Redefining Security

QUANTUM-SAFE SECURITY

Cerberis^3 User Manual

Version : 1.24
Date : 09.06.2022

ID Quantique SA
Ch. de la Marbrerie, 3bis
CH-1227 Carouge/Geneva
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

Please send any comment to
support@idquantique.com

Information in this document is subject to change without notice.

Disclaimer

THIS DOCUMENT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

No license, express or implied, to any intellectual property rights is granted herein, except that a license is hereby granted to copy and reproduce this specification for internal use only. Contact ID Quantique for information on further licensing agreements and requirements. ID Quantique disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. ID Quantique assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of ID Quantique products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right. ID Quantique products are not intended for use in medical, lifesaving, or life sustaining applications.

ID Quantique may make changes to documents, specifications, and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked reserved or undefined. ID Quantique reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Contents

1. Introduction

1.1.About ID Quantique

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises, and government organizations globally.

IDQ also commercializes a quantum random number generator, which is the reference in the security, simulation, and gaming industries.

Additionally, IDQ is a leading provider of optical instrumentation products, most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

1.2.About this document

This document, the *IDQ Cerberis3 User Guide*, provides information on the Cerberis3 QKD nodes and instruction on how to operate them.

1.3.Intended audience

This document is for system operators, network operators, and system programmers. Specific operator procedures are defined by the individual installation to meet local requirements.

1.4.Classification

This document is classified by ID Quantique as *Confidential*.

1.5.References

This section lists documents related to the IDQ Cerberis3 solution products. It also describes how to access IDQ QKD publications and IDQ QKD related resources online.

The following documents are available for the IDQ QKD Systems:

- *Cerberis3 User Guide* describes the IDQ Cerberis3 QKD node
- *Cerberis3 solution Quick start guide* describes how to install and configure the IDQ QKD Cerberis3 solution
- *IDQ QNET shell User Guide* describes the QNET CLI program required for local system administration.
- *IDQ QNET User Guide* describes the QNET CLI program required for remote system administration.
- *IDQ QNET Web API User Guidel* describes the QNET Web Server and how to use the QNET Web Application Programming Interfaces (APIs)
- *Understanding QKD log files* explains QKD logs.

You can find additional product information on the IDQ Web site: https://www.idquantique.com/resource-library/quantum-key-distribution/

1.6.Prerequisite

To read about the new functions offered in this release, see the IDQ QKD product *Release Note*.

1.7. Support information

If you have any questions or require assistance with the IDQ QKD solutions, please contact IDQ Support:

- Visit the IDQ Support site at https://www.idquantique.com/support
- Email IDQ Support at support@idquantique.com

1.8. Safety precautions

- Carefully read through this procedure before operating the Cerberis3 Node system.
- This system is intended to only be used indoors.
- Never look directly into an active fiber cable and ensure proper eyewear is worn when handling unterminated fiber ends.
- Always handle the devices using proper ESD damage prevention and grounding methods.
- Ensure all power connections are connected to a ground socket. Failure to connect to ground creates a shock hazard which may cause injury to the operator.
- Refrain from bringing water or other liquids around any part of the system. If the systems do get wet, shut all devices down immediately.

ℹ NOTE

ID Quantique shall not be held responsible for any damages to persons or property caused by incorrect installation or use of this appliance.

⚠ WARNING

The warranty is void if any module has been opened by unauthorized personnel.

1.9. EC declaration of Conformity

ID Quantique SA declares that the product:

Model(s): Cerberis3
Product type: Quantum Key Distribution System

is in conformity with following relevant directives and standards:

Directives
LVD 2014/35/EU
EMC 2014/30/EU
ROHS 2015/863/EU

Safety Standards:
EN 60950-1 :2006, A2:2013
EN 60825-1 :2014

EMC Standards:
EN 55032:2015 (Class B)

EN 55024:2010 +A1 :2015
EN 55035:2017
ETSI EN 300 386 V 2.1.1

This declaration of conformity is issued under the sole responsibility of the manufacturer.

2. Equipment and Tools

2.1.Supplied Equipment

ID #	Part Name	QTY	Function	Notes
Pt. 1.	QKD transmitter (Alice) blade (QKD-A)	1	QKD transmitter blade	
Pt. 2.	QKD receiver (Bob) blade (QKD-B)	1	QKD receiver blade	
Pt. 3.	ATCA Shelf including two power supply cables	2	Housing of the modules	• 1 ATCA shelf per blade with two empty ATCA slots per blade
Pt. 4.	Optical SFP transceiver modules	2 (1 per QKD blade)	Optical transceivers for the service channels	• ITU wavelengths (2x CH30 1553.33 nm) • Compliant with G.694.1 • Dual SMF-28 LC connectorized • 2.67 Gbps rate
Pt. 5.	Service channel fiber patchcord	1	Fiber links for the service channels	• 2m length • LC/PC-LC/PC connectorized • Type: dual SMF-28 patchcord
Pt. 6.	Quantum channel fiber patchcord	1	Fiber links for the quantum channel	• 2m length • FC/APC connectorized • Type: SMF-28 patchcord
Pt. 7.	Optical quantum channel attenuator	3	To add additional losses in the quantum channel	• FC/APC connectorized, male-female • 1x 10 dB attenuator • 1x 5dB attenuator • 1x 3dB attenuator
Pt. 8.	Optical service channel attenuators	4	To add additional losses in the service channel	• LC connectorized, male-female • 2x 15dB attenuator • 2x 7dB attenuator
Pt. 9.	Ethernet cables	2 (1 per ATCA shelf)	Network connection	• To connect the ATCA switch to the network
Pt. 10.	Fiber cleaning tool	1	Fiber cleaning	• To clean the fiber ends before attaching them.

NOTE

The equipment listed corresponds to the equipment received for standard configuration. In case of custom option, the supplied equipment will differ.

The Cerberis3 is provided with fix attenuators of different attenuation for the quantum channel (3, 5, 10dB) and the service channel (7, 15dB), to optimize the losses on both channels and maximize the system performance.

To work properly and securely the Cerberis 3 QKD system must have a losses budget on the QC between 10dB and the max attenuation supported by the system (i.e. for a 12dB grade Cerberis 3 the losses on the QC should be between 10 and 12dB, for a 18dB grade Cerberis 3 the losses on the QC should be between 10 and 18dB). The system is also provided with SFPs for the service channels optimized for 100km fiber range, so it is also recommended to have ~15dB losses on the SC.

As rule of thumb, if the system is deployed on a lab environment with a point-to-point configuration using the 2m fiber patch cords provided for the QC and SC, it is mandatory to use a 10dB attenuator on the QC and 2x 15dB attenuators on the SC (one for each SC fiber). If the system is deployed on a real network and the losses budget on the QC and SC is less than what previously described, it is possible to add the additional attenuators provided.

IMPORTANT NOTE

Before the deployment of the Cerberis 3 system on a real network is always suggested to measure the effective losses budget of the QC and SC fibers as well as the effective length (and length difference) of the QC and SC fiber.

2.2.Additional tools required

ID #	Part Name	QTY	Function	Notes
Pt. 11.	Configuration PC	1	Controlling, start up, and monitoring of the blades	• Ethernet port and SSH/Telnet connectivity required • SSH/Telnet client software installed
Pt. 12.	Standard Philips screwdriver set	1	For fixing the ATCA chassis in the 19” rack	
Pt. 13.	Wrench	1	For fixing the ATCA chassis in the 19” rack	
Pt. 14.	ESD Wrist Strap	1	ESD protection	
Pt. 15.	Grounding cable	2	Grounding of ATCA chassis	Depends on the customer infrastructure

3. Getting Started

3.1. Cerberis3 solution overview

Cerberis3 performs standard key management functions between nodes, including key generation, key storage, and key life cycle management. Cerberis3 embeds enhanced trusted security components, like tamper detection, a secure memory module, as well as an IDQ QRNG chip which provides proven randomness for all the related crypto functions. This guarantees the highest security standards, throughout the key management process, from key generation to key delivery, and including key storage.

QKD administrators can configure and monitor QKD networks via either an embedded REST WebAPI or via an Element Management System (EMS) web console by setting consumers, providers at each QKD network node, QKD links between nodes and key distribution routes between key consumers.

The WebAPI continuously collects several critical parameters, such as system status, fan, power supply, temper detection, Quantum key rate, QBER (Quantum Bit Error Rate), KMS key buffers, and can distribute them to 3rd party monitoring systems, via common protocols like SNMP, syslog, etc. Monitoring events are also generated when QBER becomes too high, warning there might be an intruder on the QKD quantum channel.

In addition, our Quantum Management System (QMS) provides a single Management and Monitoring platform for all QKD products and components. It reduces the time and effort to manage large and complex QKD Network.

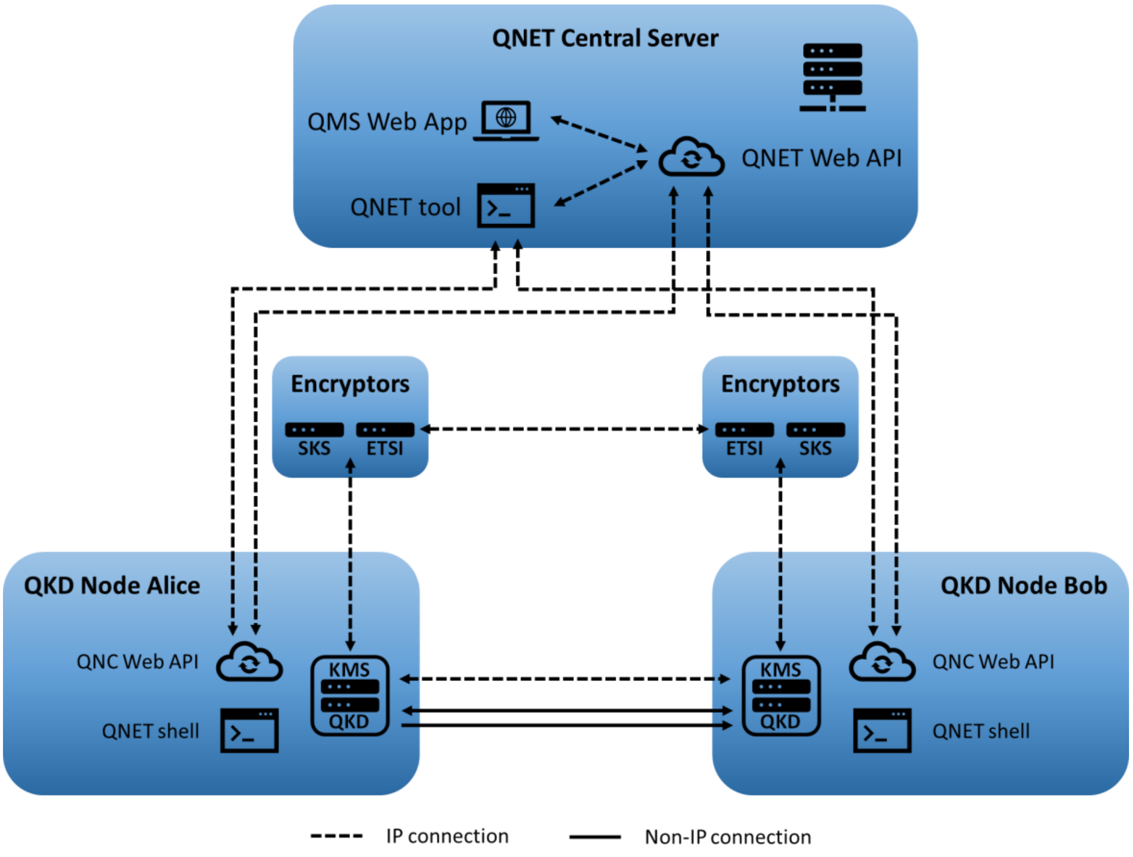


Figure 1: Cerberis3 solution for a point-to-point deployment

In Figure 1 is shown a schematic of a Cerberis3 solution deployed in point-to-point configuration. Quantum communication over the two QKD nodes are done over standard SMF-28 optical fiber. The connection between the QKD KMS (Key Management System) can be done via Ethernet copper cables or optically using a dedicated SFP transceiver. The QKD node KMS is interfaced directly via Ethernet copper cables with the encryptor, and act as an arbitrator between key distribution systems (Provider) and encryptors (Consumer).

Following the schematics of Figure 1 the function of each component can be summarized as follow:

- QNET Web API has two main purposes:
    - simplify QKD node's centralized configuration and monitoring.
    - automatize QKD node’s network configuration.
- QMS Web Application is a Graphical User Interface of the QNET Web API.
- QNET tool is a command line interface of QNET Web API. QNET tool could also be installed on a distinct computer.

Each independent QKD node can also be configured and monitored by QNET shell which is embedded in a QKD node.

Encryptors implementing ETSI 014 relying on HTTPS Restful protocol and encryptor implementing CISCO SKS protocol can be interfaced with a QKD node.

3.1.Cerberis3 QKD Node description

A.1. A point-to-point Cerberis^3 system consists of a pair of Cerberis^3 nodes implementing the COW protocol (see B.1 COW protocol description

The aim of Quantum Key Distribution is to exchange a secret key between Alice and Bob by encoding bits with quantum state carried by single photons (qubits). There are different ways to encode qubit values on single photons. One of those ways is called time-bin qubits. As shown in Figure 25 Illustration of the qubit sphere and of time-bin qubits., this method consists in creating a pair of coherent pulses propagating in the same spatial mode and separated by a given time. The first pulse is called the early pulse. The second one is called the late pulse. To generate all possible qubit values (i.e. all possible states of the qubit sphere), the intensity ratio between those two pulses can be varied between 0 and infinity. Those two extreme cases correspond to the two poles of the sphere, i.e. either when the whole optical energy of the single photon is contained in the early or late pulses. Those two quantum states compose the computational basis of the qubit space. By changing the energy level ratio between the two optical pulses, one can move the qubit state along one of the meridians of the qubit sphere. To move along one of the parallels, one needs to change the phase relation between the early and late pulses. One manner to implement time-bin qubit emitter is based on an unbalanced Mach-Zehnder interferometer where the input beam splitter ratio can be varied and the output beam recombiner is a fast switch. A possible implementation of a time-bin qubit analyzer consists in the same Mach-Zehnder interferometer where input and output ports have been swapped.

The BB84 protocol can be implemented with time-bin qubits. In this case, it is generally implemented with four qubit states located on the equatorial plan of the qubit sphere. This choice is made to guarantee as many similarities as possible in the implementation of the two bases used in BB84 protocol. In this case, the two Mach-Zehnder interferometers are made with two 50/50 couplers and one phase modulator. This kind of implementation requires a tight control on the interferometer’s stability or at least a dynamic adjustment of one interferometer compared to the other one.

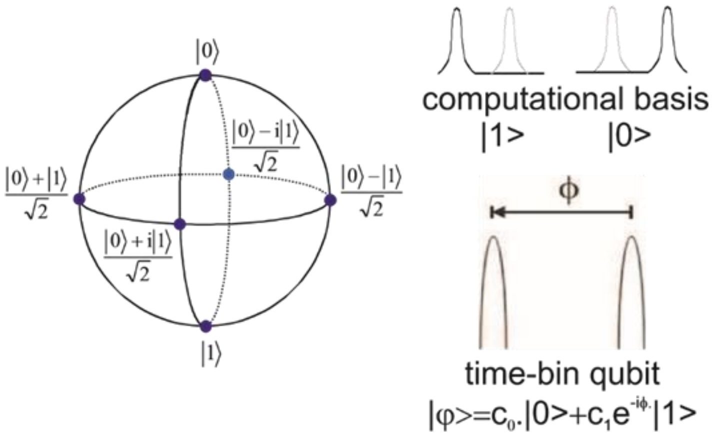

$|0\rangle$
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$|1\rangle$
computational basis
|1>
|0>
ϕ
time-bin qubit
$|\varphi\rangle = c_0.|0\rangle + c_1 e^{-i\phi}|1\rangle$

Figure 25 Illustration of the qubit sphere and of time-bin qubits.

The aim of COW protocol is to make the implementation of a QKD system as simple as possible to allow a strong increase of the final secret key rate in a manner that allow the industrialization of the system. Therefore, a first requirement of COW protocol was not to use two interferometers to avoid stabilization of one interferometer compared to another. A second requirement of this protocol was to work specifically with weak optical coherent pulses, but not with single photon pulses. This requirement is motivated by the fact that it is very simple to implement weak coherent pulse sources whereas single photon sources are still difficult to handle. Several other requirements, that are not listed here, were targeted when COW protocol was designed.

A first specificity of COW protocol is to use the qubit basis composed of the two pole states (the early and the late pulses). Hence, the measurement method to analyze this basis is simply to measure the time of detection of the optical pulse. If one detection occurs in the early time-bin, the qubit value is a |0> state, whereas if it occurs in the late time-bin, the qubit is a |1> state. This measurement method does not require any complex optical component except one single photon detector with a temporal accuracy allowing one to distinguish between the two time-bins. In COW protocol, as in any QKD protocols, two qubit bases are used to guarantee the security of transferred keys. But in this protocol, one basis will be used to generate the raw key and the other one to estimate the security level of the exchanged qubits in the first basis. The basis used to exchange the raw key is the computational basis, because as explained previously, it requires an analyzer composed uniquely on a single detector. This basis will be the more often used to maximize the raw key rate (in other protocol like BB84, the ratio because the two basis is 50/50 in general because both bases equally contribute to the generation of raw keys and to the estimation of the security level of this raw key). The second basis used in COW protocol is one of the bases located on the equatorial plan of the qubit sphere. The analyzer for this kind of basis is implemented with an unbalanced interferometer as described in the case of one example of a BB84 protocol implementation. To avoid an implementation with only one interferometer, COW protocol is based on a qubit emitter that requires no interferometer. COW emitter needs to be able to emit either early or late pulses to generate states of the computational basis. This can be done easily by switching on and off a light source at the time corresponding to the desired qubit states. One of the key ideas of COW protocol is to keep the coherence between two consecutive optical pulses belonging to the same time-bin qubit or not (i.e. one belonging to one qubit and the other one belonging to the following qubit). This coherence can be checked with the interferometer in the receiver station in both cases if the time separation between two time-bin quits equals the time between the two pulses composing one qubit. Therefore, the emitter in COW protocol needs to guarantee the same phase relation between consecutive optical pulses whether they belong to the same qubit or not. To enhance the security of COW protocol, one qubit state of the second basis of the receiver will be emitted from time to time. This state is called decoy sequence. It consists in an early and a late optical pulse with the same energy level than the early pulse in a |0> state. The phase relation between one of the two pulses of the decoy sequence and the consecutive pulses needs to be kept identical to the one between pulses of the computational basis. This decoy sequence is used in combination with the second basis analyzed in the receiver to estimate the security of the raw key exchanged using the computational basis. The ratio between the emitted states from the computational basis and the decoy sequence is in favor of the computational basis to optimize the raw key rate.

