Cost-Effective Quantum Key Distribution Solutions

Technical proposal for “A DISCRETE VARIABLE QUANTUM KEY DISTRIBUTION SYSTEM”

Prepared for the
Czech Technical University in Prague
Faculty of Nuclear Sciences and Physical Engineering

October 2024

Contents

1. Overview 3
2. Technical highlights 3
3. Power & Operating Conditions 6
4. Compatibility with other cryptographic devices, i.e. support for at least the ETSI QKD 014 standard 7
5. Reconfiguration Mechanism. 7
6. HW Reconfiguration 8
7. Data Accessibility. 10
8. Testing configurations 10
9. HEQA Security compliance to Technical University in Prague requirements 13

1. Overview

In relation to the tender for the “A DISCRETE VARIABLE QUANTUM KEY DISTRIBUTION SYSTEM”, we are honored to present this proposal for the Czech Technical University in Prague Faculty of Nuclear Sciences and Physical Engineering.

HEQA Security is a pioneer in creating cost-*effective, easy-to-integrate, ultimately secure Quantum Key Distribution (“QKD”) systems* designed for operational fiber optic networks.

This document outlines the description of the QKD devices and Heqa compliance with the tender requirements and services.

The first years of Heqa-Security's R&D began in the university's physics laboratory, similar to the Czech Technical University in Prague Faculty of Nuclear Sciences and Physical Engineering. A few years ago, Heqa-Security expanded into the commercial world by securing a commercial-standard product with unique and unmatched security and practical scalability. Our products have been commercially available for more than 2 years and installed in various customers, such as the Israeli Ministry of Defense, some EU universities, several data center providers, different communications operators, and financial institutions.

2. Technical highlights

For this tender HEQA-Security a **Sceptre Link** QKD transmitter/receiver pair in its *Dark Fiber* (DF) version. The Sceptre Link DF is a *Decoy-state BB84 QKD system*, with the quantum channel assigned to 1550 nm. Although it is designed to operate over a dedicated dark fiber, with a proper system design it is possible to multiplex the quantum channel with other optical channels.

Figure 1. Photographs of the QKD boxes offered

Heqa-Security's **Sceptre series** of QKD systems uses the *Decoy-State* BB84 protocol, the most widely used QKD scheme globally, with weak coherent states based on time-bin encoding and phase encoding. The

Sceptre systems are an all-in-one QKD solution. Each end, occupying only one rack unit, 1U, includes the physical layer for quantum state generation (**Sceptre Link qTx**) or measurement (**Sceptre Link qRx**), the post process hardware, the key management system and a web-based UI

This offering includes all the hardware and software required for key reconciliation and key management for a QKD link.

Sceptre systems can be configured to operate on a multiplexed fiber (quantum channel at 1310 nm) or on a dark fiber (quantum channel at 1550 nm).

qTx/ qRx	Multiplexed configuration (Mux)	Dark fiber configuration (DF)
Physical Parameters		
Enclosure	19" mountable chassis, 1U, 23" deep	
Dimensions	W 435 mm x L 580 mm x H 44 mm	
Operating Conditions		
Temperature (ambient)	5°c-40°c	
QKD Properties		**Dark fiber configuration (DF)**
Configuration	Single fiber multiplexing the Quantum channel, Clock channel, and user DWDM data channels	For each of qTx/qRx Two fibers: 1. Dark fiber for the quantum channel* 2. Fiber for the DWDM clock channel, and user DWDM channels. *The clock channel can be multiplexed over the dark fiber with the quantum channel
Protocol	Decoy state BB84	
Source	Weak Coherent Pulses	
Epsilon	4×10^{-9}	
Fiber type	SMF-28, G.652 compliant	
Secure Bit Rate		**Dark fiber configuration (DF)**
Typical max channel loss	>20dB	>20dB
Typical sbps @0dB	0km, 24k	0km, 24k
Typical sbps @4dB	12km, 21k	20km, 21k

Typical sbps @12dB	35km, 8k	60km, 8k
Typical sbps @20dB	60km, 2k	100km, 2k
Quantum Channel		
Quantum channel wavelength	1310nm	1550nm
Connector type	LC/PC	LC/PC
Fiber loss	0.35 db/km @1310nm	0.2 dB/km @1550nm
Clock Channel		
Wavelength	Any CWDM or DWDM optical channel	
Optical module	SFP+ approved by HEQA Security	
Fiber type	SMF-28, G.652 compliant	
Connector type	LC/PC	
Key Reconciliation and Key Management Channel		
Type	IP based	
Interface	RJ45	
Key Interface		
Method	ETSI GS QKD 014 V1.1.1 (2019-02) REST based key delivery API Cisco SKIP protocol	
Interface	RJ45	
Power		
Input	Auto-ranging 90-240VAC 50/60Hz	
Consumption	<200W	

