Quantum Key Distribution Over Metropolitan Fiber

Quantum Corridor White Paper

Dr. Bruce Chesley, Ph. D.
Ryan Lafler, CCISO
Patrick Scully, P. Eng., MBA

December 2025

Table of Contents

1. Abstract

The advent of quantum computing presents a significant threat to modern cryptographic systems, placing government, commercial and critical infrastructure communications at risk. Quantum communication is a pre-requisite to harnessing the benefit of quantum computing. As such, this white paper documents the implementation and validation of a Quantum Key Distribution (QKD) solution and its integration over a commercial metropolitan network to mitigate that threat. The goal was to demonstrate the first cross-state QKD over a live commercial metro fiber network between Illinois and Indiana, integrating with high-throughput, commercially available encryption systems. The findings from this study have far-reaching impact on commercial implementation of quantum communication tools to develop quantum safe networks, enable networking of quantum computers to solve previously large-scale unsolvable problems and future AI data centers.

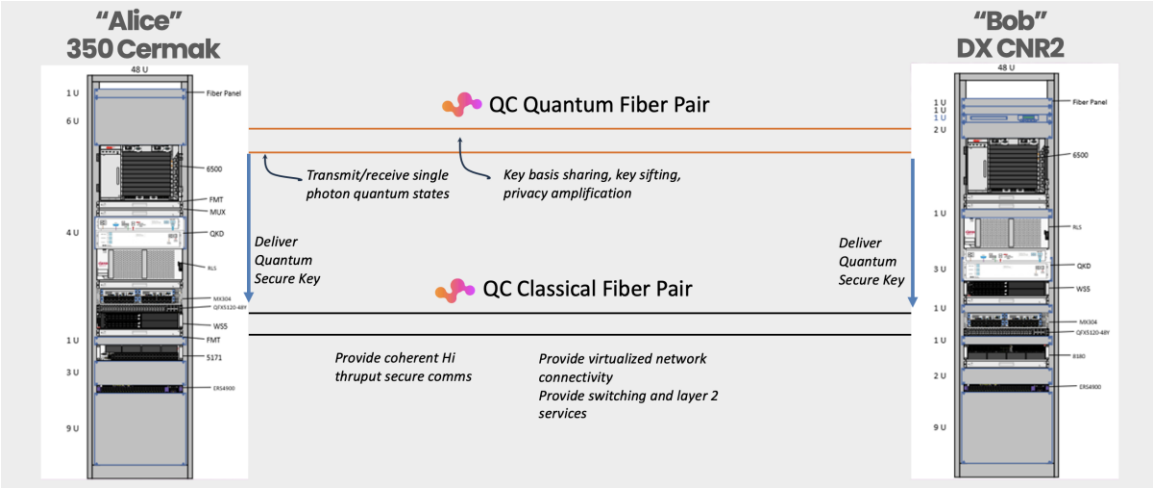


Figure 1 – Proof-of-Concept System Overview

2. Introduction

Quantum computing stands at the threshold of redefining the very foundations of information technology. With its promise of exponentially increased computational power, quantum computers are anticipated to tackle challenges that remain intractable for classical machines, opening new avenues in fields such as cryptography, material science and complex system modelling. For technology professionals, researchers and decision-makers, understanding the trajectory of quantum innovation is vital—not only for harnessing its benefits, but also for preparing for the transformative impacts it will have on industry and society.

While the spotlight often falls on the remarkable capabilities of individual quantum computers, it is the prospect of networking these systems that will truly unlock their collective potential.

Quantum networking is a future-looking technology that envisions interconnected quantum devices working collaboratively, enabling enhanced scalability, distributed quantum processing and secure communication on an unprecedented scale. The quantum internet, though still in its formative stages, represents an ambitious vision for global collaboration and resource sharing, promising to amplify the impact of quantum computing far beyond isolated breakthroughs.

Current foundational technologies are laying the groundwork for this quantum-connected future. QKD is one such technology to enable secure transmission of information, leveraging the fundamental principles of quantum mechanics to ensure privacy and resilience against emerging threats.

By implementing QKD across production-grade fiber infrastructure, Quantum Corridor seeks to enable scalable and commercially viable quantum-safe networking, and in so doing lay the foundation for the future of quantum networking.

The remainder of this paper focuses on the key activities undertaken to demonstrate this initial step towards a quantum-safe future:

- Establish a real-world QKD link between two Tier III data centers – ORD10 (350 Cermak) (Chicago) and Digital Crossroad (DX) (Hammond, IN) over a multi-state commercial network (see Figure 1).
- Validate the stability of the quantum channel over a metropolitan commercial network in the presence of typical environmental disturbances including roadways, railways and bridges (Figure 2 illustrates the fiber path through a dense urban environment).
- Demonstrate the delivery of high-speed quantum-safe communication links by integrating Generally Available (GA) coherent optical telecommunication equipment with commercially available QKD systems.
- Validate the stable operation of the quantum-secured environment over a prolonged period under real-world conditions.