In summary, as depicted in Error! Reference source not found., COW protocol consists in an emitter emitting qubits states from the computational basis or decoy sequences. The time between all consecutive pulses is identical and the phase relation between those consecutive pulses is kept constant. The ratio of the number of qubits from the computational basis and the number of decoy sequences is in favor of the computational basis. The receiver station consists in an analysis for the computational basis and an analyzer to check the phase relation between two consecutive optical pulses. The ratio of use of the analyzer for the computational basis compared to the use of the analyzer for the phase relation check is in favor of the computational basis. A QBER value is measured by counting the probability of having an error in the exchange of qubits of the computational basis. The phase relation check is quantified by measuring the visibility of interferences occurring in the second basis analyzer. Based on both values, QBER and visibility, (plus few other parameters like the ratio values) it is possible the estimate if it is possible to extract secret keys form the qubits exchanged between the emitter and the receiver stations.

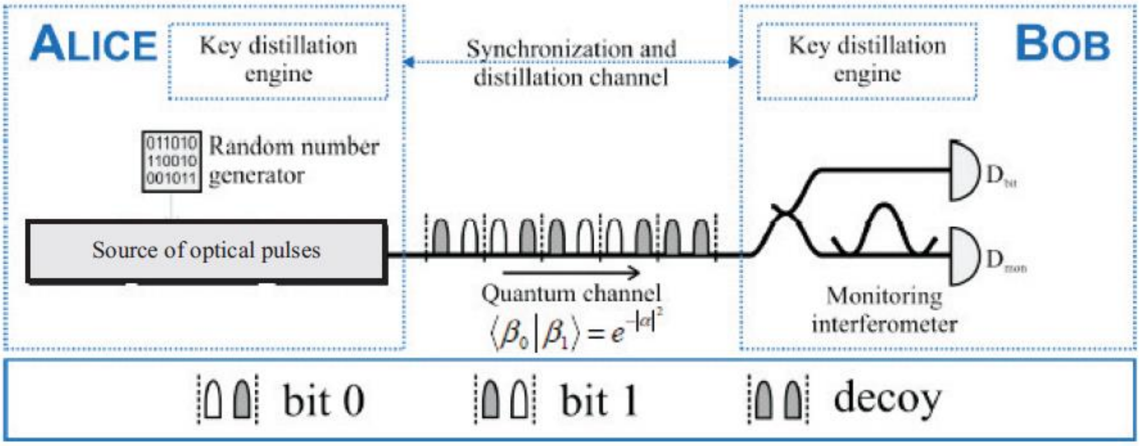


Figure 26 Illustration of COW principle

COW 4-states

Following the paper of Marcos Curty ([2101.07192] Zero-error attack against coherent-one-way quantum key distribution (arxiv.org)) describing a “theoretical” attack that could be performed on COW protocol, a security analysis has been conducted. Thanks to this analysis we can prove that the COW protocol is still safe today up to 12dB dynamic range, with the current parameters in the trusted detector scenario.
To be safe also at higher dynamic range, we adapted the protocol by implementing a countermeasure which allow us to prevent the sequential attack and extend the dynamic range to 16dB and more.
In the COW 4-states protocol an additional vacuum state is added to the protocol, this implementation significantly decreases the probability that Eve's unambiguous state discrimination measurement can produce a conclusive result.

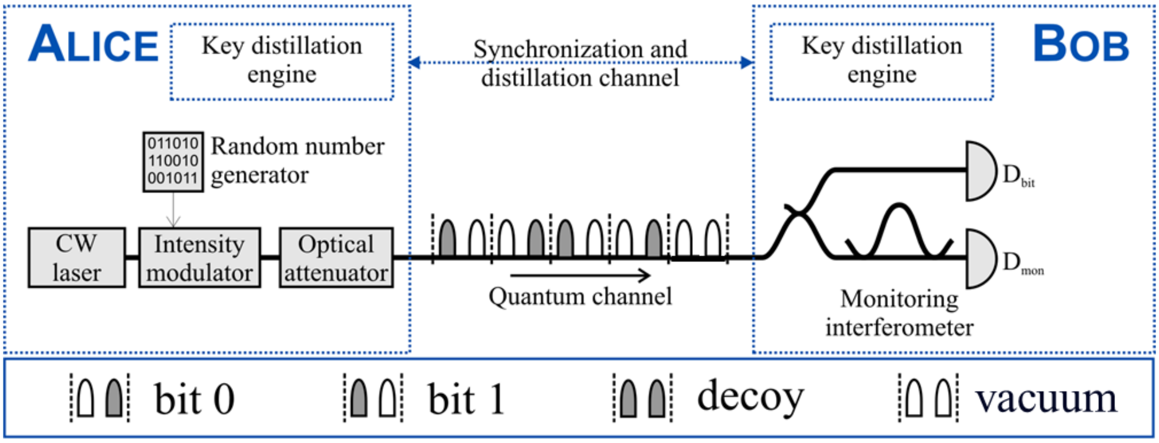


Figure 27: Illustration of the COW 4-states protocol.

Using the QNET shell on Alice QKD terminal, it is possible to see which protocol is running with the command:

protocol

the answer can be:

QKD Protocol: Cow4States

or

QKD Protocol: Cow3States

it is possible to change the protocol using the command protocol followed by the type of protocol, for ex:

protocol Cow4States

NOTE

Please contact ID Quantique for additional information about the implementation of COW 4-state protocol and its security.

A.2. Commands Summary of the QS3201 Shelf Manager

Group	Command	Description
Alarm	`alarm_clear`	Remove or clear a triggered alarm from the list of active alarms
	`alarm_reset`	Clear alarms for a given time (specified in minutes)
	`alarm_status`	Display the active alarms and whether the alarm cut-off is enabled
	`alarm_test`	Test the alarm subsystem
	`list_alarm_codes`	Translate the Advanced TCA Shelf diagnostic alarm codes
	`get_telco_alarm_state`	Display the state of Telco alarms for a given ATCA Shelf
	`get_telco_capabilities`	Display the Telco alarm states and modes for a given ATCA Shelf

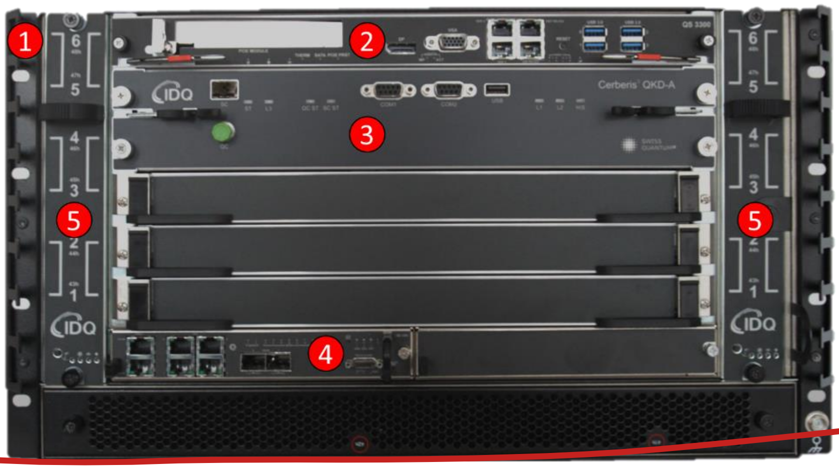
Group	Command	Description
	`set_telco_alarm_state`	Set a given Telco alarm's state
Alerting	`get_pef_config_parameters`	Display the configuration of a given Platform Event Filter (PEF) parameter, such as the configuration of the Event Filter Table and alert strings, as well as whether PEF is enabled/disabled
	`get_snmp_trap_info`	Display the status of SNMP traps and available trap destinations
	`set_pef_config_parameters`	Configure a given Platform Event Filter (PEF) parameter, such as the Event Filter Table and alert strings, as well as whether PEF is enabled/disabled
	`snmp_trap_disable`	Disable SNMP traps for a given channel
	`snmp_trap_enable`	Enable SNMP traps for a given channel
	`snmp_trap_get_address`	Display a list of SNMP trap destinations for a given channel
	`snmp_trap_remove_address`	Remove an SNMP trap destination from a given channel
	`snmp_trap_set_address`	Modify an SNMP trap destination for a given channel
	`snmp_trap_test`	Send a test SNMP trap to a given destination; get/clear status of test alert sent to a given destination
CLI	`cli_commands`	List all available CLI commands
	`cli_options`	Describe the shorthand notation used for common CLI options
	`exit`	Exit the CLI; see `q`
	`get_version`	Display the application and CLI versions
	`help`	Display help for a given command, or display all commands, organized by group
	`q`	Exit the CLI; see `exit`
Cooling	`get_cooling_parameters`	Display the Shelf cooling management parameters
	`get_fan_info`	Display the Fan Tray properties and hot-swap status for a given Fan Tray
	`get_fan_level`	Display a given Fan Tray's current operating speed level
	`list_fan_trays`	Display the locations of all Fan Trays installed in the Shelf
	`set_cooling_parameters`	Configure the Shelf cooling management parameters
	`set_fan_level`	Set the current operating speed level for a given Fan Tray
E-Keying	`get_amc_ptp`	Display AMC e-keying information
	`get_backplane_ptp`	Display backplane point-to-point information
	`get_board_ptp`	Display e-keying information for a given AdvancedTCA Board
	`get_carrier_ptp`	Display a given Carrier's Carrier point-to-point connectivity information
	`get_port_state`	Display link status for a given FRU
FRU Management	`activate`	Activate a given FRU, bring it to M4 state
	`deactivate`	Deactivate a given FRU, bring it to M1 state
	`fru_control`	Change the state of a given FRU's payload
	`fru_reset`	Reset a FRU's management controller
	`get_address_info`	Display a given FRU's address information
	`get_board_info`	Display the configuration and hot-swap information for an ATCA Board at a specified Shelf slot

Group	Command	Description
	`get_device_id`	Retrieve device information from a given FRU
	`get_event_receiver`	Display the location of the event receiver for a given FRU
	`get_fru_activation_policy`	Display the activation policy for a given FRU
	`get_fru_power_levels`	Display a given FRU's power level
	`get_fru_state`	Display the hot-swap information for a given FRU
	`get_fru_temperature`	Display the status of all temperature sensors for a given FRU
	`get_health`	Provide a summary of the FRU alarm and health status
	`list_boards_installed`	Display the list of installed AdvancedTCA Boards
	`list_frus_present`	Display the list of installed FRUs
	`list_device_sdr`	Display the list of SDRs in a given FRU's Device SDR Repository
	`list_sdr`	Display the list of SDRs in the SDR Repository
	`list_fru_storages`	Display the list of FRU Inventory Devices located at a given address
	`read_fru_storage`	Display content from a given FRU inventory device
	`set_event_receiver`	Change the location of the event receiver for a given FRU
	`set_fru_extracted`	Inform the Shelf Manager that a given FRU is no longer installed
	`set_fru_power_level`	Set the FRU power level for a given FRU
	`update_fru_version`	Change the product version number for a given FRU
	`set_fru_current_draw`	Set current draw limit required by FRU
LAN	`get_channel_access`	Display whether a given channel is enabled or disabled, whether alerting is enabled or disabled, and under what system modes the channel can be accessed
	`get_channel_cipher_suites`	Display supported authentication, integrity, and confidentiality algorithms
	`get_channel_info`	Display media and protocol information about a given channel
	`get_lan_config_parameters`	Display a given parameter related to IPMI LAN operation, such as network addressing information
	`get_session_info`	Display session information
	`list_active_sessions`	Display the list of active sessions
	`set_channel_access`	Modify whether a given channel is enabled or disabled, whether alerting is enabled or disabled, and privilege level limit
	`set_lan_config_parameters`	Modify parameters required for IPMI LAN operation, such as the network addressing information
	`set_session_privilege_level`	Request the ability to perform operations at a given privilege level for the active session
LED	`get_led_color_capabilities`	Display information about the leds supported by a given FRU
	`get_led_properties`	Display a list of leds controlled by a given FRU
	`get_led_state`	Display the state of a given LED
	`set_led_state`	Set the state of a given LED
Power	`get_power_feed_info`	Display the power information for a given Power Module
SEL	`clear_sel`	Erase the contents of a given System Event Log
	`get_sel`	Display the contents of a given System Event Log

Group	Command	Description
	get_sel_info	Display information about a given System Event Log
Sensor	get_ipmb0_info	Get FRU IPMB-0 Link status information
	get_ipmb0_status	Get FRU IPMB-0 sensor data
	get_sensor_event_enable	Display sensor event generation capabilities
	get_sensor_hysteresis	Display sensor hysteresis values
	get_sensor_info	Display sensor information
	get_sensor_reading	Display sensor reading
	get_sensor_threshold	Display sensor thresholds
	list_sensors	Display a list of sensors on a FRU
	set_sensor_event_enable	Set sensor event generation capabilities for a given sensor
	set_sensor_hysteresis	Set sensor hysteresis values for a given sensor
	set_sensor_threshold	Set sensor thresholds for a given sensor
System Administration	get_user_access	Display privilege level and channel accessibility for a given user
	list_users	Display the list of available users for the Shelf
	list_users_access	Display channel access information for all users on a given channel for the Shelf
	set_user_access	Configure privilege level and channel accessibility associated with a given user
	set_user_info	Add user, set / change a given user ID’s associated user name or password, and/or enable/disable a given user ID
System Management	chassis_control	Change the power state of the Chassis or issue a diagnostic interrupt
	check_ipmb0_status	Report the status of all IPMB-0 links
	failover	Initiate Shelf Manager failover
	get_chassis_info	Display the Chassis Information record data
	set_chassis_info	Set the Chassis Information record data
	get_shelf_address_info	Display the AdvancedTCA Shelf address
	set_shelf_address_info	Set the Shelf address
	get_address_table	Display the Shelf Address Table
	get_diagnostics	Run diagnostics and display the results
	get_fru_activation_sequence	Display the FRU activation sequence; see get_power_management_info
	get_ip_connection	Display available network interfaces to the AdvancedTCA Shelf
	set_ip_connection	Add or modify available network interfaces to the Shelf
	get_system_guid	Display the globally unique ID (GUID) of a given Shelf

Table 7: Command summary of the QS3201 Shelf Manager

A Cerberis[3] Node consists of multiple modules depicted below.



1. ATCA chassis
2. QNC Blade QS3300
3. Cerberis QKD Blade
4. Switch and Shelf Manager Blade QS3200
5. Fan units

Figure 2: A Cerberis³ Node in an ATCA chassis with QNC Blade, QKD Blade, and Shelf Manager installed.

> **NOTE**
>
> *The QKD transmitter (Alice) and receiver (Bob) blades can be distinguished by their module name imprinted on the front panels of the blade enclosures: QKD-A labels the transmitter, and QKD-B the receiver.*

Dimensions	**Value**
Width	448 mm (19” rack mount)
Height	265.8 mm (6U)
Depth	413.4 mm
Weight	**Value**
Assembled node (includes 2 fan trays, 1 shelf manager, 1 QNC blade, 1 QKD blade)	29 kg
Power	**Value**
Maximum	< 550 W

Table 1: Node Dimensions/Weight

Equipment must first be unpacked, the ATCA chassis and the modules be installed and setup, and connected to optical fibers, network cables, and suitable power supply lines.

- Please refer to Chapter 4 for a description of the requirements on the installation site and its peripherals.
- See Chapter 5 for instructions for the installation of the ATCA chassis and modules, as well as for connecting the fibers, cables and network interfaces to the system.
- See Chapter 6 for instructions for configuring the network settings.

4. Installation requirements and topologies

Before installing the Cerberis³ nodes, it must be assured that the installation site fulfils the environmental and peripheral requirements as outlined in this chapter. The QKD system will operate and interact successfully with the designated network only if those requirements are fulfilled.

4.1.Temperature, humidity, and dust

Cerberis^3 nodes require to be installed in a standard 19" rack in a weather protected site. All sides of the node's ATCA shelf must be easily accessible. To maintain proper cooling, the equipment rack must provide enough airflow to the sides of the shelf. Allow at least two inches of clearance at the air inlets and outlets. The rack must also include enough air ventilation to provide exhaust of a maximum of 3800 W or 13000 BTUs (British Thermal Units) per hour for the device.

The installation site must provide enough cooling to guarantee a constant temperature within the range of +15° C to +25° C at the location of the device, and non-condensing humidity levels within the range of 25% to 75%.

Proper operation of the device at best performance requires a clean and dust-free environment, with a maximum suspension of sand of 30 mg/m^3, of a maximum suspension of dust of 0.2 mg/m^3, and a maximum accumulation of dust by sedimentation of 1.5 mg/(m^{2}h).

Especially fibers for the quantum channel link must be kept clean und dust free.

4.2.Power and ESD protection

Cerberis^3 nodes require to be installed in an ESD protected site that provides proper earthing of the device and at least one power supply socket with an AC voltage of 110 V/220 V at 15 A with an electrical common ground connection. It is to be installed only in a restricted access area and according to the national electrical codes of the specific country. For North America, equipment must be installed in accordance with the US National Electrical Code (NEC) Articles 110–6, 110–17, and 110–18, and the Canadian Electrical Code (CEC), Sections 2-202 and 2-308.

Cerberis^3 nodes must be handled and used only while it is properly earthed.