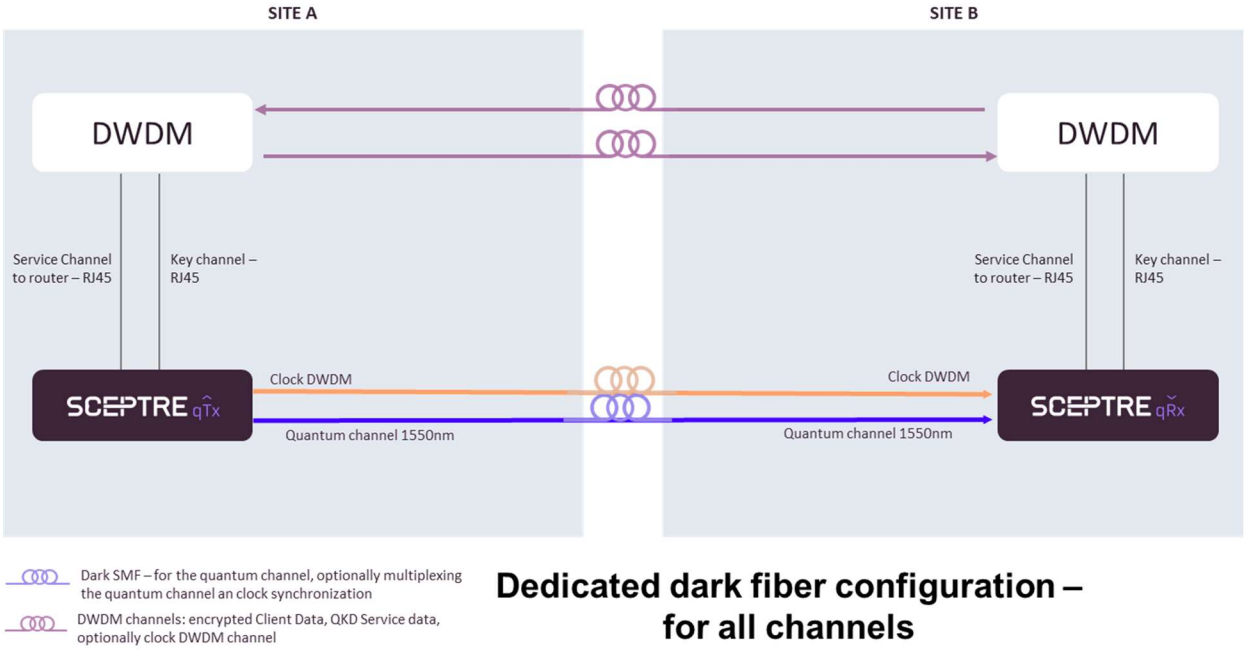

Figure 2. Basic connectivity in a Sceptre system in Dark Fiber configuration

The Figure 2 schematically shows the typical **Sceptre Link** *Dark Fiber* (DF) connectivity . The optical clock synchronization channel is based on a removable module (*pluggable*) SFP+. It can be assigned to the C-band and multiplexed with the DWDM data channels, it can be assigned to 1310 nm and multiplexed on the dark fiber (using external filters), or run on another fiber, as shown in Figure 2 (mainly recommended for laboratory testing).

To simplify the initial installation and testing processes, the QKD systems is supplied with an Ethernet hub (at no additional cost) and already configured to operate "out of the box", without the need for local network configuration.

3. Power & Operating Conditions

Sceptre systems are supplied ready for deployment in data centers and central offices in production, ready to operate in industrial/professional environments.

Sceptre systems are designed to be installed in 19-inch cabinets with a depth of 600 mm. All accessory elements for installation are supplied, including rails with adaptable lengths for installation in deeper cabinets. The systems are equipped with a standard AC plug, to be used with C13 power cables to connect to the mains. The systems are certified to EU standards for electrical safety.