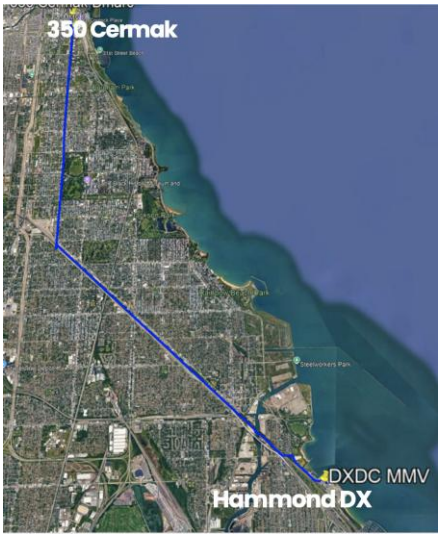


Figure 2 - Direct Fiber Link Between ORD10 and Digital Crossroad Data Centers

3. Study Platform

Figure 3 provides a high-level block diagram of the network configuration for this study, which includes the following four components:

(i) the fiber infrastructure between the two endpoints
(ii) the photonic system multiplexing the encrypted channels
(iii) the encryptors
(iv) the QKD system

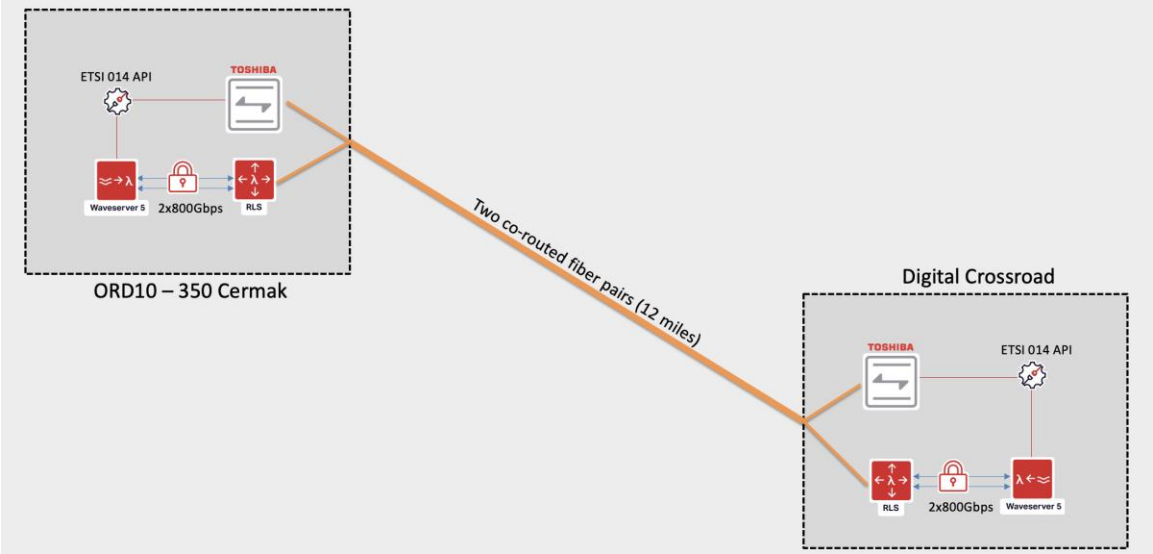


Figure 3 - High-Level Network Configuration

3.1. Infrastructure

This activity utilizes fiber infrastructure that is a key component of Quantum Corridor's backbone network, routed through protected conduits between the ORD10 data center at 350 E. Cermak Rd. in Chicago and the Digital Crossroad data center at 100 Digital Crossroad Dr. in Hammond, IN.

Over the 13.55-mile stretch between the two locations are multiple fiber strands offering the most direct path between the facilities. The fibers themselves are G.652d low-loss fibers routed in protected conduits and buried underneath the region's transit infrastructure, including roadways, railways and bridges, as illustrated in Figure 4.