4.3.Fiber and network peripherals

Each Cerberis^3 node requires access to fiber and Ethernet network peripherals and can be configured to adapt to different situations and topologies. In total, the following links must be facilitated between the two Cerberis^3 nodes:

- An optical quantum channel link without active components and with loss below specified value for the system,
- A bidirectional optical QKD-Service channel link for QKD clock synchronization and post-processing,
- An optical or electrical, bidirectional QNC-Service channel link for key management.

4.3.1. Required fibers

In the standard configuration, a dark standard single mode fiber link without any additional data or service traffic, optical signals, optical amplifiers, or other active optical elements (switches, modulators, …) is required for the system's quantum channel. The system's service channels require at least one additional bidirectional fiber link that can be realized either over one single fiber or over multiple separate fibers. Additional fiber links or Ethernet links may be required, depending on customer network specificities.

For single-fiber configuration using wavelength multiplexing, please contact ID Quantique.

The performance of the Cerberis^3 point to point system largely depends on the optical attenuation of the designated quantum channel fiber link that is required to be below the specified maximum for the specific system (12 dB for standard system).

The optical fiber link(s) for the service channels must facilitate at least 2.5 Gbps (Gigabit per second) bi-directional optical communication in the C-band (wavelength between 1525–1565 nm) in compliance with the ITU G.694.1 standard for DWDM spectral grids. The total optical attenuation for the service channel fiber link must guarantee error free operation of the implemented SFP transceiver modules, i.e. below their specified transmission budget. The receiver sensitivity of the provided standard SFP modules is specified with -28 dBm, which is the minimum necessary power of the modules to guarantee error-free communication.

IMPORTANT NOTE

Starting from OS release 3.0.0 there is "virtually" no limitation on the fiber length different between Service Channel and Quantum channel. The fiber difference between these two channels can be compensated for more than 200km difference.

4.3.2. Required network peripherals.

During the installation process, the networking address information in Table 2 will be required and referred to. If not specified prior to purchasing the Cerberis^3 system, each system parts will be pre-configured with a default setting.

Network settings must be configured for each node:

- **The Switch (M1/S1)**: This address corresponds to the Switch front panel ethernet ports GbE0-3 for Management (SNMP, syslog) and internode communications. It must be in same subnet as the QNC and QKD Blades.
- **The QNC-CPU (M2/S2)**: This address must be in same subnet as the QKD Blade and switch. It is used to connect to the QNET Shell. It must also be given to the SNMP client to obtain the SNMP monitoring information. The local QKD Blades also need to be configured to know this IP address and to be able to communicate with it.
- **The QKD-CPU (A3/B3)**: This address must be in same subnet as the QNC and switch. It is used to connect to the QNET shell. The local QNC needs to be configured to know this IP address and to be able to communicate with it.
- **The QNC key interface to the encryptors implementing ETSI interface (M4+M5/S4+S5)**: This address is used to request keys from the QNC and must be given to the encryptors that request the keys from the QNC.
- **The interfaces of the encryptors implementing ETSI interface (M6+M7/S6+S7)**: This is the address of the encryptors that request keys from the QNC.
- **The syslog server (M8/S8)**: This address must be given to the syslog client for receiving alarms. The address must in the same subnet as QNC and switch.
- **The Shelf-Manager BMC (M9/S9)**: This address is only required when updating the BMC via the shelf-manager or switch.

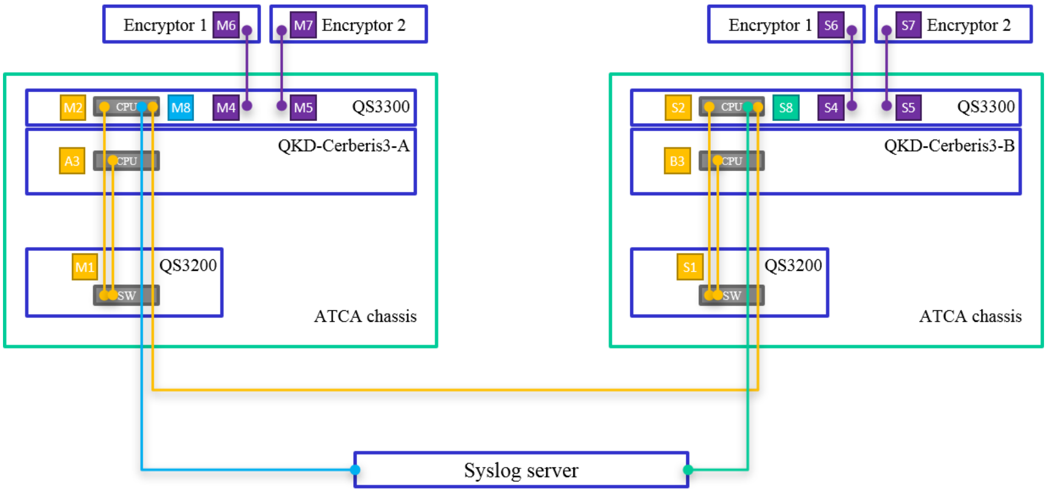


Figure 3: Cerberis^3 exemplary setup topology (scenario2).

Node 1

ID	Description	IP address	Netmask	Gateway
M1	Switch	192.168.10.100	255.255.255.0	0.0.0.0
M2	QNC-CPU	192.168.10.101	255.255.255.0	0.0.0.0
A3	QKD-CPU	192.168.10.102	255.255.255.0	0.0.0.0
M4	QNC-GbE2	192.168.20.2	255.255.255.252	0.0.0.0
M5	QNC-GbE3	192.168.30.3	255.255.255.252	0.0.0.0
M6	Encryptor 1	192.168.20.x	255.255.255.252	0.0.0.0
M7	Encryptor 2	192.168.30.x	255.255.255.252	0.0.0.0
M8	Syslog	192.168.10.200	255.255.255.0	0.0.0.0
M9	ShMM-BMC	0.0.0.0	0.0.0.0	0.0.0.0

Node 2

ID	Description	IP address	Netmask	Gateway
S1	Switch	192.168.10.105	255.255.255.0	0.0.0.0
S2	QNC-CPU	192.168.10.106	255.255.255.0	0.0.0.0
B3	QKD-CPU	192.168.10.107	255.255.255.0	0.0.0.0
S4	QNC-GbE2	192.168.20.2	255.255.255.252	0.0.0.0
S5	QNC-GbE3	192.168.30.3	255.255.255.252	0.0.0.0
S6	Encryptor 1	192.168.20.x	255.255.255.252	0.0.0.0
S7	Encryptor 2	192.168.30.x	255.255.255.252	0.0.0.0
S8	syslog	192.168.10.205	255.255.255.0	0.0.0.0
S9	ShMM-BMC	0.0.0.0	0.0.0.0	0.0.0.0

Table 2: Cerberis^3 exemplary address scheme information.

Following are the two possible connection scenarios between QKD system and encryptors.

<u>Scenario 1:</u> QKD systems and Encryptor share the same subnet. (192.168.10.0/24)
Encryptors are connected to the ShMM switch ports (M1/S1). The Frontpane ports are not connected (M4, M5/S4,S5).
Encryptors are configured to retrieve keys using QNC management IP.

NOTE

KEMS has defined an “any/all” interface to the QNC management IP. Provider and Consumer Associated KMS configurations reference this “any/all” management IP. No “KeyInternal” interfaces are defined or referenced.

<u>Scenario 2:</u> QKD systems and Encryptor are on different subnets. (192.168.10.0/24 – QKD) (192.168.20.0/24 – Encryptor)
Encryptors are connected to the Frontpane port (M4,M5/S4,S5 ,Frontpane subnet 192.168.20.0/24)
Encryptors are configured to retrieve keys using QNC Frontpane IP.

NOTE

KEMS also has defined a “KeyInternal” KMS IP address to the Frontpane IP. Provider and Consumer Associated KMS configurations reference the “KeyInternal” Frontpane IP.

4.4.Verification of the installation requirements

1. Verify that the installation site(s) is weather protected.
2. Verify that the installation site(s) provides a constant temperature within the specified operation temperature range of +15° C to +25° C.
3. Verify that the installation site(s) provides non-condensing relative humidity levels within the specified QKD system operation range of 25% to 75%.
4. Verify that the installation site(s) limits the suspension of sand to a maximum of 30 mg/m^3, of dust to a maximum of 0.2 mg/m^3, and of dust accumulation by sedimentation to a maximum of 1.5 mg/(m^{2}h).
5. Verify that the installation site(s) provides for each ATCA shelf at least one socket for AC 110 V/220 V/15 A power supply with an electrical common ground connection.
6. Verify that the installation site(s) have Ethernet routers for network connection between the 2-installation site(s).
7. Verify that the installation site(s) provides access to a dark single mode fiber between both installation site(s) without any additional traffic.
8. Verify that the dark single mode fiber for the QKD quantum channel has an optical attenuation below the specified maximum for the system.
9. Verify that the dark single mode fiber for the QKD quantum channel is free of any optical amplifier or other active optical elements (e.g. switches, modulators…).
10. Verify that the installation site(s) provides access to a second, bidirectional fiber link for the service channels between both installation site(s).
11. Verify that the second fiber link facilitates a 2.67 Gbps (Gigabit per second) bi-directional optical communication channel in the C-band (wavelength between 1525–1565 nm) in compliance with the ITU G.694.1 standard for DWDM spectral grids.
12. Verify that the fiber length difference between the quantum channel fiber link and the service channel fiber link (from Transmitter Cerberis^3 node to Receiver Cerberis^3 node) is below the maximum limit of 15 km.
13. Verify that the second fiber link has a total optical attenuation that guarantees error free operation of the implemented SFP transceiver modules, i.e. below their transmission budget.

4.5.Installation topologies

Cerberis XG systems can be deployed in any network configurations including point-to-point, relay for longer distances, ring, or star topologies, depicted in Figure 4. At each QKD network node, the embedded Key Management System (KMS) software arbitrates the key distribution between QKD and key consumers and performs add/drop or forward functions depending on the recipient’s location.

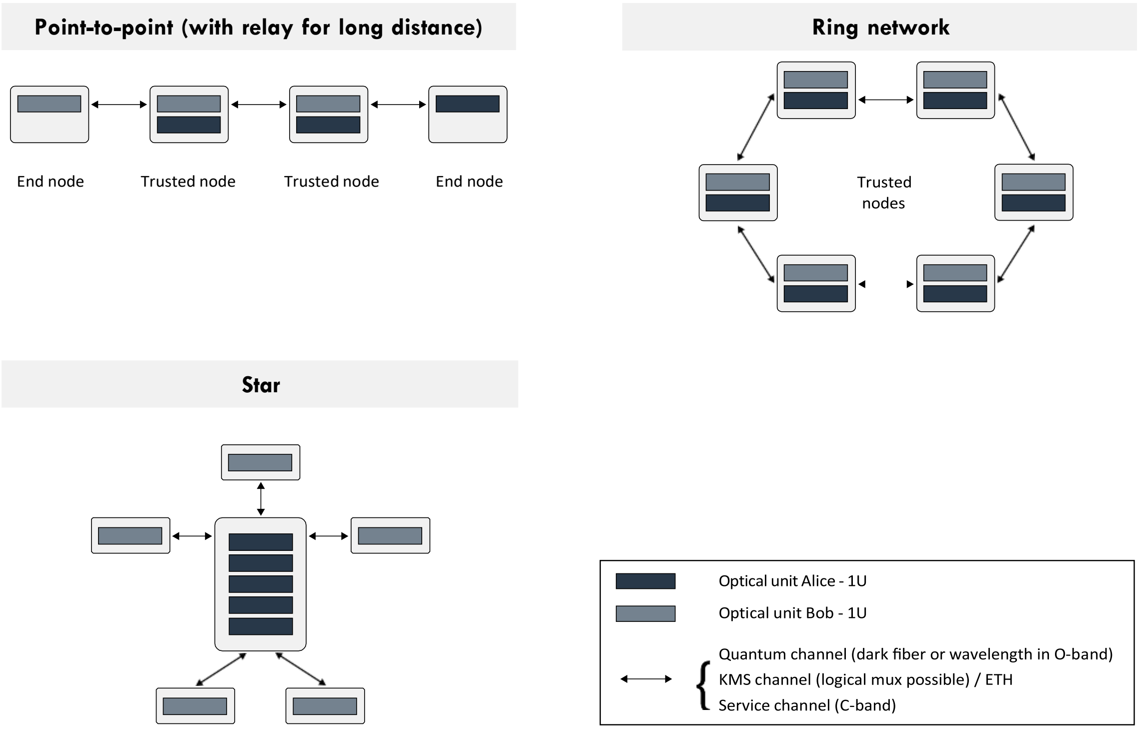
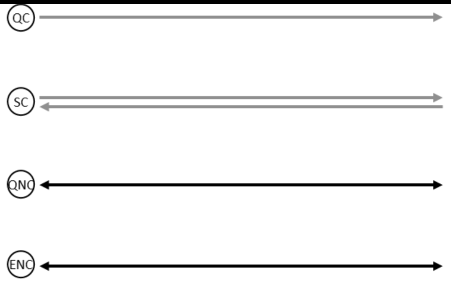

Point-to-point (with relay for long distance)
End node
Trusted node
Trusted node
End node
Ring network
Trusted nodes
Star
Optical unit Alice - 1U
Optical unit Bob - 1U
Quantum channel (dark fiber or wavelength in O-band)
KMS channel (logical mux possible) / ETH
Service channel (C-band)

Figure 4 Cerberis XG solution topologies

As starting point, a selection of the most common point-to-point topologies is listed in Table 3 below. There, (QC) denotes the Cerberis XG QKD quantum channel, (SC) denotes the QKD service channels, and (ENC) the encryptor channels. Channels colored in grey refer to optical fiber channels over standard single mode fibers (SMF-28), and channels in black refer to channels over Ethernet copper cables.

#	Topology	Comments
1a		• 3 fibers and 2 copper connections required • QKD Service channel wavelengths can be chosen arbitrarily and independently in the ITU C-band • Quantum channel wavelength in the ITU C-band

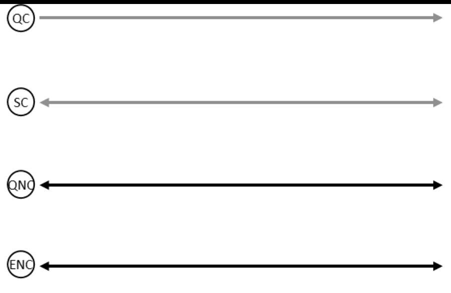
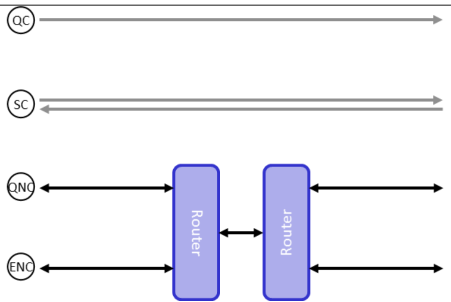
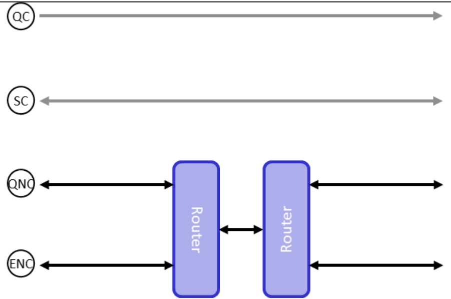
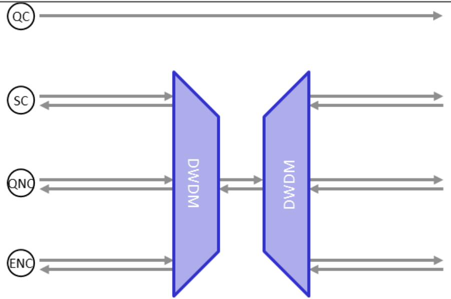
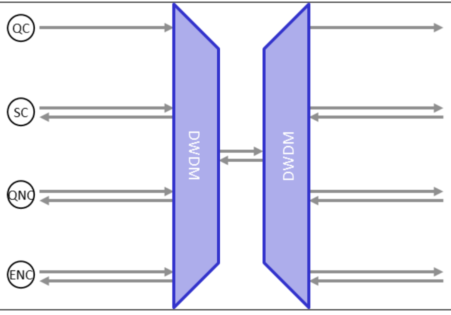
#	Topology	Comments
1b		• 2 fibers and 2 copper connections required • QKD Service channel via optical bidirectional (BiDi) SFP module • QKD Service channel wavelength in one direction is in the ITU C-band, in the opposite direction it is in the ITU O-band • Quantum channel wavelength can be chosen in the ITU C-band, or alternatively in the ITU O-band
2a		• 3 fibers and 1 copper connection required • QKD Service channel wavelengths can be chosen arbitrarily and independently in the ITU C-band or O-band • Quantum channel wavelength can be chosen in the ITU C-band
2b		• 2 fibers and 1 copper connection required • QKD Service channel via optical bidirectional (BiDi) SFP module • QKD Service channel wavelength in one direction is in the ITU C-band, in the opposite direction it is in the ITU O-band • Quantum channel wavelength can be chosen in the ITU C-band, or alternatively in the ITU O-band
3a		• 3 fibers required • All classical channel wavelengths must be in a designated ITU DWDM channel • Typically, bidirectional channel pairs allocate the same ITU channel • Quantum channel wavelength can be chosen in the ITU C-band
3b		• 2 fibers required • All classical channel wavelengths must be in a designated ITU DWDM channel in the C-band • Typically, bidirectional channel pairs allocate the same ITU channel • **Quantum channel wavelength must be at 1310 nm** • QKD system must be purchased with narrow-band filtering option

Table 3: Recommended topology options for the Cerberis^3 Node.
QC denotes the QKD quantum channel, SC the QKD service channels, QNC the QNC service channels, and ENC the encryptor channels. Channels colored in grey signify optical fiber channels, and black channels over Ethernet copper cables.