The supplied transmitter/receiver pair operates in typical data center temperature and humidity conditions. The operating temperature range is 5°C to 40°C and a non-condensing humidity. The system

has integrated tests (BIT) that monitor internal and environmental conditions and employs means of protection to prevent damage to the system in case of exception to the defined operating limits.

4. Compatibility with other cryptographic devices, i.e. support for at least the ETSI QKD 014 standard

The **Sceptre** system uses the ETSI GS QKD 014 API for key pulling by external devices. Our API implementation has been successfully tested by some of the leading vendors, such as Ciena and Nvidia, as well as several other crypto providers.

Included in this offer is a web-based system emulator for remote integration with the ETSI GS QKD 014 API. It will be available for the entire duration of the technical support.

Cisco has developed its own key pulling API, called the Secure Key Integration Protocol (SKIP), which is used for IPSec and MACSec. The offered **Sceptre** pair also supports this Cisco SKIP API.

To learn more about how this API works, please visit:
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption -ppk.pdf

5. Reconfiguration Mechanism.

The **Sceptre** system can be reconfigured and monitored using a REST-based API. This REST-API is documented for use ("**Annex 1. Sceptre REST API Manual"** attached).

Additionally, a Graphical User Interface (GUI) is provided, based on this REST-API, for interactive operation and monitoring, thus avoiding the need for customers of the **Sceptre** system to develop their interfaces ("**Annex 2. Sceptre User manual.pdf**"). It should be noted that the API allows a wider range of functions for the monitoring and control of KMS and QKD parameters.

The **Sceptre** QKD system protocol can be reconfigured using standard software engineering techniques. Below are some of the functionalities and associated parameters that can be reconfigured:

1. Decoy-state *parameters*:
   a. Average number of photons per bit (μ-value)
   b. Quantum state distribution, i.e. the probability of transmitting certain states (x4 signal states, x4 decoy states, x1 vacuum state).
2. Configuring the Random Number Source
   a. Selection between different methods for state randomization: TRNG, PRBS (not secure, only for use in R&D), or Periodic States (not safe, only for use in R&D)
3. Quality of Service.
   a. Limitation of the life of the key age.

b. Limitation of the key buffer size.
c. Bit verification configuration (bits sacrificed to verify that the EC + PA procedure produces identical blocks on both sides.
d. Format of the key entered.
e. Change of the type of certificate required for the extraction of the key by the client.

4. Key Exchange Protocol.
   a. ETSI GS QKD 014 or Cisco SKIP

6. HW Reconfiguration

The **Sceptre** system can be reconfigured in different aspects: physical connectivity, optical operation, and logical operation.

Physical reconfiguration: the systems are designed to operate with SFP+ modules for clock synchronization. The SFP+ port is on the front panel and physical reconfiguration can be done by plugging and disconnecting (*plug-in* / *plug-out*) different SFP+ modules. For example, physical reconfiguration allows you to switch between different fixed DWDM channels, allowing you to use LR SFP+, use tunable SFP+, or use gray SFP+ (on the receiver side).

Below is the image of the front panel with the optional physical connections. The top figure is the qTX module ("Alice"), and the bottom figure corresponds to the qRx module ("Bob").

