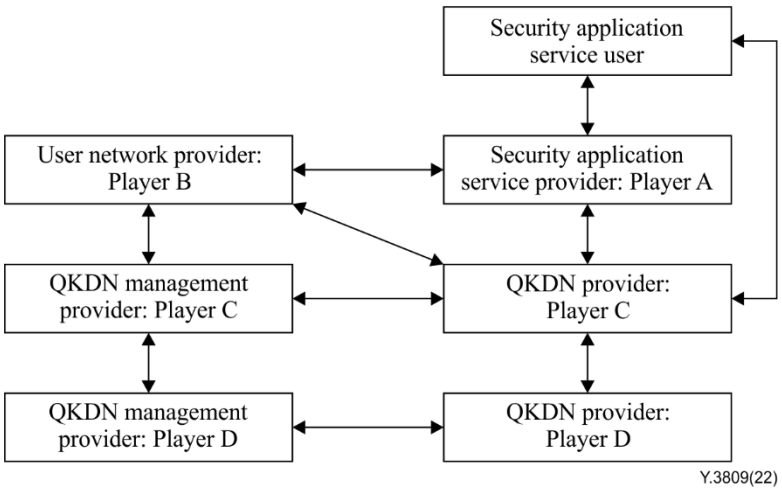

Figure 7-7 – Model 7 for QKDN based security application services

A service scenario for model 7

Player A is an application provider with security functionality. Player B is a telecom network operator. Player C and player D are QKDN infrastructure companies that provide QKDN-related key management and distribution. In this scenario, player A provides a cross-domain security application service to users (i.e., the security application service user) by using keys provided by player C. Player A consumes multiple keys from Player C. When keys are transferred through the QKDN, player C and player D interwork to transfer the keys from the source to the destination. Particularly, player C interacts with player A and player B, while player D only interacts with player C. A key is either transferred within a QKDN of player C or through the interworking QKDNs of player C and D. Data for security applications using keys from player C are transferred through the telecommunication network provided by player B.

8 Security considerations

To deploy and operate QKDN with role-based models, various security considerations and requirements such as [b-ITU-T X.1710] and [b-ITU-T XSTR-SEC-QKD] should be considered. This Recommendation describes roles, role-based models, and service scenarios in QKDN, but details of the security considerations are out of the scope of this Recommendation.

Appendix I

Implementation description of QKDN roles

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

This appendix is used to illustrate the engineering implementation of the QKDN roles in the conceptual structures of a QKDN and a user network (i.e., QKDN architecture) from [b-ITU-T Y.3800].

I.1 Introduction

It is important to clarify the relationship between the QKDN role-based model and the QKDN architecture and explain how the model maps it to the QKDN architecture.

I.2 Existing structure

– Layer structure defined in [b-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 [b-ITU-T Y.3800]: QKD module, key manager (KM), QKDN controller, 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 shown in Figure I.1.

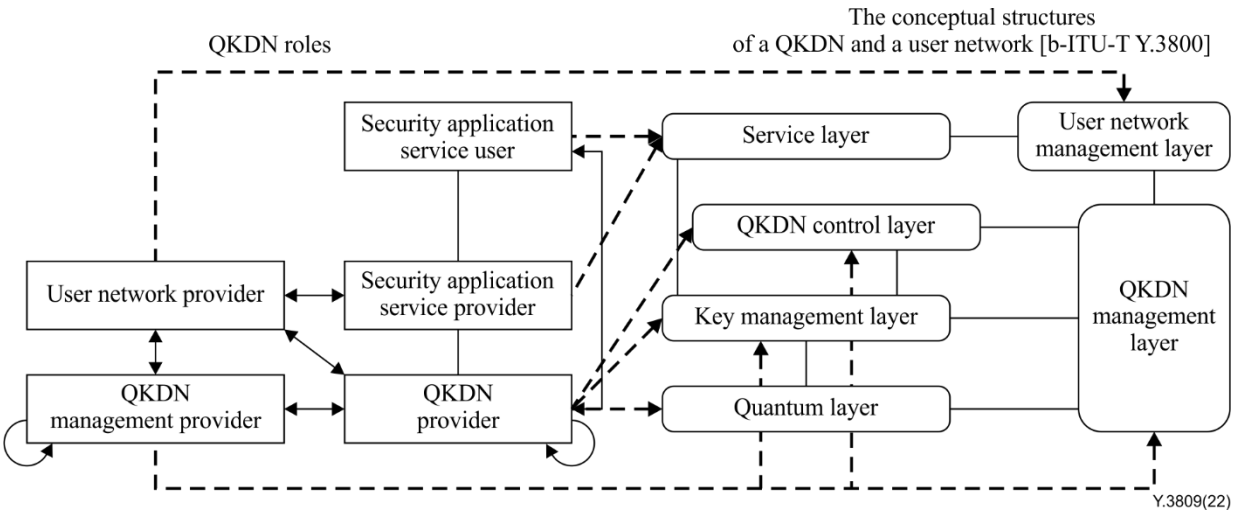

Figure I.1 – Mapping process

– **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 the security application service users. In a **service layer**, the following functional element exists i.e., the cryptographic application function. It consumes the shared key pairs provided by a QKDN and performs secure services between remote parties. Therefore, security application service users and security application service providers are mapped by the service layer.

– The **user network provider** is the owner of the user network. In a **user network management layer**, there exists a user network manager function: it performs FCAPS

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

– The **QKDN management provider** is responsible in managing the QKDN resources. In a **QKDN management layer**, a QKDN manager function is to manage 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 the QKD modules and QKD links, relay the keys, and supply the keys to the 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. This way, the QKDN management layer, key management layer, and QKDN control layer can realize the function of the QKDN management provider.

– The **QKDN provider** provides key distribution including managing the lifecycle of keys and providing these keys. In a **quantum layer**, the quantum key distribution keys (QKD keys) are generated. In a **key management layer**, a KM function is to receive and manage keys generated by the QKD modules and QKD links, relay the keys, and supply the keys to the 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 the QKDN provider can be provided by the quantum layer, key management layer, and the QKDN control layer.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[b-ITU-T P.10] Recommendation ITU-T P.10/G.100 (2017), *Vocabulary for performance, quality of service and quality of experience*.

[b-ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

[b-ITU-T Y.1401] Recommendation ITU-T Y.1401 (2008), *Principles of interworking*.

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

[b-ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.

[b-ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.

[b-ITU-T XSTR-SEC-QKD] Technical Report ITU-T XSTR-SEC-QKD Corrigendum 1 (2021), *Security considerations for quantum key distribution networks*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022