NOTE

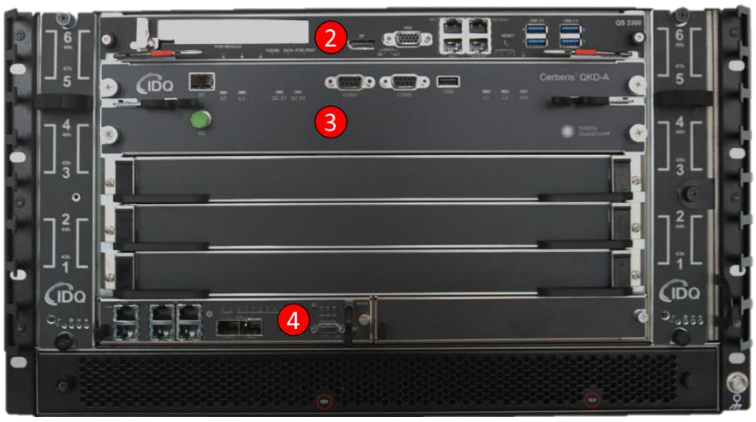
With standard supplied equipment (see section 2.1) and a pair of encryptors, the topology 1a can be implemented in a back to back setup for lab test.

ℹ *NOTE*

The Cerberis3 QKD system in configuration 3b (with quantum channel at 1310nm and narrow band filtering option), allows the multiplexing of the platform's classical channels as well as some external classical channels (ITU DWDM channel in the C-band). Please contact ID Quantique for more details on the total number of classical channels allowance and launch power per channel.

5. Cerberis3 QKD node installation instructions

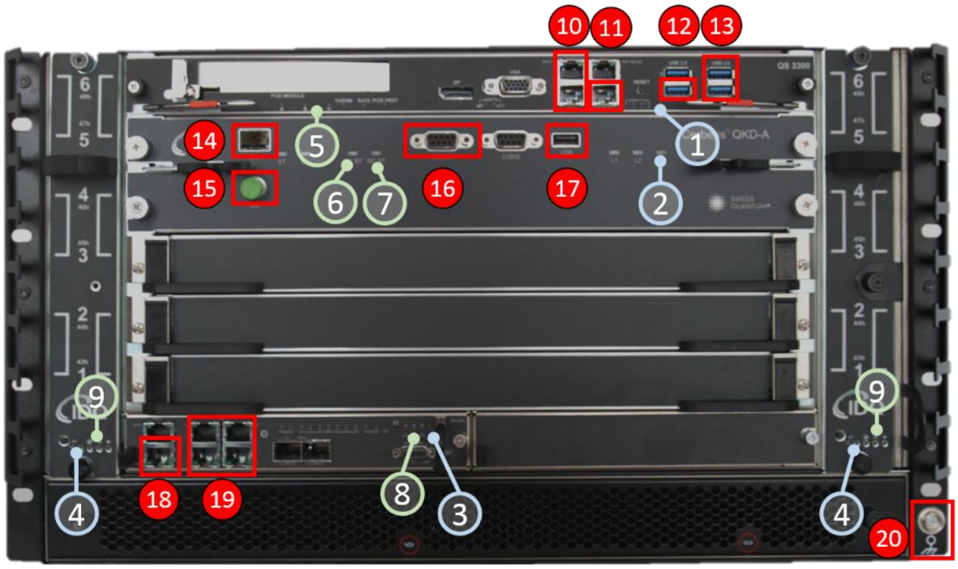
The different modules of a Cerberis^3 node are recommended to be installed in the ATCA chassis following the configuration shown in Figure 5.



Slot	Module
Slot #6	QNC Blade ②
Slot #5	QKD Blade ③
Slot #4	
Slot #3	Empty
Slot #2	Empty
Slot #1	Empty
ShMM #1	Shelf Manager and Switch Blade ④
ShMM #2	Empty

Figure 5: Recommended ATCA slots configuration for a Cerberis^3 node.

The most relevant interfaces and status indicators of a Cerberis^3 node are indicated in Figure 6 below and explained in more detail in the following sections.



ATCA Hot-Swap LEDs

1. QNC ATCA H/S LED
2. QKD ATCA H/S LED
3. ShMM ATCA H/S LED
4. Fan units ATCA H/S LED

Alarm and Status indicators

5. QNC Alarm LEDs
6. Quantum Channel status LED
7. Service Channel status LED
8. ShMM/Switch Alarm LEDs
9. Fan Units Alarm LEDs

Interface ports

10. QNC ETSI Key interfaces
11. QNC Serial Management port
12. QNC USB port
13. QNC IDQ3P Key interfaces
14. QKD SFP module slot
15. QKD Quantum channel port
16. QKD Serial Management port
17. QKD USB port
18. ShMM Serial port
19. ShMM/Switch Ethernet ports

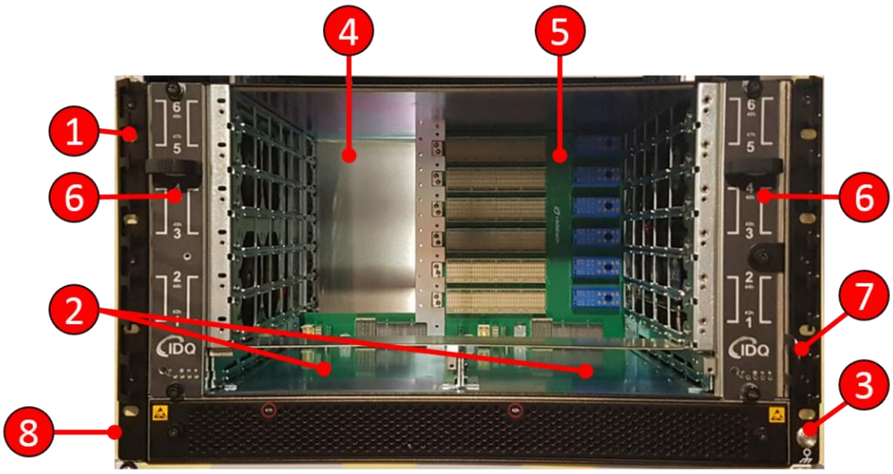
ESD

20. ESD Wrist band connector

Figure 6: Interface ports and status indicators on the front of a Cerberis^3 node.

5.1. ATCA chassis

5.1.1. ATCA chassis description



#	Component	Description
1	Mounting flanges	Mounting flanges on each side to be fastened to the19-inch rack.
2	Shelf Manager slots	Slots for one or two shelf manager(s), controlling and managing the shelf.
3	ESD terminal	Front ESD wrist strap terminal.
4	Card cage	Portion of the shelf that holds the blades that are plugged into the backplane. Mechanically compliant with all aspects of PICMG 3.1.
5	Backplane	Supports up to 6 ATCA-compliant front boards, and the complementary rear transition modules (RTM).
6	Fan tray	Two Fan trays cool the shelf.
7	Air filter tray	Keeps the airflow free of dust and particles.
8	Power supplies	Up to 4 integrated swappable 1300 W AC power supplies (rear side not visible)

Figure 7: ATCA chassis components - Front view

5.1.2. Mounting the chassis in the 19” rack

The chassis is provided with mounting flanges on either side of the front of the chassis, appropriate for standard 19” racks. Prior for rack mounting, confirm that the rack is stable so that the weight of the chassis does not cause it to tip over. The rack mounting is to be carried out by at least two technicians. Eight 6x10 screws are needed to mount the chassis on the rack.

1. Install support L brackets on the rack.
2. Two people are required to lift and insert the chassis into the rack, one on each side of the chassis, grasping the base on the front and the back. With a person on each side of the chassis, lift it and fit it onto the L brackets in the rack. The chassis must be leveled and not positioned at an angle in the rack. The rack’s doors must be able to be closed.
3. While one person is holding the chassis in place, the second person fastens the chassis to the rack rails using eight screws (not provided), four on each side of the chassis or as appropriate for your rack type.

5.1.3. Connecting the chassis to earth

The chassis includes a two-hole earthing lug. 6 AWG grounding cable is to be used with this lug. Grounding design must comply with the country or local electrical codes. In the United States, grounding must comply with Article 250 of the NEC unless superseded by local codes.

> ⚠ **WARNING**
>
> *An earthing connection is essential before connecting the power supply.*

To connect the earthing of the ATCA chassis:

1. On the rear of the chassis, locate the earthing connection on the right (see Figure 8 point (1)).
2. Using the appropriate wrench, unfasten the two nuts and remove the lug.
3. Crimp 6 AWG grounding wire to the lug.
4. Return the lug to its place on the rear-right of the chassis and refasten the screws.
5. Connect the ground wire to the appropriate ground connection to the building's earthing system.

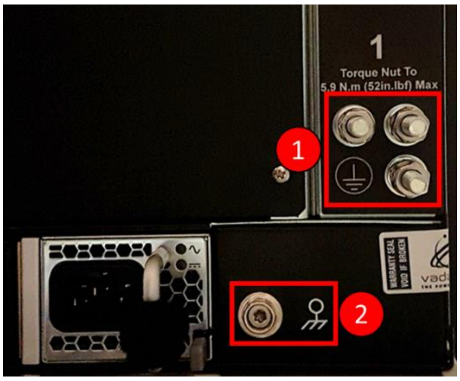


Figure 8: Rear grounding lug (1) and rear-connector for the ESD wrist band (2).

5.1.4. Preparing of the ESD protection

Electronic components on printed circuit boards are extremely sensitive to static electricity. Normal amounts of static electricity generated by clothing can damage electronic equipment. To reduce the risk of damage due to electrostatic discharge when installing or servicing electronic equipment, use anti-static grounding straps and mats.

The chassis contains two (ESD) grounding sockets, one at the front of the chassis and one in the rear of the chassis. Persons involved in the shelf installation must wear an ESD Wrist Strap and attached to one of these grounding sockets.

To prepare ESD protection:

1. Locate the ESD grounding sockets on the shelf. Refer to Figure 6 for the location of the Front ESD point (19), and Figure 8 for the Back ESD point (2).
2. Attach a wrist strap for electrostatic discharge (ESD) and connect it to one of the ESD grounding points on the shelf using a banana plug or an alligator clip.

5.1.5. Connecting the power source

For power cables, use a C15 type connector with a 15 A cable. To connect to AC power:

1. Check circuit breaker at the mains is off.
2. Insert an AC power cable into each AC power inlet on the rear-bottom of the shelf.

5.1.6. Powering the chassis up

If applicable, share the power cables among more than one electrical phase to ensure the supply of power should one phase fail. To power up the shelf:

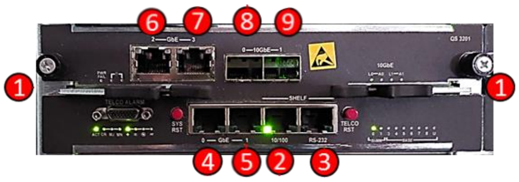
1. Connect the mains to the power line.
2. Wait up to one minute for the shelf to stabilize until all the Hot-Swap (H/S) LEDs on the front panel turn off (see Figure 6).
3. Check that the LEDs of each shelf component appear in normal mode (see Figure 6).

5.2.QS3201 ShMM+Switch Blade

5.2.1. Description

The QS3201 Shelf Manager and Switch blade combines the functions of an PICMG 3.0 compliant ATCA Shelf Manager with an integrated Managed Layer 3 GbE Switch on the same module. Normally, it comes pre-installed in the ATCA chassis upon delivery.

The Shelf Manager board's front panel contains the displays and interfaces as shown in Figure 9.



Number	Name	Description
①		Hot-swap handle
②	Shelf 10/100	10/100 Shelf Manager interface
③	RS-232	Serial Shelf Manager interface through RJ-45 connector
④	GbE 0	Gigabit Ethernet interface 0
⑤	GbE 1	Gigabit Ethernet interface 1
⑥	GbE 2	Gigabit Ethernet interface 2
⑦	GbE 3	Gigabit Ethernet interface 3
⑧	10GbE 0	10 Gigabit Ethernet interface 0 through SFP+
⑨	10GbE 1	10 Gigabit Ethernet interface 1 through SFP+

Figure 9: Shelf Manager Front Panel interfaces.

5.2.2. Installing the QS3201 ShMM+Switch Blade

The following procedure describes the installation of the Shelf Manager and Switch blade in a hub slot and assumes that your system is powered up. If your system is powered down, you can disregard the blue LED and thus skip its respective step. In this case what follows is a purely mechanical installation.

1. Visually inspect the blade and backplane connectors for damage or bent pins before attempting to insert a board. If any connector damage or pin damage in observed, stop before inserting the blade and contact IDQ.
2. Pull the hot swap handles ① to its open position towards you.
3. Insert the module into the Shelf guide rails and push the front panel firmly until it is fully seated into the connector. If the card does not go fully in, do not force it, and instead remove it and check for proper orientation or obstructions.

4. If your shelf is powered up, as soon as the blade is connected to the backplane power pins, the blue LED should go to solid ON.
5. Push the hot swap handles to their closed position (towards the shelf). The Blue LED should blink for a short duration indicating that the blade announces its presence to the shelf management controller, and then goes to solid OFF. The green LED should be solid ON to indicate that the payload power was applied.
6. Wait until the blue LED is switched off, then tighten the face plate screws by turning it clockwise to secure the blade to the shelf.

5.2.3. Removing the ShMM+Switch Blade

This section describes how to remove the QS3201 Shelf Manager and Switch blade from an ATCA chassis. The module should only be removed from a running shelf when the Blue H/S LED is solid ON.

1. Loosen the cap screw by turning it anticlockwise.
2. Pull the hot swap handles ① to their open position towards you.
3. The Blue LED should blink for a short duration and then go solid ON.
4. Once the Blue H/S LED is ON, pull the module straight out firmly to remove the module from the shelf.

> ⚠ WARNING
>
> *Important: Removing the module before the Blue H/S LED is on may cause severe damage to the device.*

5.2.4. Setting up the connections of the QS3201 ShMM+Switch blade

1. **Node connection**: Connect the QS3201 ShMM+Switch blade to the Ethernet network by plugging the RJ45 connector from the network into GbE0 sockets on the front panel (marked red in Figure 10)
   1.1. This cable links the QNC to remote QNCs eventually through a network equipment for inter node connection.
   1.2. This cable allows also remote access for maintenance and configuration eventually through a network equipment for remote access management.

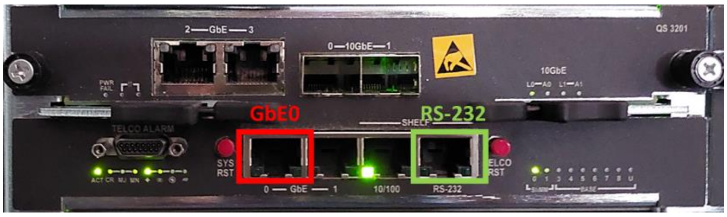


Figure 10: ETH1 Front panel socket of the Switch blade.

The AdvancedTCA Shelf Command Line Interface (CLI) provides an interface to an AdvancedTCA Shelf Manager. The CLI is based on the IPMI 2.0, AdvancedTCA™ PICMG 3.0, and PICMG® AMC.0 R2.0 specifications. It uses a subset of commands that can be accessed directly or through a higher-level Management Application. Administrators can access the CLI though a telnet session, SSH, or the VadaTech AdvancedTCA Shelf Manager serial port. Using the CLI, users can access information about the current state of the Shelf, obtain information such as the FRU population, or monitor alarms, power management, current sensor values, and the overall health of the Shelf. The interface can also be used to update Shelf-configurable parameters.

The Shelf Manager is accessible via the RS-232 serial management port or either of the two Ethernet ports Any of these interfaces can be used to log in to the Shelf Manager. Once connected to the system, users can manage and monitor the state of the Shelf Manager.

5.2.5. Setting up the serial connection to the QS3201 ShMM+Switch blade through RS-232

If the IP addresses of the ShMM and Switch blade is not configured / not configured properly for its network, logging onto the console the first time must be done via the serial port console.

To change the IP addresses of the ShMM and Switch blade from the default values the first time, connect to the console port on the front panel of the ShMM and Switch blade (marked green in Figure 10). The shelf manager is accessible by a serial RS-232 interface through a RJ-45 connector.

1. Use the Y cable from port 1 to port 2, with port 1 connected to the RJ-45 port labelled RS-232 and port 2 connected to a Serial to USB converter.
2. Connect the USB converter to the USB port of the PC.
3. Start a terminal program and set the following parameters for the serial connection:
    a. Baud speed: 115200
    b. Data bits: 8
    c. Stop bits: 1
    d. Parity: None
4. Open the serial connection.
5. In the appearing terminal window press the ENTER key once to see the login prompt.
6. Login. The default username and password for connections are *root* and *root*, respectively.

Once the Shelf Manager IP address has been configured properly as described in sec. 5.5.2, the user can communicate with the Shelf Manager over the network.

5.3.QNC Blade QS3300

5.3.1. Installing the QNC Blade

The following procedure describes the installation of the QNC Blade in the ATCA chassis and assumes that your system is powered up. If your system is powered down, you can disregard the blue LED and thus skip its respective step. In this case what follows is a purely mechanical installation.

Before proceeding with the following installation steps, visually inspect the QNC blade and backplane connectors for damage or bent pins before attempting to insert the board. If any connector damage or pin damage in observed, stop before inserting the blade and contact IDQ.

1. Insert the QNC Blade into the chassis by placing the left and right edges of the blade in the card guides of the shelf. Make sure that the guiding module of shelf and blade are aligned properly.

> ⚠ *WARNING*
>
> *Important: Only touch the blades at the metallic enclosure and avoid contact with the circuitry or any electronic part!*

2. Apply equal and steady pressure to the QNC blade to carefully slide the blade into the shelf until you feel resistance. Continue to gently push the QNC blade until the blade connectors engage.
3. Squeeze the lever and the latch together and hook the lower and the upper handle into the shelf rail recesses (see Figure 11). If an abnormal amount of force is needed during blade insertion to insert the blade into the slot, please extract the QNC blade, then carefully inspect the blade and slot for problems to prevent damage.
4. If your shelf is powered up, as soon as the blade is connected to the backplane power pins, the blue LED on the QNC Front Panel is illuminated (see Figure 11). When the blade is completely installed, the blue LED starts to blink. This indicates that the blade announces its presence to the shelf management controller.