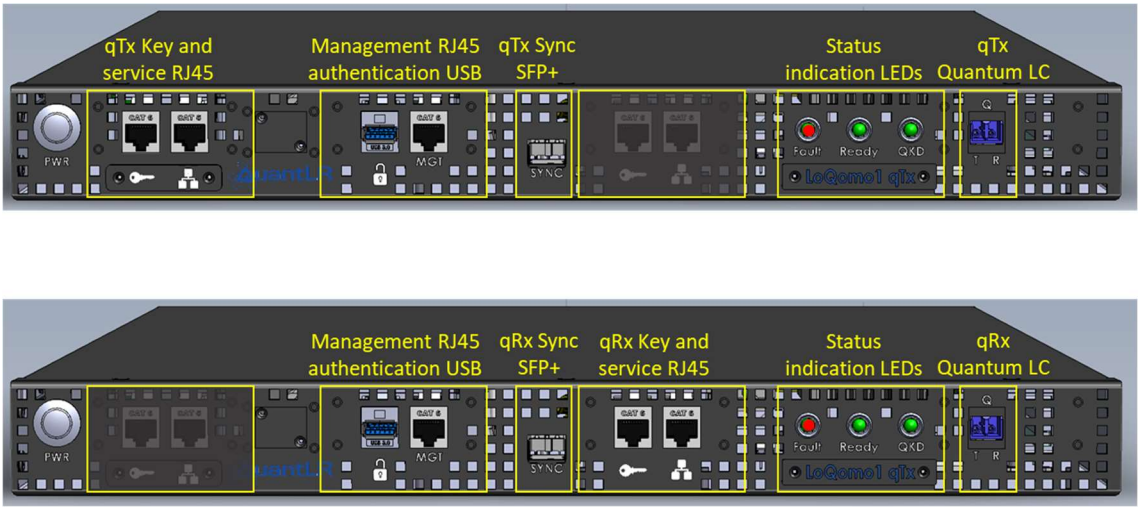

Figure 3. Physical connections of the qTX/qRx pair offered for Lot 4

Optical and logical reconfiguration is done by reconfiguring the software, firmware, and FPGA (*Field-Programmable Gate Array*). Standard techniques such as APIs and language interpreters are used for this reconfiguration.

The system allows remote reconfiguration of parameters via the management port, connected to the laboratory network.

The user manual attached to this report details the configuration capabilities; among others, it has instructions for changing Linux operating system configurations or instructions for updating software. Instructions and examples for using the browser-based GUI to reconfigure different parameters can also be found in the user manual; this GUI is implemented on top of the API.

Other particular methods, based on standard software engineering techniques, such as CLI and Python scripts, are also used to perform some of the reconfigurations and are made available via APIs before delivery to Czech Technical university in Prague. All proprietary reconfiguration methods that are not implemented via API interface are well-documented and ready for use.

No special equipment or additional licenses are required for system reconfiguration.

All reconfiguration options are documented in the user manuals and will be explained in detail during the training session. Similarly, additional support for all reconfiguration mechanisms will be provided to the Czech Technical University in Prague Faculty of Nuclear Sciences and Physical Engineering.

7. Data Accessibility

The functionalities and parameters associated with the quantum information that is transmitted in photons of the Sceptre QKD system encoding/decoding system can be reconfigured using standard software engineering techniques. Below are some of those features and associated parameters that can be reconfigured:

5. Detector properties (for both SPADs):
    a. Detector gate width
    b. Detector hold-off time
    c. Detector Temperature
    d. Detector comperator Threshold
6. Interferometer stabilization feedback loop (for the qRx end):
    a. Time interval between steps
    b. Step Size
7. Properties of the Laser:
    a. Laser power μ
    b. Gain-switch window width
    c. Gain-switch window delay

8. Testing configurations

The Sceptre system has been successfully tested on QKD test beds in several countries in the EU, USA, Canada, and Israel. For reasons of confidentiality, we can cite Nvidia, some large optical vendors, the Israeli government, and one of the world's largest data centers, all of which have tested the Dark Fiber Sceptre system. These tests included but were not limited to: extracting keys from multiple systems and encrypting lines up to 400G, both in the lab and in the field. After the corresponding tests, these customers and partners declared that the Sceptre system is suitable for deployment in production transmission networks.

The system can be tested on both the physical layer and the cryptographic layer. The typical test setup for a DF QKD link, such as the one offered for this tender, for example, includes the blocks in the figure below:

