

I n t e r n a t i o n a l   T e l e c o m m u n i c a t i o n   U n i o n

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1715**

(07/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Quantum communication – Security design for QKDN

---

**Security requirements and measures for  
integration of quantum key distribution network  
and secure storage network**

Recommendation ITU-T X.1715

ITU-T

ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

|                                                        |                      |
|--------------------------------------------------------|----------------------|
| PUBLIC DATA NETWORKS                                   | X.1–X.199            |
| OPEN SYSTEMS INTERCONNECTION                           | X.200–X.299          |
| INTERWORKING BETWEEN NETWORKS                          | X.300–X.399          |
| MESSAGE HANDLING SYSTEMS                               | X.400–X.499          |
| DIRECTORY                                              | X.500–X.599          |
| OSI NETWORKING AND SYSTEM ASPECTS                      | X.600–X.699          |
| OSI MANAGEMENT                                         | X.700–X.799          |
| SECURITY                                               | X.800–X.849          |
| OSI APPLICATIONS                                       | X.850–X.899          |
| OPEN DISTRIBUTED PROCESSING                            | X.900–X.999          |
| INFORMATION AND NETWORK SECURITY                       |                      |
| General security aspects                               | X.1000–X.1029        |
| Network security                                       | X.1030–X.1049        |
| Security management                                    | X.1050–X.1069        |
| Telebiometrics                                         | X.1080–X.1099        |
| SECURE APPLICATIONS AND SERVICES (1)                   |                      |
| Multicast security                                     | X.1100–X.1109        |
| Home network security                                  | X.1110–X.1119        |
| Mobile security                                        | X.1120–X.1139        |
| Web security (1)                                       | X.1140–X.1149        |
| Application Security (1)                               | X.1150–X.1159        |
| Peer-to-peer security                                  | X.1160–X.1169        |
| Networked ID security                                  | X.1170–X.1179        |
| IPTV security                                          | X.1180–X.1199        |
| CYBERSPACE SECURITY                                    |                      |
| Cybersecurity                                          | X.1200–X.1229        |
| Countering spam                                        | X.1230–X.1249        |
| Identity management                                    | X.1250–X.1279        |
| SECURE APPLICATIONS AND SERVICES (2)                   |                      |
| Emergency communications                               | X.1300–X.1309        |
| Ubiquitous sensor network security                     | X.1310–X.1319        |
| Smart grid security                                    | X.1330–X.1339        |
| Certified mail                                         | X.1340–X.1349        |
| Internet of things (IoT) security                      | X.1350–X.1369        |
| Intelligent transportation system (ITS) security       | X.1370–X.1399        |
| Distributed ledger technology (DLT) security           | X.1400–X.1429        |
| Application Security (2)                               | X.1450–X.1459        |
| Web security (2)                                       | X.1470–X.1489        |
| CYBERSECURITY INFORMATION EXCHANGE                     |                      |
| Overview of cybersecurity                              | X.1500–X.1519        |
| Vulnerability/state exchange                           | X.1520–X.1539        |
| Event/incident/heuristics exchange                     | X.1540–X.1549        |
| Exchange of policies                                   | X.1550–X.1559        |
| Heuristics and information request                     | X.1560–X.1569        |
| Identification and discovery                           | X.1570–X.1579        |
| Assured exchange                                       | X.1580–X.1589        |
| Cyber Defence                                          | X.1590–X.1599        |
| CLOUD COMPUTING SECURITY                               |                      |
| Overview of cloud computing security                   | X.1600–X.1601        |
| Cloud computing security design                        | X.1602–X.1639        |
| Cloud computing security best practices and guidelines | X.1640–X.1659        |
| Cloud computing security implementation                | X.1660–X.1679        |
| Other cloud computing security                         | X.1680–X.1699        |
| QUANTUM COMMUNICATION                                  |                      |
| Terminologies                                          | X.1700–X.1701        |
| Quantum random number generator                        | X.1702–X.1709        |
| Framework of QKDN security                             | X.1710–X.1711        |
| <b>Security design for QKDN</b>                        | <b>X.1712–X.1719</b> |
| Security techniques for QKDN                           | X.1720–X.1729        |
| DATA SECURITY                                          |                      |
| Big Data Security                                      | X.1750–X.1759        |
| Data protection                                        | X.1770–X.1789        |
| IMT-2020 SECURITY                                      | X.1800–X.1819        |