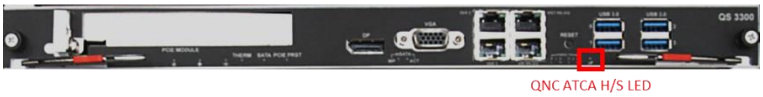


Figure 11: Location of the Blue LED for the QNC blade indicating the ATCA hot-swap (H/S) state.

5. Wait until the H/S blue LED is switched off (see Figure 11), then tighten the face plate screws which secure the blade to the shelf. When the blue LED is switched OFF and the green LED "OK" is switched ON, this indicates that the payload has been powered up and that the blade is active.

5.3.2. Setting up the serial connection through USB

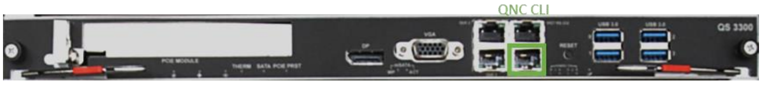


Figure 12: The QNC USB front panel connection to the serial interface.

1. Use the Y cable from port 1 to port 2, with port 1 connected to the RJ-45 port labelled x86 RS-232 (marked green in Figure 12) and port 2 connected to a Serial to USB converter.
2. Connect the USB converter to the USB port of the PC.
3. Start a terminal program and set the following parameters for the serial connection:
   - Baud speed: 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow Control: None
4. Open the serial connection. In the appearing terminal window press the ENTER key once to see the login prompt.
5. Refer to sec. 6.3 for the available commands.

5.3.3. Connecting to the QNC blade via SSH through an Ethernet connection

1. Connect a PC with a SSH client terminal (e.g. Putty) to the same network as the QNC.
2. Start the SSH terminal and connect with the IP address of the QNC.
3. Refer to sec. 6.3 for the available commands.

```
<command> --help.
```

5.3.4. Connecting an Encryptor via Ethernet to the QS3300 QNC blade

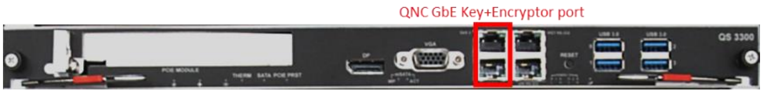


Figure 13: The QNC Front panel connections for the Key and Encryptor interfaces.

1. Connect the QNC-Encryptor cable to the GbE 2 Ethernet interface on the top left of the QNC Front panel (marked red in Figure 13).
2. Connect the other end of the QNC-Encryptor cable to the RJ45 Key interface port of the consumer device, or equivalently to an intermediate network hub.

5.4.QKD Blade

5.4.1. Installing a QKD Blade

Before proceeding with the following installation steps, visually inspect the QKD blade and backplane connectors for damage or bent pins before attempting to insert the board. If any connector damage or pin damage in observed, stop before inserting the blade and contact IDQ.

1. Ensure that the left and right ejector handles are in the outward position by squeezing the lever and the latch together (see Figure 14).

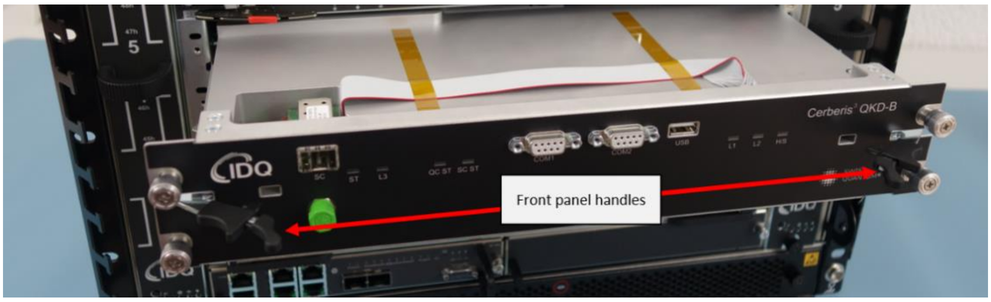


Figure 14: Proper position of the front panel handles before inserting the blade.

2. Insert the QKD blade into the chassis by placing the left and right edges of the blade in the card guides of the shelf. Make sure that the guiding module of shelf and blade are aligned properly.

> ⚠ *IMPORTANT*
>
> *Only touch the blades at the metallic enclosure and avoid contact with the circuitry or any electronic part!*

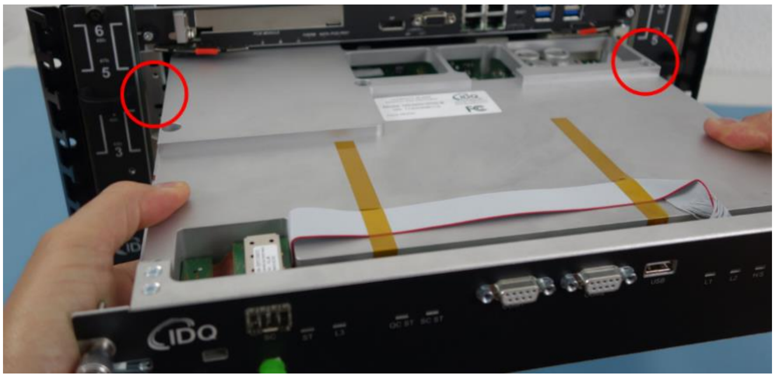


Figure 15: Inserting the QKD blade by aligning the ridges at the sides of the blade with the rails of an ATCA shelf slot.

3. Apply equal and steady pressure to the QKD blade to carefully slide the blade into the shelf until you feel resistance. Continue to gently push the QKD blade until the blade connectors engage.
4. Ensure that the left and right ejector handles are in the outward position by squeezing the lever and the latch together (see Figure 16).

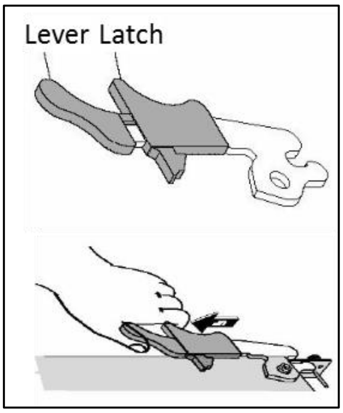


Figure 16: Using the ATCA Front panel handle.

5. Hook the left and the right handle into the shelf rail recesses (see Figure 17). If an abnormal amount of force is needed during blade insertion to insert the blade into the slot, please extract the QKD blade, then carefully inspect the blade and slot for problems to prevent damage.

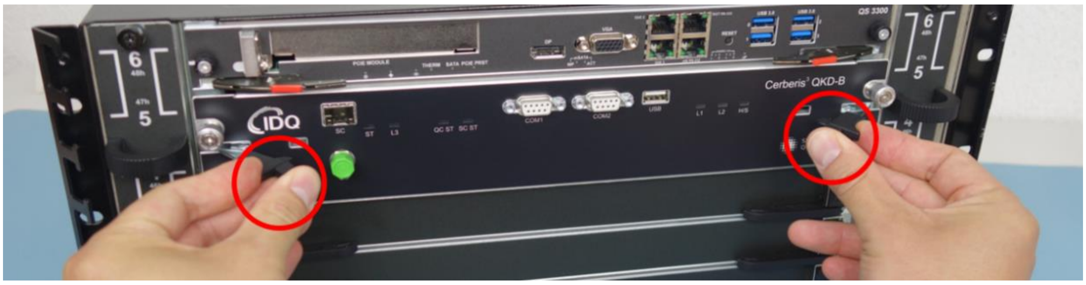


Figure 17: Closing the front panel handles.

6. If your shelf is powered up, as soon as the blade is connected to the backplane power pins, the blue LED on the QKD Front Panel is illuminated. When the blade is completely installed, the blue LED starts to blink (see Figure 18). This indicates that the blade announces its presence to the shelf management controller.

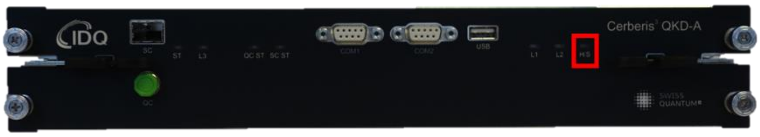


Figure 18: Location of the Blue LED for the QKD blade indicating the ATCA hot-swap (H/S) state.

7. Wait until the blue LED is switched off, then tighten the face plate screws which secure the blade to the shelf. When the blue LED is switched OFF, this indicates that the payload has been powered up and that the blade is active.

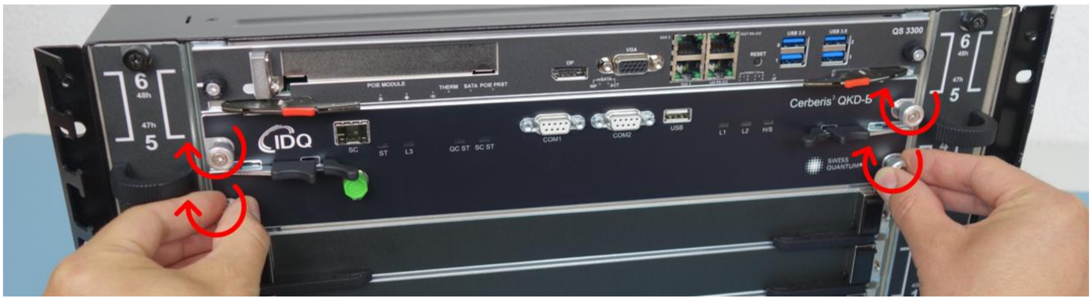


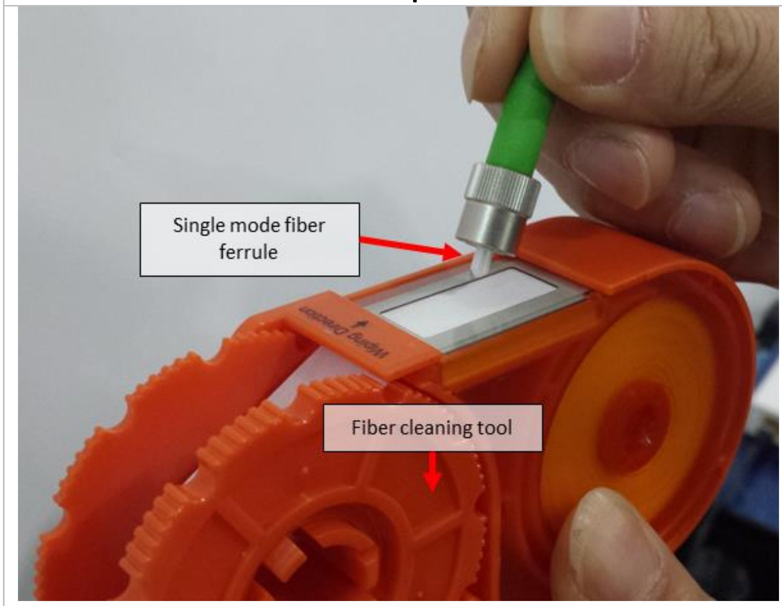
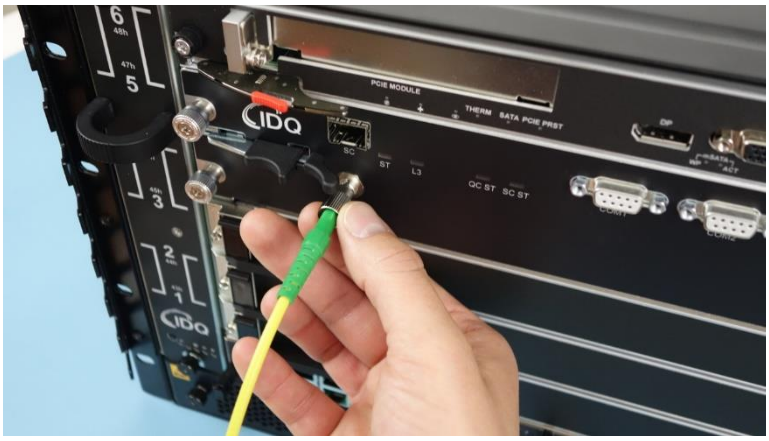
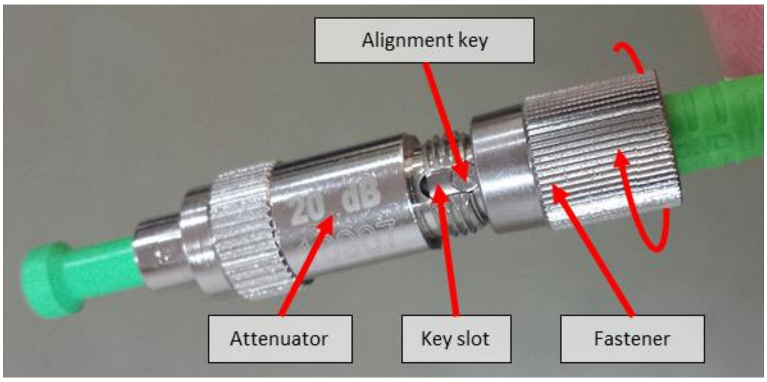
Figure 19: Tightening the face plate screws.

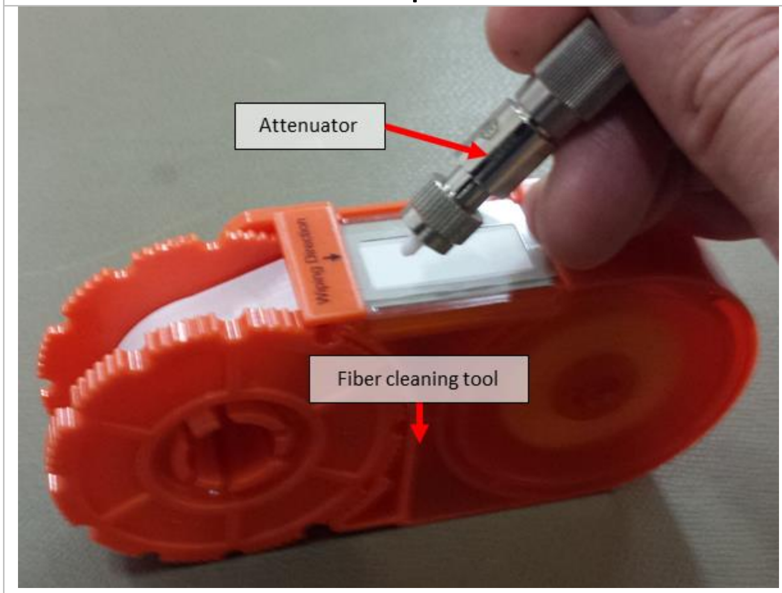
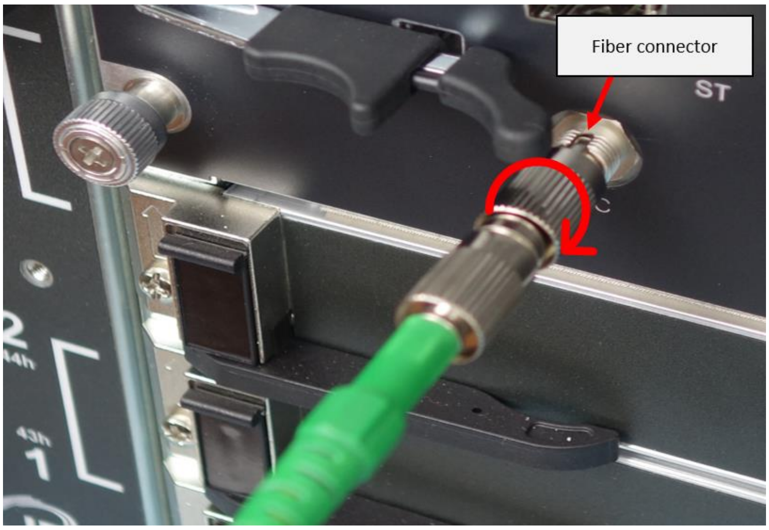
> **NOTE**
>
> *After the system is active, about two minutes are necessary for the system to boot and initialize and be accessible through management port or network port*

5.4.2. Setting up the QKD Quantum Channel connection

Follow the steps below to set up the optical connections of the QKD Blade.