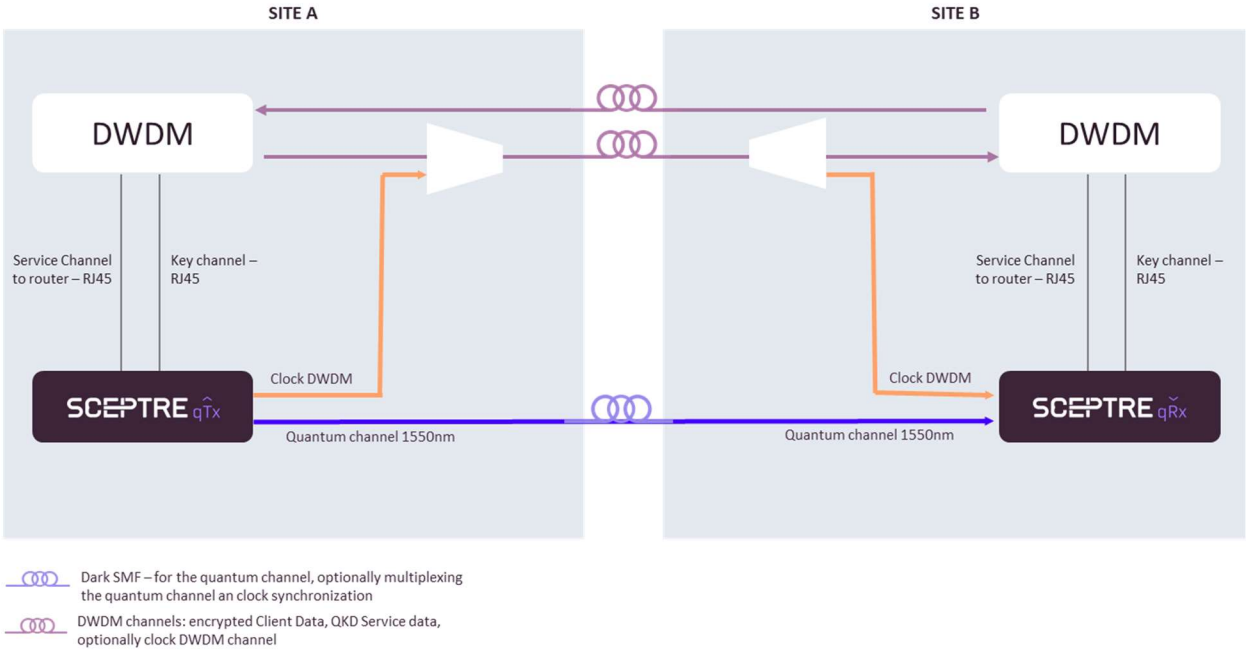

Figure 4. Example of a test configuration for a Dark Fiber QKD link, where the clock synchronization channel is multiplexed with the data channels

The figure above shows the connectivity between the different elements of the system. The quantum channel at 1550 nm is transmitted directly between qTx and qRx via a dedicated dark fiber. The clock synchronization channel (any DWDM channel) is multiplexed and demultiplexed with the system's DWDM channels into a standard multiplexing unit that can also be amplified. At the other end of the fiber, the clock sync channel is demultiplexed and the qRx SFP+ module is entered. Each system has 3 ethernet ports, one for keys, one for communication between qTx and qRx and one to the management network (not shown in Figure 4); The latter is used for remote monitoring and system reconfiguration. HEQA supplies an 8-port Ethernet switch that implements the management network for easy initial installation.

As examples of the tests to be carried out in the **physical layer** of Czech Technical University in Prague Faculty of Nuclear Sciences and Physical Engineering that may be relevant for this tender we can mention:

1. Secure bitrate (SBR) testing as a function of fiber length.
2. SBR tests with added attenuation (no added dispersion) for a fixed fibre length.
3. Tests on the coexistence of the 1550 nm quantum channel with a 1310 nm clock synchronization SFP+ (better use of infrastructure at the cost of a worsening of the SBR, requires external filters).
4. For a specific configuration, performance tests by modifying QKD system parameters:
    a. Detector properties (for both SPADs).
        i. Modifying the width of the detector gate: *trade-off* between a high *dark* count and a non-uniform detector bias for the different time intervals (shorter gate).
        ii. Modifying the detector hold-off: with low attenuation, a short hold-off will increase the SBR; with high attenuation, a long hold-off will increase the SBR.

   iii. Modifying the temperature of the detector TEC so that it operates at a higher ambient temperature, with a *trade-off* between a wider temperature range and reduced performance.
   iv. Modifying the detector threshold: higher detection efficiency with higher dark counts.
  b. Properties of the laser
   i. Laser Power μ Setting – A high μ value will result in a higher SBR when there is a high noise level in the detector or high attenuation. For low noise and low attenuation, a lower μ will result in a higher SBR.
   ii. Configuring the distribution of the *decoy state*: can be optimized based on μ.
   iii. Gain-switch *window width setting*: Gain switching is used for phase randomization between successive bits. A narrow window: fewer dark counts, but a lower laser uniformity.
   iv. Setting the width and position of the bits within the laser operation window: required especially when the window is narrow, to position the bits during periods of uniform laser power.
5. Tests of the stability of the detection interferometer against temperature changes. Setting the parameters of the feedback circuit (on the qRx side).
  a. Time interval between laser frequency correction steps.
  b. Laser frequency correction step size.
6. End-to-end solution:
  a. Testing on the maximum key extraction rate (limited by the HTTPS request rate); More than 10 successful key requests are expected per second.
  b. Connecting and Disconnecting Different Cables: Quantum Channel, Clock Channel, Service Channel, Key Channel, Management Channel, Power and Test Cable:
   i. Recovery time.
   ii. Key Availability.
   iii. Other monitored system parameters.

