ETSI GS QKD 008 V1.1.1 (2010-12)

Group Specification

Quantum Key Distribution (QKD); QKD Module Security Specification

Disclaimer

This document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership

Reference
DGS/QKD-0008

Keywords
analysis, protocols, Quantum Key Distribution,
security, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group on Quantum Key Distribution systems (QKD - ISG).

Introduction

The present document specifies the security requirements for QKD modules utilized within security systems to protect sensitive information in telecommunication systems. The present document has been developed by the ETSI Quantum Key Distribution Industry Specification Group (QKD-ISG) composed of both operators and vendors. The working group has identified requirements for QKD modules to provide data security.

Following the methodology used in conventional cryptographic security modules and systems, eleven security aspects have been identified, and the present document will establish the minimum requirements that QKD modules will fulfil to be in accordance with the present document. Because of the particular requirements and final quality that the Quantum Key Distribution systems have, the present document has not considered the possibility of having different security levels included in the present document, and it does not consider different degrees of data sensitivity nor different application environments.

In the present document, software requirements are given great prominence because software controls all the actual measurement and communications systems and software security appears as the cornerstone of the general system security. In the present document, requirements that protect the QKD modules against non-invasive attacks are also provided.

While the security requirements specified in the present document are intended to maintain the security provided by a QKD module, conformance to them is necessary but not sufficient to ensure that a particular module is secure. The operator of a QKD module is responsible for ensuring that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted. Similarly, the use of a validated QKD module in a computer or telecommunications system is not sufficient to ensure the security of the overall system.

The importance of security awareness and of making information security a management priority should be communicated to all users, managers and system administrators. Since information security requirements vary for different applications and scenarios, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses.

Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, as well as backup and contingency planning.

1 Scope

The present document aims to establish the necessary requirements for a QKD module to have a high probability of detecting and responding precisely and timely to attempts of direct physical access, and use or modification of modules inside. The principal objective is to detect any possible penetration with high probability, and resulting in the immediate zeroization of all Critical Security Parameters in plain text.

This objective requires mechanisms to provide a complete envelope of protection around the QKD module, and sensors and circuits to detect and respond in time to all unauthorized attempts of physical access. This can be obtained using strong enough enclosures and redundant tamper detection and response circuitry that zeroizes all plaintext Critical Security Parameters. Enclosure's integrity can be controlled using tamper-evident coatings or seals, and pick-resistant locks on all removable covers or doors of the module.

Strong enclosures must be opaque to all visual and non-visual radiation examination and the tamper detection and zeroization circuitry is protected against disablement. When zeroization is required, Public and Critical Security Parameters are zeroized.

Access and module operation must require identity-based authentication mechanisms that enhance a role-based organization. This authentication must require at least two-factor authentication for operator authentication (secret password, physical key or token, biometric.). The proper operation requires the operator's identity authentication and to verify that he is authorized to assume a specific role and perform a corresponding set of services.

Entry or output of Critical Security Parameters must be done using ports that are physically separated from other ports, or trough interfaces that are logically separated using a trusted-channel from any other interfaces.

All QKD secure modules must be protected against environmental conditions or fluctuations outside of the module's normal operating ranges, because such deviations can be seen as an attack, or they can increase the module failure probability and that can compromise the module security and its operation. The environmental magnitudes to control must be darkness (when required), temperature, voltage, pressure, humidity, atmosphere chemical composition, mechanical vibrations and the presence of nuclear and any other ionizing radiation. Because QKD modules include optical and electro-optical subsystems, it is necessary to control any environmental variable that could affect specifically to that components and the way that they perform, no matter if it is temporally or permanently.

A QKD module is required to either include special environmental protection features designed to detect fluctuations and zeroize Critical Security Parameters, or to undergo rigorous Environmental Failure Testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise its security.

In particular, all QKD modules require the protection of Critical Security Parameters against Timing Analysis attacks, Simple Power Analysis, Differential Power Analysis attacks, Electromagnetic Emanation Attacks and any attack performed through the optical channels.

QKD modules must use strong cryptographic protection to detect and prevent the disclosure and modification of Public Security Parameters as well as Critical Security Parameters when the module is inactive.

To be sure that every time the module is operating in a safe mode, the module must have a clear indication that the module is operating in an Approved Mode.

Because software has the final control in any QKD module, this component must provide robust and tested solutions for the encryption and authentication of all the Critical Security Parameters, all the Sensitive Security Parameters in the system and also to provide secure integrity tests for the software code when the module is not in use.

QKD Module software components can be executed on a general purpose computing system if the operating system provides the auditing of all operator accesses to the audit data, to all requests to use authentication data management mechanisms, all use of security-relevant Crypto Officer Functions, and to all requests to access authentication data associated with the QKD module. In particular, the operating system running the general purpose computing system has to:

- prevent operators in the user role from modifying software, system Sensitive Security Parameters (SSPs), and audit data stored in the operational environment of the module;
- communicate all SSPs, authentication data, control inputs, and status outputs via a trusted channel; and
- audit the operation of any trusted channel.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

approved data authentication technique: approved method that may include the use of a digital signature, message authentication code or keyed hash

EXAMPLE: RSA, ECDSA and hMAC

approved mode of operation: mode of the QKD module that employs only Approved or Allowed security functions

NOTE: Not to be confused with a specific mode of an Approved security function.

EXAMPLE: AES in CBC mode.