> **IMPORTANT**
>
> *Optical components for the Quantum channel should be perfectly cleaned and handled with care, otherwise system will not operate properly!*

Step	Description
 Single mode fiber ferrule Fiber cleaning tool Wiping Direction	Remove the protective cap from the FC/APC connector end of the single mode fiber patch cord and clean the exposed fiber ferrule end by wiping it twice on the cleaning tool. Only wipe in the direction depicted on the cleaning tool!
	*Only for Transmitter (Alice) blade:* Carefully connect the fiber to the front panel fiber connector. Tighten the fastener of the fiber attenuator by turning it clockwise. ***Important: Verify that the alignment key is well aligned with the alignment slot of the connector!***
 Alignment key Attenuator Key slot Fastener 20 dB	*Only for Receiver (Bob) blade:* Unscrew the protective cap from the optical attenuator by turning it counterclockwise and carefully connect the optical attenuator to the patch cord fiber ferrule. tighten the fastener of the fiber patch cord by turning it clockwise. ***Important: Verify that the alignment key of the fiber pigtail is well aligned with the alignment slot of the attenuator!***

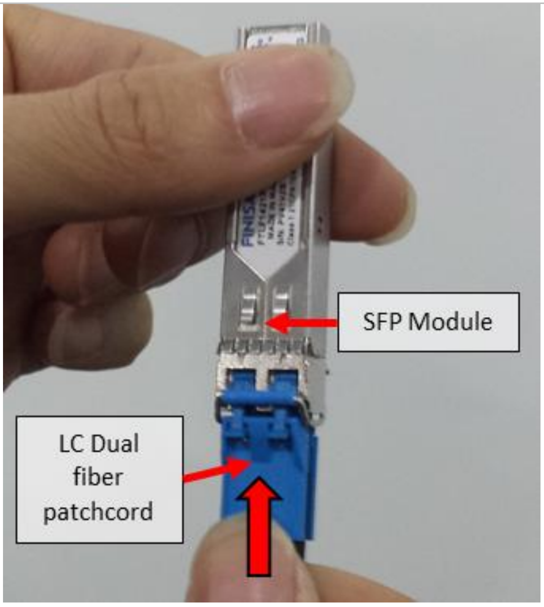
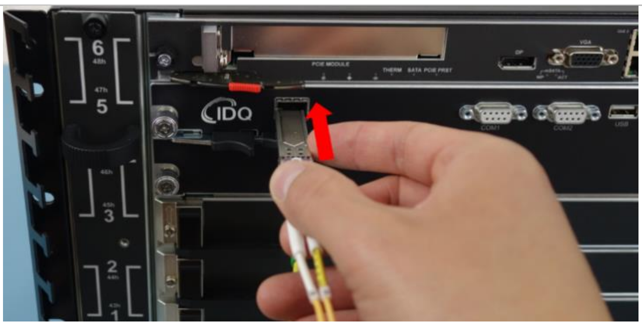
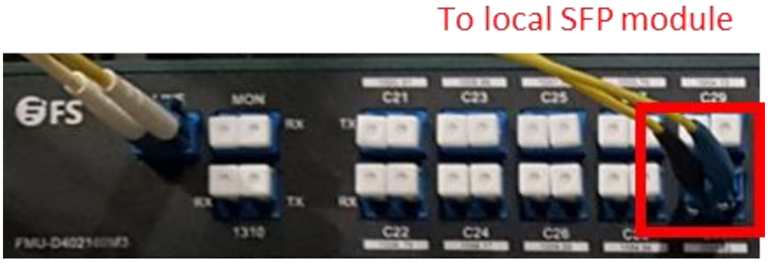
Step	Description
	*Only for Receiver (Bob) blade:* Remove the protective cap from the attenuator and clean the exposed fiber ferrule end by wiping it twice on the cleaning tool. Only wipe in the direction depicted on the cleaning tool!
	*Only for Receiver (Bob) blade:* Remove the protective cap from the Front panel fiber connector by turning it counterclockwise. Carefully connect the optical attenuator to the front panel fiber connector. Tighten the fastener of the fiber attenuator by turning it clockwise. ***Important: Verify that the alignment key is well aligned with the alignment slot of the connector!***

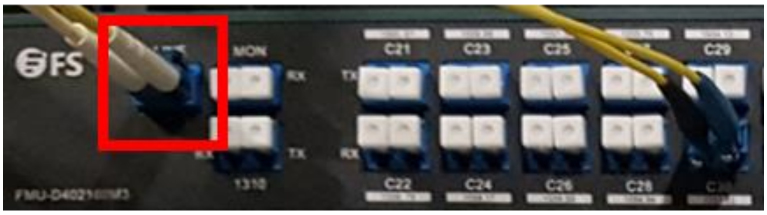
5.4.3. Setting up the QKD Service Channels connection

Each QKD Blade requires a suitable SFP transceiver module for the service channel. The modules provided by IDQ are from Finisar’s “FWLF1632xx Fixed Channel DWDM 120km SFP Optical Transceiver” family. Those modules are available for transmitter wavelengths between 1528.77 nm and 1563.86 nm and obey the main specifications as summarized in Table 4 below. The part number of standard module provided by IDQ is FWLF163230, corresponding to ITU Channel 32, 1553.33nm.

Parameter	Value	Notes
Data Rate	2.7 Gbps (or more)	SONET OC-3/12/48 compatible
Total link budget	28 dB (or more)	at 2.5 Gbps with BER <10^{-12}
Center Wavelength Spacing	100 GHz / 0.8 nm	
Modulated Spectral Width	0.3 nm	Full width, -20 dB
Side Mode Suppression Ratio	30 dB	Modulated
Optical Rise/Fall Time	160 ps	Unfiltered, 80%-20%
Optical Output Power	4 dBm	Average output power
Transmitter Extinction Ratio	8.2 dB	
Transmitter Eye Opening	10 %	
Transmitter Jitter	75 mUI	peak-to-peak
Relative Intensity Noise	-120 dB/Hz	
Dispersion Power Penalty at 2400 ps/nm	3.0 dB	
Receiver Jitter	75 mUI	
Optical Input Power	-9 dBm - -28 dBm	at 2.5 Gbps with BER <10^{-12}
Receiver Damage Threshold	+6 dBm	
Dispersion Noise Penaltyat 2400 ps/nm	3.0 dB	
Operating/Storage Temp.	-5°C-70°C / -40°C-85°C	Ambient temperature
Supply Voltage	3.13 V - 3.50 V	
Supply Current	380 mA	
Inrush Current	410 mA	
Maximum Power	1.3 W	
Transmitter Input Impedance	100 Ω	
Single ended data input swing	250 mV - 1200 mV	
Transmit Disable Voltage	1.83 V - 4.2 V	
Single ended data output swing	175 mV - 1000 mV	
Data Output Raise/Fall Time	150 ps	
Receiver LOS Assert Level	-36 dBm	
Receiver LOS Deassert Level	-34 dBm	
Receiver LOS Hysteresis	2 dB	

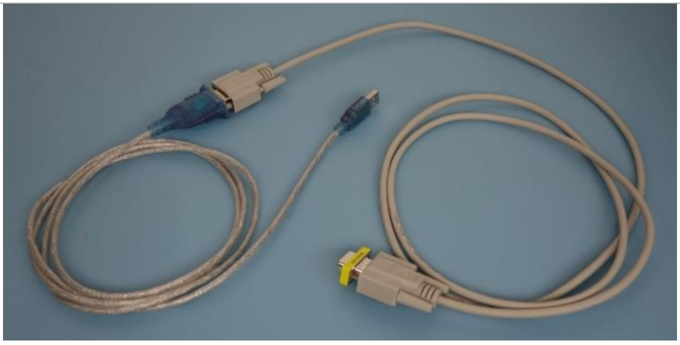
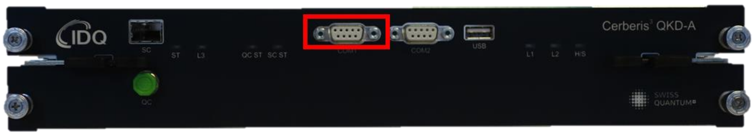
Table 4: Required characteristics of the SFP Transceiver for the QKD Service Channel.

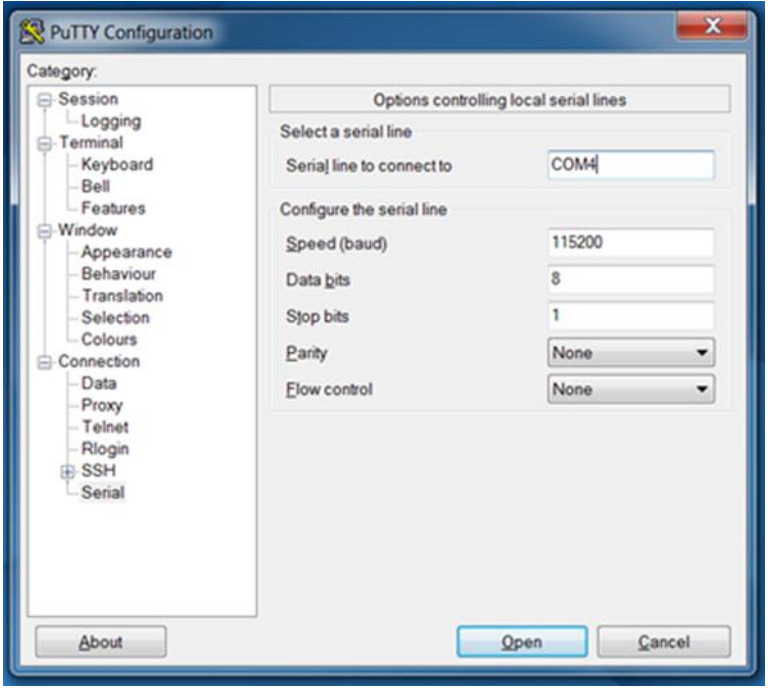
Step	Description
	Remove both protective caps from the LC connector of the dual fiber patch cord and clean the exposed fiber ferrules by wiping them on the cleaning tool. Only wipe in the direction depicted on the cleaning tool! Remove the protective cap from the SFP module and carefully insert the LC connector into the SFP module. ***A proper connection is confirmed by an audible click when inserting the module. Verify that the metallic handle is in an upward position!***
	If the service channel fibers have less than 10 dB of losses, add the 15-dB fix LC attenuators to prevent saturation of the SFP modules.
	Slide the SFP module into the front panel mount at the QKD blade. A proper installation is confirmed by an audible click when inserting the module.
	At the other end of the dual fiber patch cord, remove both protective caps and clean the exposed fiber ferrules by wiping them on the cleaning tool. Only wipe in the direction depicted on the cleaning tool! Carefully insert the LC connector into the respective port of the multiplexer. ***A proper connection is confirmed by an audible click when inserting the module.***

Step	Description
To fiber link 	Connect the common fiber port of the multiplexer to the fiber link towards the remote node.

5.4.4. Connecting to the QKD Blade via a RS-232 serial connection

To connect to the QKD Blade via its front panel COM1 serial port, follow the steps below:

Step	Description
	If necessary, prepare the serial null modem cable by connecting the USB-to-serial adapter to the null modem cable and the male-male mini-gender adapter to the null modem cable
COM1 Port 	Connect the serial cable to the 9-pin COM1 port on the QKD-Blade front panel.
	Connect the other end of the serial cable to the serial port or USB port of the Configuration PC.

Step	Description
  PuTTY Configuration Options controlling local serial lines Select a serial line Serial line to connect to: COM4 Configure the serial line Speed (baud): 115200 Data bits: 8 Stop bits: 1 Parity: None Flow control: None	Start a terminal program and set the following parameters for the serial connection: Baud speed: 115200 Data bits: 8 Stop bits: 1 Parity: None Flow Control: None Terminal mode: Implicit LF in every CR.
	Open the serial connection. In the appearing terminal window press the ENTER key once to see the login prompt.
	Refer to sec. 6.3 for the available commands.

5.4.5. Connecting to the QKD blade via SSH through an Ethernet connection

1. Connect a PC with a SSH client terminal (e.g. Putty) to the QKD blade network.
2. Start the SSH terminal and connect with the IP address of the QKD blade.
3. Refer to sec. 6.3 for the available commands.

<command> --help.

5.5.Shelf Manager and Switch QS3201 network configuration

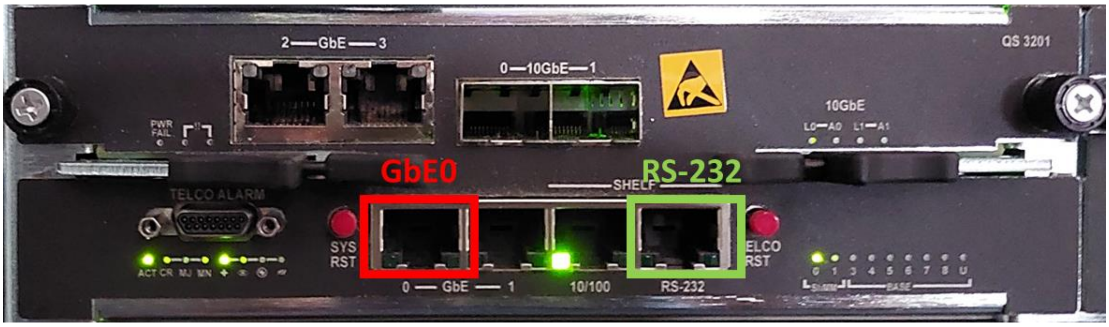


Figure 20: Serial interface of the QS3201 Shelf Manager and Switch blade through RJ-45 connector.

5.5.1. Configuration of the Switch GbE0 to GbE3 IP addresses

The 4 Ethernet ports (labelled GbE0 to GbE3) on the front panel of the QS3201 Shelf Manager and Switch are connected to interface 4. For initial configuration of the interfaces, a CLI connection through the RS-232 front panel port is recommended.

The interface is configured by editing the interface configuration file as follows:

1. Connect to the QS3201 through the RS-232 as described in section 5.2.5.
2. In the file */etc/rc.d/rc.conf*, edit the *interface 4* parameters using the installed vi-editor:
   2.1. Enter *vi /etc/rc.d/rc.conf*
   2.2. Press *i* to be in Edit mode
   2.3. Set the settings corresponding to item M1/S1 in Table 2, section 4.3.2.:
      2.3.1.Set HOSTNAME value to <switch_hostname>
      2.3.2.Set IPADDR4 value to <switch_IP_address>
      2.3.3.Set NETASK4 value to <switch_netmask>
   2.4. Remove the BROADCAST4 line
3. Save and close the interface configuration file:
   3.1. Type *:wq*
   3.2. Press Enter.
4. Reboot the QS3201:
   4.1. Type *reboot* and press Enter.

After changing this address, the IP address must be given to the local QNC as described in section 6.3.1.

Exemplary interface configuration file

For instance, if the hostname is switch.company.com, the corresponding line in the interface configuration file should be as following:

```
export HOSTNAME="hostname switch.company.com"
```

For setting the IP address to the address scheme example of Table 2, section 4.3.2, the section interface 4 should be as following:

```
# net interface 4 for VT031, VTSM Virtual interface
export SYSCFG_IFACE4=y
export IPADDR4="10.10.10.190"
export NETMASK4="255.0.0.0"
export INTERFACE4="eth4"
export GATEWAY4="0.0.0.0"
export NAMESERVER4="0.0.0.0"
```

5.5.2. Configuration of the Shelf Manager IP address

The Shelf Manager interface allows access to the Shelf Manager resources. This address is only required when updating the BMC via the switch.

To view the current IP address setting of the ShMM:

1. Connect to the QS3201 through the RS-232 port as described in section 5.2.5
2. Type *get_ip_connection*
3. Press Enter. The current IP connection record for the Shelf Manager is shown, for example:

```
IP Connection Record 0IP Address: 0.0.0.0
Gateway Address: 0.0.0.0
Netmask: 0.0.0.0
```

To change the network configuration of the Shelf Manager interface to the address scheme configuration of Table 2:

1. Type

   ```
   set_ip_connection -i 0 -a <ShMM_IP_Addr> -g <ShMM_gateway> -n <ShMM_netmask>
   ```

2. Press Enter.
3. Enter *reboot*. The Shelf Manager reboots and the CLI is terminated.

The IP address to be used are items M9/S9 in the address scheme example of Table 2, section 4.3.2, for which the connection record shows:

```
IP Connection Record 0IP Address: 10.10.10.194
Gateway Address: 255.0.0.0
Netmask: 0.0.0.0
```

5.6.QKD blade network configuration

To provide network access for the QKD Blade through the front panel of the ShMM and Switch blade, the QKD Blade must be set to the same network as the Switch. For initial configuration of the QKD Blade, a local connection through the QKD Blade front panel port is recommended.

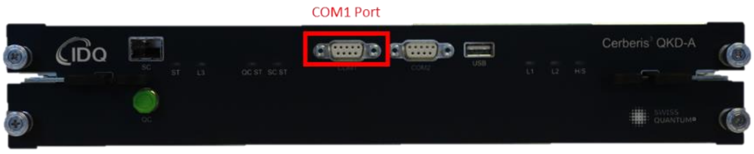


Figure 21: Front panel port on the QKD Blade to access the CLI.

To configure the IP addresses of QKD blade:

1. Connect to the QKD Blade front panel port labeled COM1 as described in section 5.4.4.
2. Login with the *admin* role.
3. Use the command *network* (see sec. 6.3.1) to set the IP address, netmask, and gateway. The IP addresses to be used are items A3/B3 in the address scheme example of Table 2, section 4.3.2.

After this, the QKD Blade is also available through the Ethernet port on the front panel of the ShMM and Switch blade.

5.7.QNC blade network configuration

The QNC Blade is embedding the Key Management System (KMS) depicted on the Figure 1.

To provide network access for the QNC Blade through the front panel of the ShMM and Switch blade, the QNC must be set to the same network as the Switch.

For initial configuration of the QNC, a local connection through the QNC front panel port is recommended.

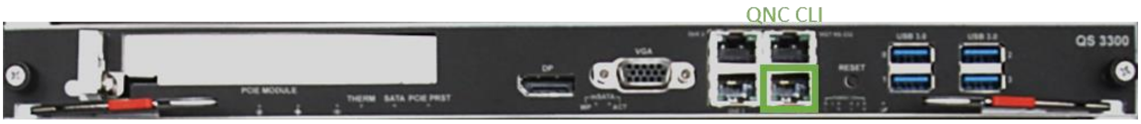


Figure 22: The QNC USB Front panel connection to the serial interface.

To configure the IP addresses of QNC blade:

1. Connect to the QNC front panel port labeled x86 RS-232 as described in section 5.3.3.
2. Login with the *admin* role.
3. Use the command *network* (see sec.6.3.1) to set the IP address, netmask, and gateway. The IP addresses to be used are items M2/S2 in the address scheme example of Table 2, section 4.3.2.

After this, the QNC is also available through the front panel ShMM and Switch blade. Its address must also be given to the SNMP client to obtain the SNMP monitoring information (see section 6.4.1).

5.8.QNC-to-Encryptor key interface network configuration

Encryptors can access the keys from the QNC through the QNC front panel ports ETH2 and ETH3.

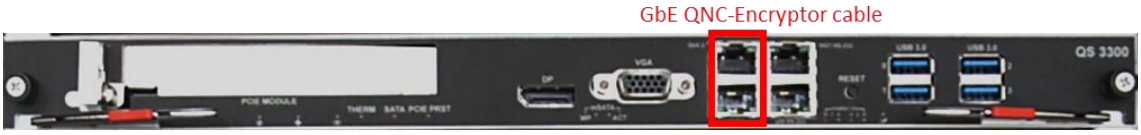


Figure 23: GbE interfaces for the keys and encryptors.

To configure the IP addresses of QNC front panel ports through which encryptors can access keys:

1. Connect to the QNC through the QNC front panel port labeled x86 RS-232 as described in section 5.3.3.
2. Login with the *admin* role.
3. Use the command *network* (see sec. 6.3.1) The IP addresses to be used are items M4+M5/S4+S5 in Table 2, section 4.3.2.

This address must be given to the encryptors that request keys from the QNC and must therefore be in the same subnet as the encryptors.

5.9.QNC Syslog interface network configuration

Alarms are sent using syslog though the Switch front panel ethernet port.