Test results can be obtained using the API ("**Annex 1 Sceptre REST API Manual.pdf**" attached) or the GUI ("**Annex 2. Sceptre User Manual**" attached). Among the parameters that can be monitored are:

1. Total QBER: The combined bit error rate of all signal states.
2. Decoy QBER: Combined bit error rate of all decoy states.
3. QBER by state: QBER measured for each of the 9 states (signal x4, *decoy* x4, empty x1).
4. Secure Bitrate: The bitrate used for the key, after post-processing.
5. Raw bitrate: The bitrate before *sifting* and post-processing.
6. Raw bitrate by state: The bitrate before *sifting* and post-processing for each of the 9 states.
7. Measured Photon Rate: Rare photons count for each of the 2 SPADs.
8. Temperatures of the enclosure and components: measured with the sensors in the **Scetpre** enclosure and reported by different modules in the system.
9. Component currents and voltages: measured by different system modules.
10. SFP+ Power Input and Output: Measured by the SFP+ modules at both ends.
11. Watchdogs: Optical control of the inputs and outputs of optical components and filters at both ends; can be used to identify attacks.
12. Other standard telemetry, as specified in the user manual and API manual.

9. HEQA Security compliance to Technical University in Prague requirements

A system (Sceptre Link) means a set of a transmitter and a receiver (Alice & Bob), with an integrated Key Management System (KMS).

Annex No. 6 to the Procurement Documents

Technical parameters and evaluation for public contract "A DISCRETE VARIABLE QUANTUM KEY DISTRIBUTION SYSTEM"

A) MINIMUM TECHNICAL REQUIREMENTS OF THE CONTRACTING AUTHORITY

		Participants will supplement the specific values offered for the technical parameters or if no specific values are requested, indicate YES/NO	Control of technical parameters by the evaluation committee
The subject of delivery must work with encoding into discrete variables and must meet the following basic technical requirements:			
1.	Prepare & measure with BB84 protocol	**YES**	
2.	quantum channel for fiber communication in the C band region (near 1550 nm);	**YES**	
3.	the following information must be submitted as part of the offer:		
	- repetition frequency of the laser;	**80MHz**	
	- typical/guaranteed efficiency of detectors;	**20%**	
	- number of detector dark counts	**DCR<500 per detector**	
	- dead time of detectors;	**15-40 Micro sec – it is configurable**	
	- what RNG is used:	**QRNG Integrated Circuit**	
	- typical error rate (QBER)	**1.5%**	

	- the extent of compatibility with other cryptographic devices (e.g. ETSI QKD 014), which standards the device meets;	**YES ETSI 014, Cisco SKIP**	
	- used connectors for optical and electrical interfaces;	**YES LC/PC, RJ45**	

B) The quality of the performance offered for evaluation purposes

Č.	**Parameter**	**Criterion type**	**Parameter offered by Participant**	the number of points assigned by the evaluation committee
1.	Possibility to preview the optical part	c	**YES – Heqa will Provide photos of the interior of the device including the optical system.** **During the training, the customer will be able to see the inside of the device. Heqa will bring another QKD system that will allow the customer to view it in detail.**	
2.	The possibility of connecting external detectors	c	**NO**	
3.	Software Libraries: software libraries for system control, coincidence measurements, error rate estimation, and key sifting with well well-described API interface	c	**YES**	
4.	Data Accessibility: Raw outputs of detectors and sifted key fully accessible to users.	c	**YES**	
5.	Software for monitoring and controlling the entire system	c	**YES**	
6.	Communication Interfaces: Ethernet or USB or other industry standards	c	**YES**	

Č.	Parameter	Criterion type	Parameter offered by Participant	the number of points assigned by the evaluation committee
7.	Compatibility with other cryptographic devices, i.e. support for at least the ETSI QKD 014 standard	c	**YES**	
8.	Error correction and privacy amplification	c	**YES**	
9.	Maximum allowable losses for a secure key rate higher than 10 kbit/s	a	**10dB**	
10.	Faster delivery (min 1 month – max 4 months)	b	**1 month**	
11.	Extended warranty (min 2 years - max 5 years)	a	**2 years**	

** Column highlighted in green will be filled in by Participant*