ETSI GS QKD 012 V1.1.1 (2019-02)

Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment

Disclaimer

The present 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-0012_DeployParam

Keywords
quantum cryptography, Quantum Key Distribution

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes the main communication resources involved in a QKD system and the possible architectures that can be adopted when performing a QKD deployment over an optical network infrastructure.

The scope of the present document is restricted to QKD deployments over fibre optical networks. Architectural options are also restricted to point-to-point communication.

The different entities that can take part in a QKD deployment and the possible contexts of deployment capturing the roles played by the different entities are defined. One specific context (context1) is then addressed where one entity (QKD_O), operating QKD Modules, plans a QKD deployment over an optical network infrastructure, operated by another entity (NET_O).

The information regarding the QKD system parameters and the network parameters to be exchanged (in context1) are listed and prioritized. The corresponding tables, placed at the end of the present document, can be used as a standard template for the exchange of information between QKD_O entities and NET_O entities involved in the QKD deployment.

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

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

Not applicable.

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 Definition of terms, symbols and abbreviations

3.1 Terms

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

channel: "logical channel", i.e. a communication link, between a sender and a receiver, over which some logical information is exchanged

NOTE: Throughout the present document, the term "channel" refers by default to a "logical channel", i.e. a communication link, between a sender and a receiver, over which some logical information is exchanged. Depending on the context, the channel implementation, i.e. the physical nature of the channel, related to the physical encoding of the information, will also often be considered. In that case the name "channel" will refer to both the logical nature of the channel, and to the physical nature of its implementation.

classical optical channel: optical implementation of a communication channel for transmitting classical information

NOTE: Classical optical signals typically consist of optical pulses containing a large number of photons, over which some information is encoded (in time, phase, intensity, polarization, etc.). Classical optical signals are perfectly distinguishable and communication over a classical optical channel is therefore vulnerable to zero-error attacks where an eavesdropper non-destructively reads the signals, without introducing errors and yet fully copies the logical data.

context: "context of deployment", i.e. a scenario specifying some aspects of the roles played by the different entities, and their interplay

disturbance on the quantum channel: disturbance on the quantum channel related to the noise on the QKD quantum channel

NOTE: Disturbance is measured by evaluating the correlation level between the classical strings (raw data) shared by A and B after the quantum communication phase.

matching QKD module: QKD Module that when connected by appropriate communication channels can cooperate to run a QKD protocol with the QKD Module it is matched with

NOTE: Typically a type A QKD Module could be a matching QKD Module for a type B QKD Module and vice versa where compatibility requirements are met.

network operator: entity in charge of operating technically the optical network infrastructure and in particular providing communication interfaces to QKD at points A and B

EXAMPLE: In the context of a deployment, this role is typically assumed by a service provider.

QKD distillation channel: channel used to exchange digital classical information, typically between QKD Modules of type A and B, in order to agree on a shared secret key starting from the raw data the QKD Modules initially obtain in an earlier stage of a quantum key distribution protocol

NOTE 1: The communication over the distillation channel is typically used to perform two stages of a QKD protocol:

- *Sifting:* A and B communicate classical information to select a subset of the raw data, leading to the sifted key.
- *Classical post-processing:* A and B agree on a secret key from their respective raw data via public discussion over the distillation channel.

NOTE 2: The QKD distillation channel can be implemented over different types of transmission media (optical, copper wire, etc.).

NOTE 3: The name "Distillation" normally refers to the notion of classical post-processing excluding sifting that can be performed prior to distillation. Nevertheless the name "distillation" is used as the name for this channel that can also include communications associated with sifting, since this name is non-ambiguous and expresses clearly the nature of the information exchanged on the channel. (Similarly the name "Synchronization channel" is used to refer to a channel that can convey information wider than time synchronization.)

NOTE 4: The QKD Distillation channel can also be called the "Distillation channel".

NOTE 5: One of the security requirements of QKD protocols is that the Distillation channel is authenticated. Discussing security and cryptographic requirements of QKD is outside of the scope of the present document. Deployment and initialization of matched QKD modules should be done in accordance with an approved security policy.

QKD module: set of hardware and software components that implements QKD cryptographic functions and quantum optical processes, including cryptographic algorithms and protocols and key generation, and is contained within a defined cryptographic boundary

NOTE: A QKD Module constitutes one endpoint in a QKD link. It can be of type A (sender) or B (receiver). A QKD Module typically has three communication channel interfaces:

- QKD quantum channel,
- QKD synchronization channel,
- QKD distillation channel.

QKD operator: entity in charge of operating technically the QKD Modules

EXAMPLE: In the context of a deployment, the "QKD Operator" role would typically be the responsibility of the owner of the QKD Module. It might also be the responsibility of a tier (possibly the QKD manufacturer) in charge of QKD Module operation and maintenance.

QKD quantum channel: quantum optical channel, typically between QKD Modules of type A and B, used to perform quantum key distribution

NOTE 1: It is implemented by sending quantum optical signals (typically weak coherent states of light), on which information is encoded (different encodings can be used: phase, polarization, time-bin, spatial mode, etc.).

NOTE 2: In the context of the present document, it is assumed that the quantum channel is implemented over an optical fibre.

NOTE 3: The QKD Quantum channel can also called "Quantum channel".

QKD synchronization channel: channel that carries reference signals for the purpose of reference frame sharing (synchronisation, phase reference, polarization reference etc.), typically between QKD Modules of type A and B, in order to perform quantum key distribution

NOTE 1: It is typically implemented by encoding analogic information encoded over classical optical signals, sent over an optical fibre.