To set the IP address of the syslog server on the QNC, use the QNET application (see “IDQ QNET User Guide”). The IP addresses to be used are items M8/S8 in the address scheme example of Table 2, section 4.3.2.

6. Operation

6.1.LED states

The most relevant interfaces and status indicators of a Cerberis XG node are indicated in Figure 24 and explained in more detail in Table 5.

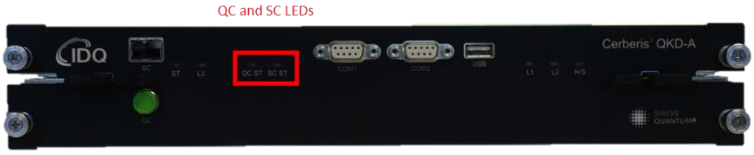


Figure 24: Location of the Quantum channel (QC) and QKD Service channel (SC) LEDs on the QKD Blade.

LED	LED Status	Status Description
Quantum	OFF	Cerberis XG node Quantum Channel is desynchronized
	ON (Green)	Cerberis XG node Quantum Channel is synchronized
Service	OFF	Cerberis XG node Service Channel is desynchronized
	Blinking (Green)	Cerberis XG node Service Channel is synchronizing
	ON (Green)	Cerberis XG node Service Channel is synchronized
	Blinking (Red)	Cerberis XG node Service Channel error

Table 5: Description of the Service Channel Front Panel LED status.

6.2.Command Line Interface of the QS3201 Shelf Manager

The Shelf Manager on the QS3201 provides a Command Line interface (CLI) for its operation that can be accessed with the root access. A list summarizing the available commands is given in the Appendix B.1.

To complete list all available CLI commands on the Shelf Manager:

1. Connect to the Shelf Manager CLI as described in section 5.2.4.
2. Type

   ```
   cli_commands
   ```

3. Press Enter. The available ShMM commands are listed.

6.2.1. Setting User Information and Passwords

The default administrative username and password are *root* and *root*, respectively, for console authentication. To add a new user, change a username, set, and change user passwords, and enable and disable users, use the Shelf Manager CLI command *set_user_info*. The *set_user_info* command takes the following options:

Parameter	Description
-i|--user-id USER_ID	USER_ID is a 1-based number used to identify a user record. User ID 1 is reserved for the null username.
-n|--username USER_NAME	USER_NAME is an ASCII string with maximum length of 16 characters.
-p|--password PASSWORD	PASSWORD is a string of no more than 20 characters that follows NIST guideline for password policy. This option is required when assigning a password.
-t|--test-password PASSWORD	test-password verifies the password value against the password saved in storage.
-e|--enable	The user must be Enabled before the username assigned to the user can be used.
-d|--disable	A user can be disabled

Table 6: The Shelf Manager set_user_info *CLI command.*

To set the password *password* of the user with user ID 2, run the following command in the Shelf Manager CLI:

```
set_user_info -i 2 -p password
```

To assign a new username *david* to the user with user ID 2, run the following command:

```
set_user_info -i 2 -n david
```

To verify that the password *newPassword* was set for user with ID 2, run the following command:

```
set_user_info -i 2 -t newPassword
```

To enable the user with ID 2, run the following command:

```
set_user_info --user-id 2 --enable
```

When adding a new user, by default, the user is disabled with the access available only during callback connection, the link authentication being disabled, the IPMI messaging being disabled, and a current and maximum operating level of NO ACCESS. To change the access rights and configure privilege level and channel accessibility associated with a given user ID, use the Shelf Manager CLI command `set_user_access` (see **Error! Reference source not found.** in Appendix B.1 for more details).

6.2.2. Shutting down the chassis and all modules from the ShMM CLI

The Shelf Manager provides a command for power, reset, and diagnostic interrupt control of the Chassis. To power down the whole chassis including the installed modules:

1. Connect to the Shelf Manager CLI as described in section 5.2.4.
2. Type

```
chassis_control -d
```

3. Press Enter. The system goes into the SOFT OFF state.
4. Wait until all H/S Blue LEDs stop flashing and turn into solid Blue.
5. Disconnect the chassis from the power supply.

6.2.3. Restoring the Factory Default Configuration of the QS3201 Shelf Manager

To restore the factory default configuration on the Shelf Manager, run the CLI command:

```
setShelfmanagerDefaults
```

The `setShelfmanagerDefaults` command takes no parameters. The chassis must be power cycled for the default configuration to be applied.

6.3. QNET Shell

QNET shell is a command line interface embedded in your Cerberis XG QKD node. This tool provides some administration and configuration commands. Depending on their profile, users have different permissions to the shell functions.

QNET shell is defined for 4 defined users:

user id	role description	Password
admin	full administration privileges	admin
monitor	security privileges	monitor
crypto	monitoring privileges	crypto
user	read-only	user

The first time the system is accessed as admin, monitor, crypto or user, a password change is requested.

> ⚠ WARNING
>
> *If a user provides the wrong password three times, the account is locked. To be able to access it again, the system needs to be rebooted. To do so once an account is looked (for ex. admin) use another account that has reboot rights (crypto for ex.) and reboot the node.*

NOTE: Before setting the new password, it is important to mention that the new password must fulfill the following criteria:

- Minimum password length is 15 characters.
- No character can be repeated more than twice.
- Password must be composed of capital/small letters, numbers, and special characters.

- Have maximum 4 consecutive characters of the same class.

A new password must differ of 8 characters at least from the old password.

To set the user profile password, type:

```
password
```

The QKD and QNC systems provide a shell for their operation according to different user profiles. For a full description of the QNET Shell capabilities, please refer to: *IDQ QNET shell User Guide*.

The key functions related to Network Configuration, Channel delays settings and update via USB key are described in more detail in the next sections.

6.3.1. Showing or setting the network configuration

To show the system network configuration of QKD or QNC blades, type on the corresponding Qnet shell interface:

```
network
```

To change the network configuration, type:

```
network -i <arg> -a 10.10.10.191 -n 255.0.0.0 -g 0.0.0.0
```

where arg is the interface number (refer to the address scheme configuration of Table 2):

- QNC: 0 for the management interface on the backplane (QNC-CPU), 2 (Encryptor 1) or 3 (Encryptor 2) for the front panel interfaces
- QKD: 0 for the management interface on the backplane (QKD-CPU)

If connected to the system via SSH, the connection will be terminated after changing the IP address.

6.3.2. Inspecting the QKD Log Files

The log files related to the operation of the QKD Blade can be inspected using the *loginspect* command.

To show the list of available log files, type:

```
Loginspect -L
```

To inspect an available log file, type:

```
Loginspect
```

The log file is printed on the screen and can be analyzed using the options of the LINUX *less* command. Press *q* to quit the log file inspector.

ℹ *USAGE OF THE LOGINSPECT MODE*

- Once in the loginspect mode, a full help of the command is available by typing `h`.
- You can scroll through the log file using the arrow UP and DOWN keys, as well as the PgUP and PgDOWN keys.
- To quickly go to the beginning of a file, type *g*. To quickly go to the end of a file, type *G*.

- You can search for a pattern within the log file by entering slash '/' (forward direction) or question mark '?' (backward direction) followed by the search term, e.g. to search for "QBER", type:

```
/QBER
```

- To show only lines that contain a specified search pattern, enter '&' followed by the search term, e.g. to show only lines that contain "Visibility", type:

```
&Visibility
```

6.3.3. Shutting down

There are two ways to shut down the system: either by opening the system front panel handle mechanically, or by using QNET shell. With the later, type:

```
shutdown
```

The blue H/S front panel LED starts flashing. Wait until the blue H/S front panel LED is solid blue, indicating that the system has been shut down.

6.3.4. Updating the system

The system can be updated from a USB stick that contains a valid signed image and is plugged in the front panel USB port.

> *NOTE*
>
> *The USB stick used for the update must be maximum 4GB in size and FAT32 formatted*

Plug in a USB stick with a valid signed image in the front panel USB port.

To list all available updates on the USB stick, type:

```
update
```

To update the system, select the image file to use for the upgrade, and confirm.

The system will take up to 10 minutes to update. After the update is complete **you MUST confirm the reboot question by typing *y*** to reboot the system.

> *WARNING*
>
> *On a QNC system, the update might complete successfully but display a failed update message. After reboot, check that the version corresponds to the updated image.*

Once the system has rebooted, re-connect to the system as *admin* and type:

```
version -a
```

The new system version should be displayed.

6.4. Monitoring the system via SNMP

6.4.1. Configuration of the SNMP client for QNC monitoring

The Cerberis[3] system implements the SNMP v3 protocol with a dedicated MIB. This section describes the SNMP configuration and collection of monitoring values, for example using the GPLv2 MIB browser *SnmpB* (https://sourceforge.net/projects/snmpb/). Note that any alternative SNMPv3 client can be used but must be configured according to the following example.

1. If necessary, download and install SnmpB from https://sourceforge.net/projects/snmpb/
2. On the provided USB stick, locate the correct Management information base (MIB) for the Cerberis[3] system named `IDQ-CERBERIS3-QKD-NODE-MIB.mib`
3. Launch the SnmpB application and add the MIB:
   3.1. Click Options → *Preferences...*
   3.2. Select *Modules*.
   3.3. Enter the path to the MIB file and click *OK*.
   3.4. Go to the tab *Modules* and transfer the MIB from the left-hand pane to the right-hand pane.
4. Add a user profile:
   4.1. Click *Options* → *Manage SNMPv3 USM Profiles...*
   4.2. Right-click on the left-hand pane and select *New USM profile*.
   4.3. Set *Security User Name* to *cerberis3*.
   4.4. Set *Authentication Protocol* to *SHA*.
   4.5. Set *Authentication Password* to *cerberis3*.
   4.6. Set *Privacy Protocol* to *AES128*.
   4.7. Set the *Privacy Password* to *cerberis3*.
5. Add the agent profile:
   5.1. Click *Options* → *Manager Agent Profiles...*
   5.2. Right-click on the left-hand pane and select *New agent profile*.
   5.3. Set *Agent Address/Name* to the Cerberis[3] QNC IP address.
   5.4. Set *Agent Port* to *161*.
   5.5. Set *Supported SNMP Version* to *SNMPV3*.
   5.6. Unfold the agent profile in the left-hand pane and select *SnmpV3*.
   5.7. Set *Security Name* to *cerberis3*.
   5.8. Set *Security Level* to *authPriv*.
6. In the tab *Tree*, select the newly created agent profile and browse the tree down to *MIB Tree → iso → org → dod → internet → private → enterprise → idq → cerberis3QkdSystem*
   → cerberis3QkdNode
   6.1. In subtree *ne*, right-click on *neTable* and select *Table View*. Wait a few seconds and the return values should appear in the right-hand pane.
   6.2. In subtree *qkdBlade*, right-click on *qkdBladeTable* and select *Table View.* Wait a few seconds and the return values should appear in the right-hand pane.

6.4.2. Specification of the Cerberis[3] MIB

The following monitoring functions are available through the SNMP MIB module “IDQ-CERBERIS3-QKD-NODE-MIB” of the Cerberis[3] Node system (MIB Revision: 201809281200Z):

Name	Object ID	Description

qkdNE	1.3.6.1.4.1.22328.2.1.2.1.1.1	The identifier of the network element which is unique within a family of network elements.
qkdState	1.3.6.1.4.1.22328.2.1.2.1.1.2	The QKD system's state: 0: poweredOff 1: poweringOn 2: executingSelfTest 3: executingGeneralInitialization 4: executingSecurityInitialization 5: running 6: poweringOff 7: handlingError 8: updatingSoftware 9: zeroizing
qkdCompressionRatio	1.3.6.1.4.1.22328.2.1.2.1.1.3	The QKD system's compression ratio.
qkdLaserPower	1.3.6.1.4.1.22328.2.1.2.1.1.4	The QKD system's laser power.
qkdQber	1.3.6.1.4.1.22328.2.1.2.1.1.5	The QKD system's QBER.
qkdVisibility	1.3.6.1.4.1.22328.2.1.2.1.1.6	The QKD system's visibility.
qkdKeyRate	1.3.6.1.4.1.22328.2.1.2.1.1.7	The QKD system's quantum key rate (bits/s).
qkdTotalDetectionCount	1.3.6.1.4.1.22328.2.1.2.1.1.8	The QKD system's detection count on DATA and MONITOR.

Name	Object ID	Description
neIndex	1.3.6.1.4.1.22328.2.1.1.1.1.1	The index uniquely identifies the network element in the context of the Cerberis^3 QKD Node.
neType	1.3.6.1.4.1.22328.2.1.1.1.1.2	The type of the network element: 1: QNC 2: QKD
neIpAddress	1.3.6.1.4.1.22328.2.1.1.1.1.3	The network element's IP address.
neSerialNumber	1.3.6.1.4.1.22328.2.1.1.1.1.4	The network element's serial number.
neSwVersion	1.3.6.1.4.1.22328.2.1.1.1.1.5	The network element's firmware version.
neSysUptime	1.3.6.1.4.1.22328.2.1.1.1.1.6	The network element's uptime.
neCpuLoad	1.3.6.1.4.1.22328.2.1.1.1.1.7	The network element's average CPU load over 1 minute.
neMemUsage	1.3.6.1.4.1.22328.2.1.1.1.1.8	The network element's RAM usage.
neTemperature	1.3.6.1.4.1.22328.2.1.1.1.1.9	The network element's temperature.
neFanState	1.3.6.1.4.1.22328.2.1.1.1.1.10	The network element's fans state: 0: unhealthy 1: healthy
nePowerSupplyState	1.3.6.1.4.1.22328.2.1.1.1.1.11	The network element's power supply state: 0: unhealthy 1: healthy
neOperationalState	1.3.6.1.4.1.22328.2.1.1.1.1.12	The network element's operational state: 0: inactive 1: active

Name	Object ID	Description
cerberis3QkdNodeCompliance	1.3.6.1.4.1.22328.2.1.3.1.1	The compliance statement for SNMPv2 entities which implement Cerberis^3 QKD Node.
cerberis3QkdNodeGroup	1.3.6.1.4.1.22328.2.1.3.2.1	The current Cerberis^3 QKD Node group of objects providing for management of Cerberis3 QKD Node.

6.5.Understanding the QKD Log files

The log files are accessible through QNET shell in various ways: by "Inspecting the log files" as described in section 6.3.2, by "Monitoring the log files" as described in section 6.4.

. A full description on how to correctly interpret the information shown on the log file can be found in the document: *Understanding the QKD log files.*

B. Appendix

B.1. COW protocol description

The aim of Quantum Key Distribution is to exchange a secret key between Alice and Bob by encoding bits with quantum state carried by single photons (qubits). There are different ways to encode qubit values on single photons. One of those ways is called time-bin qubits. As shown in Figure 25 Illustration of the qubit sphere and of time-bin qubits., this method consists in creating a pair of coherent pulses propagating in the same spatial mode and separated by a given time. The first pulse is called the early pulse. The second one is called the late pulse. To generate all possible qubit values (i.e. all possible states of the qubit sphere), the intensity ratio between those two pulses can be varied between 0 and infinity. Those two extreme cases correspond to the two poles of the sphere, i.e. either when the whole optical energy of the single photon is contained in the early or late pulses. Those two quantum states compose the computational basis of the qubit space. By changing the energy level ratio between the two optical pulses, one can move the qubit state along one of the meridians of the qubit sphere. To move along one of the parallels, one needs to change the phase relation between the early and late pulses. One manner to implement time-bin qubit emitter is based on an unbalanced Mach-Zehnder interferometer where the input beam splitter ratio can be varied and the output beam recombiner is a fast switch. A possible implementation of a time-bin qubit analyzer consists in the same Mach-Zehnder interferometer where input and output ports have been swapped.

The BB84 protocol can be implemented with time-bin qubits. In this case, it is generally implemented with four qubit states located on the equatorial plan of the qubit sphere. This choice is made to guarantee as many similarities as possible in the implementation of the two bases used in BB84 protocol. In this case, the two Mach-Zehnder interferometers are made with two 50/50 couplers and one phase modulator. This kind of implementation requires a tight control on the interferometer's stability or at least a dynamic adjustment of one interferometer compared to the other one.

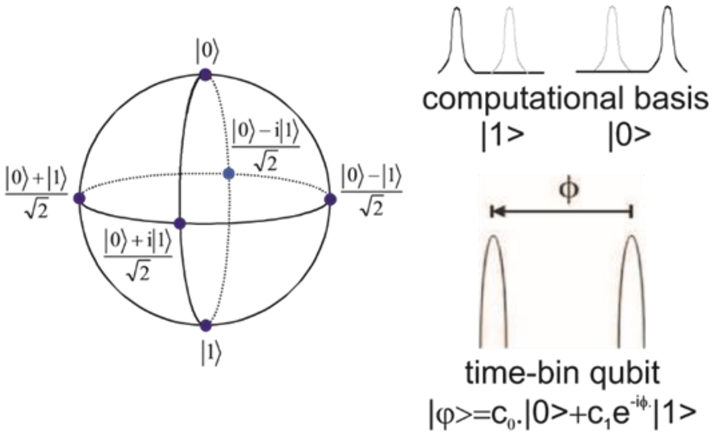

$|0\rangle$
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$|1\rangle$
computational basis
|1>
|0>
ϕ
time-bin qubit
$|\varphi\rangle = c_0.|0\rangle + c_1 e^{-i\phi}.|1\rangle$

Figure 25 Illustration of the qubit sphere and of time-bin qubits.

The aim of COW protocol is to make the implementation of a QKD system as simple as possible to allow a strong increase of the final secret key rate in a manner that allow the industrialization of the system. Therefore, a first requirement of COW protocol was not to use two interferometers to avoid stabilization of one interferometer compared to another. A second requirement of this protocol was to work specifically with weak optical coherent pulses, but not with single photon pulses. This requirement is motivated by the fact that it is very simple to implement weak coherent pulse sources whereas single photon sources are still difficult to handle. Several other requirements, that are not listed here, were targeted when COW protocol was designed.