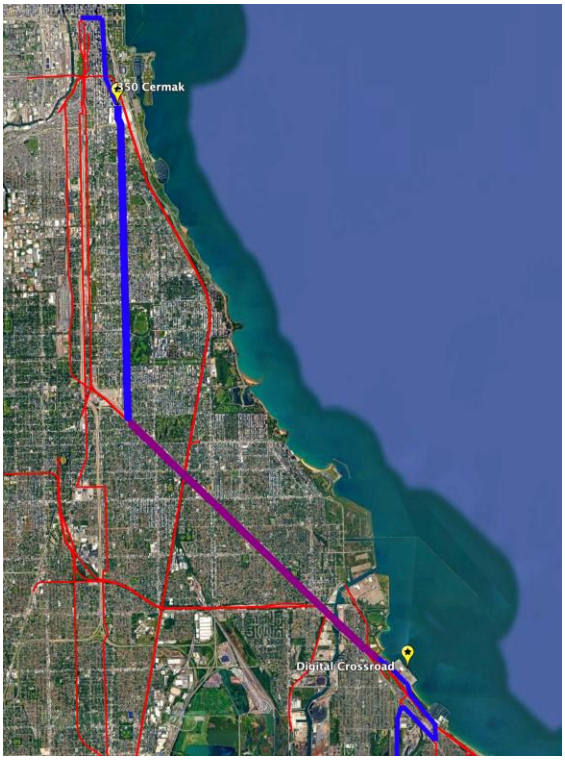


Figure 4 - Overlay of Fiber Route and Metropolitan Railway System

The two fiber pairs used in this PoC demonstration were co-routed along QC's metropolitan route, with routing accommodations for roadways and bridges as illustrated in Figure 5.

Figure 5 - Examples of Metropolitan Fiber Routing

Prior to this activity, the fiber pairs were characterized and the following OTDR traces in Figures 6 and 7 measured a 7.25dB loss on one pair (used for the classical channels) and 7.57dB loss on the second pair (used for the quantum channels).

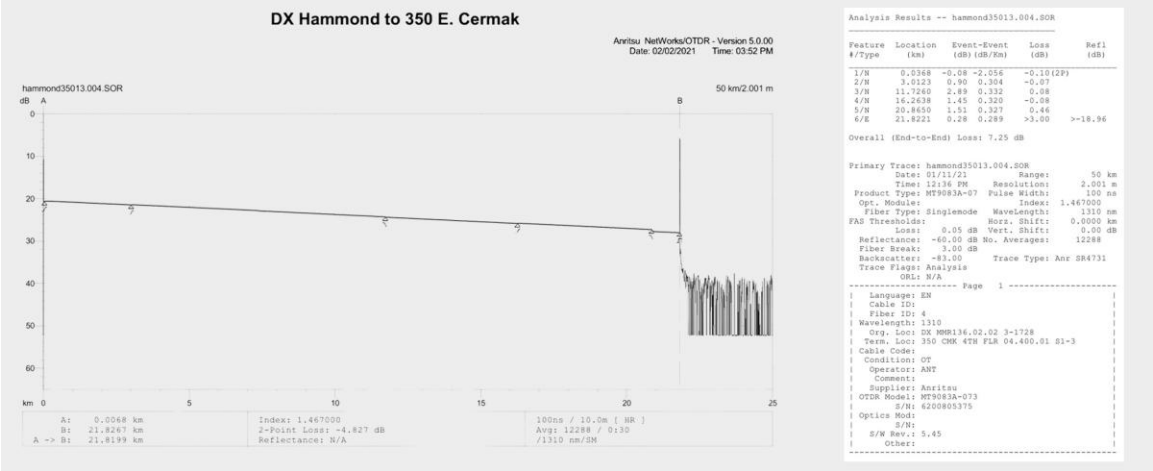


Figure 6 - OTDR Trace for Fiber Pair 1 (Used for Classical Channels)