NOTE 2: The name "Synchronization" normally refers exclusively to the notion of time reference sharing and no other types of reference information. Nevertheless the name "Synchronization" is used as the name for this channel that can also include other types of reference information, since this name is non-ambiguous and expresses clearly the nature of the information exchanged on the channel. (Similarly the name "Distillation channel" is used to refer to a channel that can convey information wider than distillation.)

NOTE 3: The QKD Synchronization channel can also be called the "Synchronization channel".

QKD system: system composed of a pair of matching QKD Modules (of type A and B)

NOTE: When properly connected to the appropriate communication channels a QKD system can perform quantum key distribution: establishment between A and B of a symmetric secure key.

Quantum Key Distribution (QKD): procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory

quantum optical channel: optical implementation of a communication channel for transmitting quantum signals

NOTE: It is implemented by encoding quantum information, i.e. non-orthogonal quantum states, on dim optical pulses containing a low mean photon number. The optical link on which the quantum channel is implemented is in general required to be transparent, i.e. it cannot contain any amplifier elements.

raw data: raw correlated classical data at A and B that was shared using a quantum channel and after any sifting has been implemented

NOTE 1: In many implementations quantum signals are prepared at A, sent on the quantum channel and then received and detected (with finite probability and fidelity) at B.

NOTE 2: The name "raw data" refers to more than one classical string, e.g. one at A and one at B. These raw strings are typically correlated but not identical.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A	Alice, designating either a QKD Module, or the operator of said device, or the location of said device
AES	Advanced Encryption Standard
B	Bob, designating either a QKD Module, or the operator of said device, or the location of said device
CV	Continuous Variable
$Distil_B$	Distillation channel interface of B
NET	Network
NET_O	Network Operator
PMD	Polarization Mode Dispersion
QKD	Quantum Key Distribution
QKD_O	Quantum Key Distribution Operator
QKD_A	Quantum Key Distribution device of type A
QKD_B	Quantum Key Distribution device of type B
WDM	Wavelength Division Multiplexing

4 QKD Communication channels and architecture

4.1 QKD processes

A QKD system consists of two QKD Modules (QKD_A and QKD_B, in short A and B) connected by communication channels (a Quantum channel, a Distillation channel and possibly a Synchronization channel). The two QKD Modules, connected by communication channels, follow a protocol that can be described as a set of processes, executed in parallel or sequentially to establish a symmetric secure key at both A and B.

A high-level list and description of the three main processes that are executed by a QKD system are provided in table 1, focusing on the communication needs associated with these three processes.

Table 1: Three typical main QKD processes

Process Description	QKD Modules running the process	Relevant Communication channel	Remarks
Alice encodes classical information on quantum states and sends those quantum states on the quantum channel to Bob.	Alice	**Quantum channel**	In QKD, the states prepared by Alice should be such that they cannot be distinguished from each other with no error. As a consequence the set of states used in a QKD protocol is a non-orthogonal set of states (e.g. the four BB84 states).
Alice prepares classical analogic optical signals (needed for reference sharing purposes) and sends those signals on the Synchronization channel to Bob.	Alice	**Synchronization channel**	Typical applications: clock synchronization, polarization drift monitoring and correction, phase drift monitoring and correction. Reference frame sharing requires the exchange of physical reference signals (as opposed to digital information). Those signals are usually not at the quantum level (i.e. they typically contain large number of photons).
Alice and Bob exchange classical messages between Alice and Bob, to perform: • Sifting (to agree on the raw data to be retained for subsequent classical post-processing); and • Classical post-processing.	Alice and Bob	**Distillation channel**	"Classical post-processing" takes the raw data as input, and outputs a secret key. Post-processing is often decomposed in sub-protocols: error correction, privacy amplification and confirmation. Bidirectional classical communication is most of the time used in classical post-processing for QKD.

4.2 QKD Communication channels

As can be seen from table 1, a QKD system runs different processes locally at A / B and some processes require communication between A and B. These communications may occur on up to three different types of channels:

a) QKD Quantum channel.

b) QKD Synchronization channel (typically an analogic optical classical channel).

c) QKD Distillation channel (typically conventional bidirectional digital channel(s) - one or more depending on the implementation).

Some characteristics of these communication channels are described in clauses 4.3 to 4.5.

4.3 QKD Quantum channel

The Quantum channel is typically a unidirectional optical channel. This optical channel can be fibre-based or free-space. The Quantum channel is typically used in a QKD protocol, to send non-orthogonal quantum states, conveying classical information from A to B.

QKD protocols typically rely upon monitoring the disturbance (errors) when transmitting random classical data over the quantum channel. If the disturbance is too high the QKD system assumes the disturbance could be due to an adversary and is unable to distil secure keys. The level of disturbance below which secure keys can be distilled depends upon various protocol-specific security parameters. The ability to detect potential eavesdropping of the quantum signals in transit through the disturbance this would necessarily introduce is the unique proposition of QKD.

Quantum channel parameters, in particular optical losses and noise sources (such as optical attenuation, imperfect optical encoding at A, reference frame stability between A and B, imperfect detection at B, external optical signals, etc.), play a crucial role in determining the practicality of distributing secure keys using QKD. To a large extent, the ability to perform QKD over a given Quantum channel with fixed optical losses depends on the ability to minimize the end–to–end noise level.