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

## Recommendation ITU-T X.1715

### Security requirements and measures for integration of quantum key distribution network and secure storage network

#### Summary

Recommendation ITU-T X.1715 specifies security requirements and measures for integrating a quantum key distribution network (QKDN) with a secure storage network (SSN) in the service layer (Recommendation ITU-T Y.3800) and public key infrastructure (PKI) (Recommendation ITU-T X.509).

#### History

| Edition | Recommendation | Approval   | Study Group | Unique ID*                                                                   |
|---------|----------------|------------|-------------|------------------------------------------------------------------------------|
| 1.0     | ITU-T X.1715   | 2022-07-14 | 17          | <a href="http://handle.itu.int/11.1002/1000/11830-en">11.1002/1000/14995</a> |

#### Keywords

QKD, QKDN, security measures, security requirements, SSN.

---

\* 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 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/>.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

|   |                                                                                           | Page |
|---|-------------------------------------------------------------------------------------------|------|
| 1 | Scope .....                                                                               | 1    |
| 2 | References.....                                                                           | 1    |
| 3 | Definitions .....                                                                         | 2    |
|   | 3.1 Terms defined elsewhere .....                                                         | 2    |
|   | 3.2 Terms defined in this Recommendation.....                                             | 2    |
| 4 | Abbreviations and acronyms .....                                                          | 2    |
| 5 | Conventions .....                                                                         | 3    |
| 6 | Introduction .....                                                                        | 3    |
| 7 | Functional elements and information assets .....                                          | 5    |
|   | 7.1 Functional elements.....                                                              | 5    |
|   | 7.2 Information assets in SSN .....                                                       | 6    |
| 8 | Security threats .....                                                                    | 6    |
|   | 8.1 Eavesdropping .....                                                                   | 7    |
|   | 8.2 Spoofing .....                                                                        | 7    |
|   | 8.3 Deletion or corruption .....                                                          | 7    |
|   | 8.4 Repudiation.....                                                                      | 7    |
|   | 8.5 Denial of service.....                                                                | 7    |
| 9 | Security requirements and measures .....                                                  | 11   |
|   | 9.1 Security requirements and measures on original data .....                             | 11   |
|   | 9.2 Security requirements and measures on (data) share .....                              | 12   |
|   | 9.3 Security requirements and measures on SSN control and management<br>information ..... | 14   |
|   | Bibliography.....                                                                         | 16   |



# Recommendation ITU-T X.1715

## Security requirements and measures for integration of quantum key distribution network and secure storage network

### 1 Scope

This Recommendation specifies a framework for integrating a quantum key distribution network (QKDN) with a secure storage network (SSN) and public key infrastructure (PKI).

This Recommendation includes for an SSN:

- analysis of security threats;
- identification of security requirements; and
- specification of measures to meet identified security requirements.

### 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 X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.
- [ITU-T X.1712] Recommendation ITU-T X.1712 (2021), *Security requirements and measures for quantum key distribution networks – Key management*.
- [ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.
- [ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.
- [ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.
- [ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.
- [ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*.
- [ITU-T Y.3808] Recommendation ITU-T Y.3808 (2022), *Framework for integration of quantum key distribution network and secure storage network*.

## 3 Definitions

### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 certification authority (CA)** [ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

**3.1.2 key data** [ITU-T Y.3803]: Random bit strings that are used as a cryptographic key.

**3.1.3 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.

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

**3.1.5 quantum key distribution link** [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

**3.1.6 quantum key distribution module** [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

**3.1.7 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.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

**3.1.8 quantum key distribution network controller** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

**3.1.9 quantum key distribution network manager** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

**3.1.10 quantum key distribution node** [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

### 3.2 Terms defined in this Recommendation

None.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA              Certification Authority

DoS             Denial of Service

FCAPS          Fault, Configuration, Accounting, Performance and Security