A first specificity of COW protocol is to use the qubit basis composed of the two pole states (the early and the late pulses). Hence, the measurement method to analyze this basis is simply to measure the time of detection of the optical pulse. If one detection occurs in the early time-bin, the qubit value is a |0> state, whereas if it occurs in the late time-bin, the qubit is a |1> state. This measurement method does not require any complex optical component except one single photon detector with a temporal accuracy allowing one to distinguish between the two time-bins. In COW protocol, as in any QKD protocols, two qubit bases are used to guarantee the security of transferred keys. But in this protocol, one basis will be used to generate the raw key and the other one to estimate the security level of the exchanged qubits in the first basis. The basis used to exchange the raw key is the computational basis, because as explained previously, it requires an analyzer composed uniquely on a single detector. This basis will be the more often used to maximize the raw key rate (in other protocol like BB84, the ratio because the two basis is 50/50 in general because both bases equally contribute to the generation of raw keys and to the estimation of the security level of this raw key). The second basis used in COW protocol is one of the bases located on the equatorial plan of the qubit sphere. The analyzer for this kind of basis is implemented with an unbalanced interferometer as described in the case of one example of a BB84 protocol implementation. To avoid an implementation with only one interferometer, COW protocol is based on a qubit emitter that requires no interferometer. COW emitter needs to be able to emit either early or late pulses to generate states of the computational basis. This can be done easily by switching on and off a light source at the time corresponding to the desired qubit states. One of the key ideas of COW protocol is to keep the coherence between two consecutive optical pulses belonging to the same time-bin qubit or not (i.e. one belonging to one qubit and the other one belonging to the following qubit). This coherence can be checked with the interferometer in the receiver station in both cases if the time separation between two time-bin quits equals the time between the two pulses composing one qubit. Therefore, the emitter in COW protocol needs to guarantee the same phase relation between consecutive optical pulses whether they belong to the same qubit or not. To enhance the security of COW protocol, one qubit state of the second basis of the receiver will be emitted from time to time. This state is called decoy sequence. It consists in an early and a late optical pulse with the same energy level than the early pulse in a |0> state. The phase relation between one of the two pulses of the decoy sequence and the consecutive pulses needs to be kept identical to the one between pulses of the computational basis. This decoy sequence is used in combination with the second basis analyzed in the receiver to estimate the security of the raw key exchanged using the computational basis. The ratio between the emitted states from the computational basis and the decoy sequence is in favor of the computational basis to optimize the raw key rate.

In summary, as depicted in **Error! Reference source not found.**, COW protocol consists in an emitter emitting qubits states from the computational basis or decoy sequences. The time between all consecutive pulses is identical and the phase relation between those consecutive pulses is kept constant. The ratio of the number of qubits from the computational basis and the number of decoy sequences is in favor of the computational basis. The receiver station consists in an analysis for the computational basis and an analyzer to check the phase relation between two consecutive optical pulses. The ratio of use of the analyzer for the computational basis compared to the use of the analyzer for the phase relation check is in favor of the computational basis. A QBER value is measured by counting the probability of having an error in the exchange of qubits of the computational basis. The phase relation check is quantified by measuring the visibility of interferences occurring in the second basis analyzer. Based on both values, QBER and visibility, (plus few other parameters like the ratio values) it is possible the estimate if it is possible to extract secret keys form the qubits exchanged between the emitter and the receiver stations.

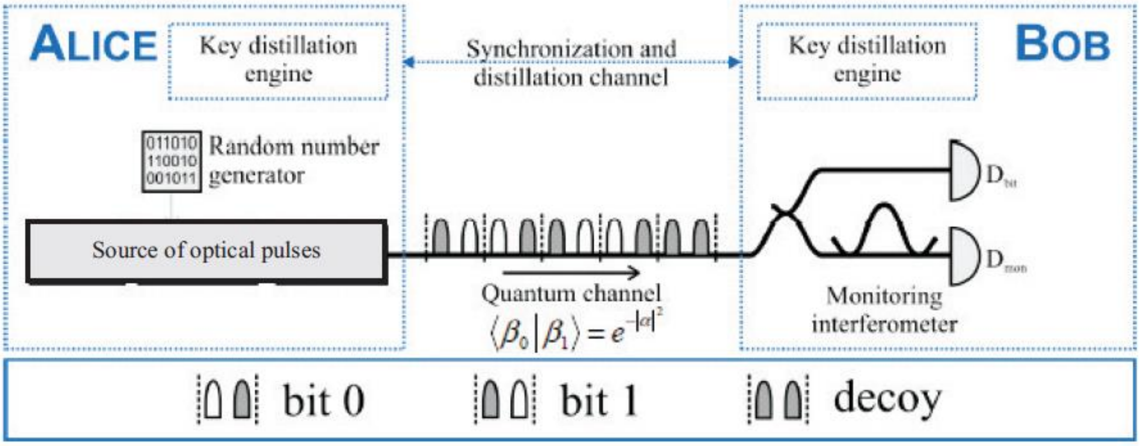


Figure 26 Illustration of COW principle

B.2. COW 4-states

Following the paper of Marcos Curty ([2101.07192] Zero-error attack against coherent-one-way quantum key distribution (arxiv.org)) describing a "theoretical" attack that could be performed on COW protocol, a security analysis has been conducted. Thanks to this analysis we can prove that the COW protocol is still safe today up to 12dB dynamic range, with the current parameters in the trusted detector scenario. To be safe also at higher dynamic range, we adapted the protocol by implementing a countermeasure which allow us to prevent the sequential attack and extend the dynamic range to 16dB and more. In the COW 4-states protocol an additional vacuum state is added to the protocol, this implementation significantly decreases the probability that Eve's unambiguous state discrimination measurement can produce a conclusive result.

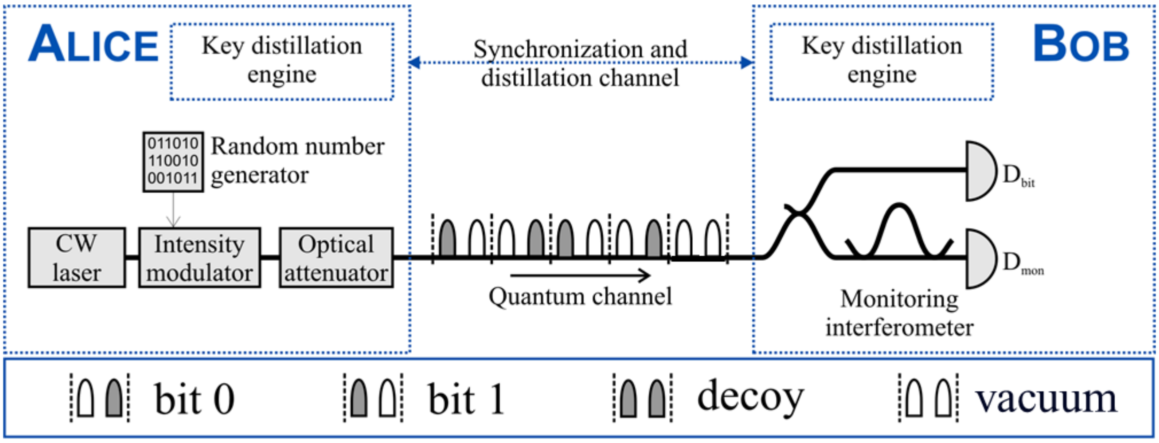


Figure 27: Illustration of the COW 4-states protocol.

Using the QNET shell on **Alice QKD terminal**, it is possible to see which protocol is running with the command:

protocol

the answer can be:

QKD Protocol: Cow4States

or

QKD Protocol: Cow3States

it is possible to change the protocol using the command *protocol* followed by the type of protocol, for ex:

protocol Cow4States

NOTE

Please contact ID Quantique for additional information about the implementation of COW 4-state protocol and its security.

B.3. Commands Summary of the QS3201 Shelf Manager

Group	Command	Description
Alarm	`alarm_clear`	Remove or clear a triggered alarm from the list of active alarms
	`alarm_reset`	Clear alarms for a given time (specified in minutes)
	`alarm_status`	Display the active alarms and whether the alarm cut-off is enabled
	`alarm_test`	Test the alarm subsystem
	`list_alarm_codes`	Translate the Advanced TCA Shelf diagnostic alarm codes
	`get_telco_alarm_state`	Display the state of Telco alarms for a given ATCA Shelf
	`get_telco_capabilities`	Display the Telco alarm states and modes for a given ATCA Shelf
	`set_telco_alarm_state`	Set a given Telco alarm's state
Alerting	`get_pef_config_parameters`	Display the configuration of a given Platform Event Filter (PEF) parameter, such as the configuration of the Event Filter Table and alert strings, as well as whether PEF is enabled/disabled
	`get_snmp_trap_info`	Display the status of SNMP traps and available trap destinations
	`set_pef_config_parameters`	Configure a given Platform Event Filter (PEF) parameter, such as the Event Filter Table and alert strings, as well as whether PEF is enabled/disabled
	`snmp_trap_disable`	Disable SNMP traps for a given channel
	`snmp_trap_enable`	Enable SNMP traps for a given channel
	`snmp_trap_get_address`	Display a list of SNMP trap destinations for a given channel
	`snmp_trap_remove_address`	Remove an SNMP trap destination from a given channel
	`snmp_trap_set_address`	Modify an SNMP trap destination for a given channel
	`snmp_trap_test`	Send a test SNMP trap to a given destination; get/clear status of test alert sent to a given destination
CLI	`cli_commands`	List all available CLI commands
	`cli_options`	Describe the shorthand notation used for common CLI options

Group	Command	Description
	`exit`	Exit the CLI; see `q`
	`get_version`	Display the application and CLI versions
	`help`	Display help for a given command, or display all commands, organized by group
	`q`	Exit the CLI; see `exit`
Cooling	`get_cooling_parameters`	Display the Shelf cooling management parameters
	`get_fan_info`	Display the Fan Tray properties and hot-swap status for a given Fan Tray
	`get_fan_level`	Display a given Fan Tray's current operating speed level
	`list_fan_trays`	Display the locations of all Fan Trays installed in the Shelf
	`set_cooling_parameters`	Configure the Shelf cooling management parameters
	`set_fan_level`	Set the current operating speed level for a given Fan Tray
E-Keying	`get_amc_ptp`	Display AMC e-keying information
	`get_backplane_ptp`	Display backplane point-to-point information
	`get_board_ptp`	Display e-keying information for a given AdvancedTCA Board
	`get_carrier_ptp`	Display a given Carrier's Carrier point-to-point connectivity information
	`get_port_state`	Display link status for a given FRU
FRU Management	`activate`	Activate a given FRU, bring it to M4 state
	`deactivate`	Deactivate a given FRU, bring it to M1 state
	`fru_control`	Change the state of a given FRU's payload
	`fru_reset`	Reset a FRU's management controller
	`get_address_info`	Display a given FRU's address information
	`get_board_info`	Display the configuration and hot-swap information for an ATCA Board at a specified Shelf slot
	`get_device_id`	Retrieve device information from a given FRU
	`get_event_receiver`	Display the location of the event receiver for a given FRU
	`get_fru_activation_policy`	Display the activation policy for a given FRU
	`get_fru_power_levels`	Display a given FRU's power level
	`get_fru_state`	Display the hot-swap information for a given FRU
	`get_fru_temperature`	Display the status of all temperature sensors for a given FRU
	`get_health`	Provide a summary of the FRU alarm and health status
	`list_boards_installed`	Display the list of installed AdvancedTCA Boards
	`list_frus_present`	Display the list of installed FRUs
	`list_device_sdr`	Display the list of SDRs in a given FRU's Device SDR Repository
	`list_sdr`	Display the list of SDRs in the SDR Repository
	`list_fru_storages`	Display the list of FRU Inventory Devices located at a given address
	`read_fru_storage`	Display content from a given FRU inventory device
	`set_event_receiver`	Change the location of the event receiver for a given FRU
	`set_fru_extracted`	Inform the Shelf Manager that a given FRU is no longer installed

Group	Command	Description
	`set_fru_power_level`	Set the FRU power level for a given FRU
	`update_fru_version`	Change the product version number for a given FRU
	`set_fru_current_draw`	Set current draw limit required by FRU
LAN	`get_channel_access`	Display whether a given channel is enabled or disabled, whether alerting is enabled or disabled, and under what system modes the channel can be accessed
	`get_channel_cipher_suites`	Display supported authentication, integrity, and confidentiality algorithms
	`get_channel_info`	Display media and protocol information about a given channel
	`get_lan_config_parameters`	Display a given parameter related to IPMI LAN operation, such as network addressing information
	`get_session_info`	Display session information
	`list_active_sessions`	Display the list of active sessions
	`set_channel_access`	Modify whether a given channel is enabled or disabled, whether alerting is enabled or disabled, and privilege level limit
	`set_lan_config_parameters`	Modify parameters required for IPMI LAN operation, such as the network addressing information
	`set_session_privilege_level`	Request the ability to perform operations at a given privilege level for the active session
LED	`get_led_color_capabilities`	Display information about the leds supported by a given FRU
	`get_led_properties`	Display a list of leds controlled by a given FRU
	`get_led_state`	Display the state of a given LED
	`set_led_state`	Set the state of a given LED
Power	`get_power_feed_info`	Display the power information for a given Power Module
SEL	`clear_sel`	Erase the contents of a given System Event Log
	`get_sel`	Display the contents of a given System Event Log
	`get_sel_info`	Display information about a given System Event Log
Sensor	`get_ipmb0_info`	Get FRU IPMB-0 Link status information
	`get_ipmb0_status`	Get FRU IPMB-0 sensor data
	`get_sensor_event_enable`	Display sensor event generation capabilities
	`get_sensor_hysteresis`	Display sensor hysteresis values
	`get_sensor_info`	Display sensor information
	`get_sensor_reading`	Display sensor reading
	`get_sensor_threshold`	Display sensor thresholds
	`list_sensors`	Display a list of sensors on a FRU
	`set_sensor_event_enable`	Set sensor event generation capabilities for a given sensor
	`set_sensor_hysteresis`	Set sensor hysteresis values for a given sensor
	`set_sensor_threshold`	Set sensor thresholds for a given sensor
System Administration	`get_user_access`	Display privilege level and channel accessibility for a given user
	`list_users`	Display the list of available users for the Shelf
	`list_users_access`	Display channel access information for all users on a given channel for the Shelf
	`set_user_access`	Configure privilege level and channel accessibility associated with a given user

Group	Command	Description
	set_user_info	Add user, set / change a given user ID's associated user name or password, and/or enable/disable a given user ID
System Management	chassis_control	Change the power state of the Chassis or issue a diagnostic interrupt
	check_ipmb0_status	Report the status of all IPMB-0 links
	failover	Initiate Shelf Manager failover
	get_chassis_info	Display the Chassis Information record data
	set_chassis_info	Set the Chassis Information record data
	get_shelf_address_info	Display the AdvancedTCA Shelf address
	set_shelf_address_info	Set the Shelf address
	get_address_table	Display the Shelf Address Table
	get_diagnostics	Run diagnostics and display the results
	get_fru_activation_sequence	Display the FRU activation sequence; see get_power_management_info
	get_ip_connection	Display available network interfaces to the AdvancedTCA Shelf
	set_ip_connection	Add or modify available network interfaces to the Shelf
	get_system_guid	Display the globally unique ID (GUID) of a given Shelf

Table 7: Command summary of the QS3201 Shelf Manager

B.4. Detailed MIB entry formats

Name:	qkdNE
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.1
Composed Type:	Unsigned32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The identifier of the network element which is unique within a family of network elements (neIndex).

Name:	qkdState
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.2
Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	poweredOff (0) poweringOn (1)

	executingSelfTest (2) executingGeneralInitialization (3) executingSecurityInitialization (4) running (5) poweringOff (6) handlingError (7) updatingSoftware (8) zeroizing (9)
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's state.

Name:	qkdCompressionRatio
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.3
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's compression ratio.

Name:	qkdLaserPower
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.4
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's laser power.

Name:	qkdQber
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.5
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's QBER.

Name:	qkdVisibility
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.6
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's visibility.

Name:	qkdKeyRate
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.7
Composed Type:	Unsigned32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's quantum key rate (bits/s).

Name:	qkdTotalDetectionCount
Oid:	1.3.6.1.4.1.22328.2.1.2.1.1.8
Composed Type:	Unsigned32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The QKD system's detection count on DATA and MONITOR.

Name:	neIndex
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.1
Composed Type:	Unsigned32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE

Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The index uniquely identifies the network element in the context of the Cerberis3 QKD Node.

Name:	neType
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.2
Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	qnc (1) qkd (2)
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	These are the types of the network elements.

Name:	neIpAddress
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.3
Composed Type:	IpAddress
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	4 .. 4
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's IP address.

Name:	neSerialNumber
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.4
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's serial number.

Name:	neSwVersion

Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.5
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's firmware version.

Name:	neSysUptime
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.6
Composed Type:	Unsigned32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's uptime.

Name:	neCpuLoad
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.7
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's CPU load on average during 1 minute.

Name:	neMemUsage
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.8
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE

Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's RAM usage.

Name:	neTemperature
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.9
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's temperature.

Name:	neFanState
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.10
Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	unhealthy (0) healthy (1)
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's fans state.

Name:	nePowerSupplyState
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.11
Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	unhealthy (0) healthy (1)
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's power supply state.

Name:	neOperationalState
Oid:	1.3.6.1.4.1.22328.2.1.1.1.1.12

Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	inactive (0) active (1)
Module:	IDQ-CERBERIS3-QKD-NODE-MIB
Description:	The NE's operational state.

Name:	cerberis3QkdNodeCompliance
Oid:	1.3.6.1.4.1.22328.2.1.3.1.1
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Compliance
SMI Type:	MODULE-COMPLIANCE
Value List	IDQ-CERBERIS3-QKD-NODE-MIB
Module:	The compliance statement for SNMPv2 entities which implement Cerberis3 QKD Node.
Description:	cerberis3QkdNodeCompliance

Name:	cerberis3QkdNodeGroup
Oid:	1.3.6.1.4.1.22328.2.1.3.2.1
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Group
SMI Type:	OBJECT-GROUP
Value List	IDQ-CERBERIS3-QKD-NODE-MIB
Module:	The current Cerberis3 QKD Node group of objects providing for management of Cerberis3 QKD Node
Description:	cerberis3QkdNodeGroup