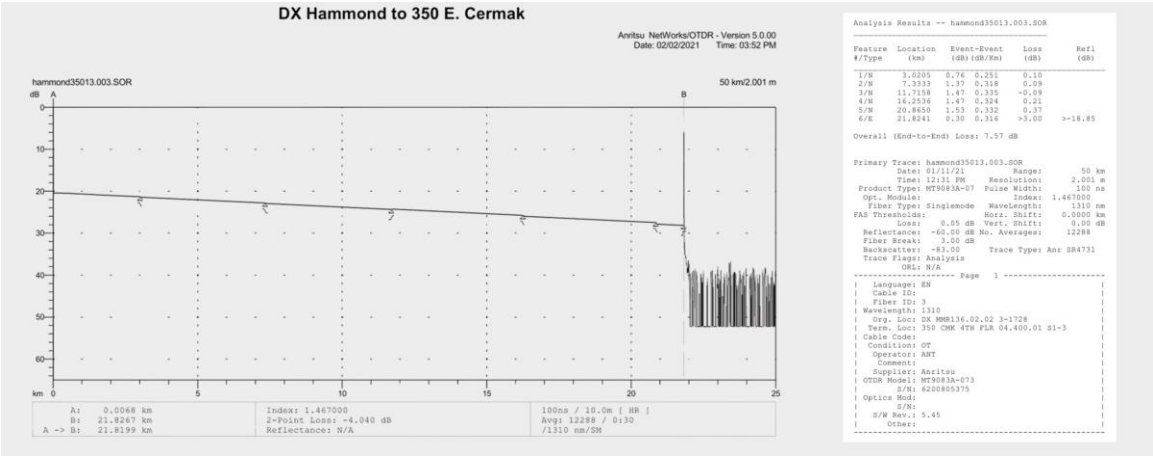


Figure 7 - OTDR Trace for Fiber Pair 2 (Used for Quantum and Service Channels)

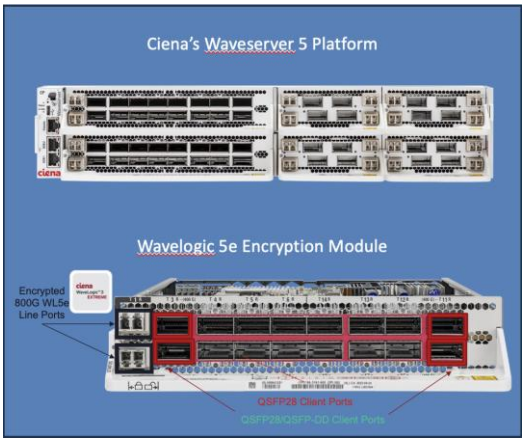
3.2. Photonic Layer

The photonic layer used for this activity was Ciena's 6500 Reconfigurable Line System (RLS). Each location was fitted with a 4RU-high R4 chassis equipped with a C-band Reconfigurable Add Drop Multiplexer (ROADM) RLA. The system multiplexed two classical 800Gbps, 95Gbaud coherent channels and amplified the channels for transmission across the 13.55-mile network between the two data centers.

The flexible 16-channel colorless mux/demux filters used on the RLS system allow for the multiplexing of the existing 800Gbps, 95 Gbaud, coherent encrypted channels and is ready to support the upcoming 1.6Tbps, 200Gbaud, coherent encrypted channels.

3.3. Encryptors

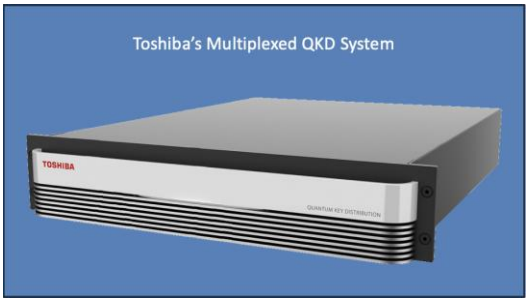
The encryptors used for the activity are the Wavelogic 5e Encryption Modules, part of Ciena's Waveserver 5 platform. Each Wavelogic 5e Encryption Module is equipped with a pair of 800Gbps line ports generating a 95Gbaud coherent signal. Each line port supports a mix of 100G and 400G client services (100GE signals are used in this activity). Each line port also supports independent OTNsec encryption functions, powered by bit-transparent FIPS 140-3 Level 2 certified AES-256-GCM encryption engines.



The Waveserver 5 chassis also provides an ETSI 014 compliant external key interface to allow the encryption modules to request and obtain encryption keys from an external system. In this activity, the external key interface (REST API) is configured to request keys from the co-located Toshiba QKD system. The Waveserver system was running generally available (GA) software version 2.4.52.

3.4. Quantum Key Distribution

Toshiba's Multiplexing (MU) QKD servers were used for this PoC. The pair of servers was graciously loaned to Quantum Corridor by Toshiba and the University of Chicago for the preparation and execution of this activity.



The MU QKD system from Toshiba is designed to multiplex both classical DWDM channels and the quantum and control channels used for key generation. For the purpose of this activity, Quantum Corridor dedicated a fiber pair to the QKD system independent of the classical DWDM channels on the RLS system due to a wavelength conflict between the two systems that were on hand. The Toshiba MU system uses a 1310nm O-band quantum channel for key generation. The Transmitter node (Alice) was located at ORD10 while the Receiver node (Bob) was located at Digital Crossroad as illustrated in Figure 1. Each was also equipped with a Control Server for communication with the Ciena encryptors.

3.5. System Configuration

The complete system configuration and interconnection is depicted in Figure 8. At both locations, in addition to the equipment described in the above sections, an Avaya ERS4950 layer 2 switch was configured between the management ports of the Waveserver and Toshiba devices.

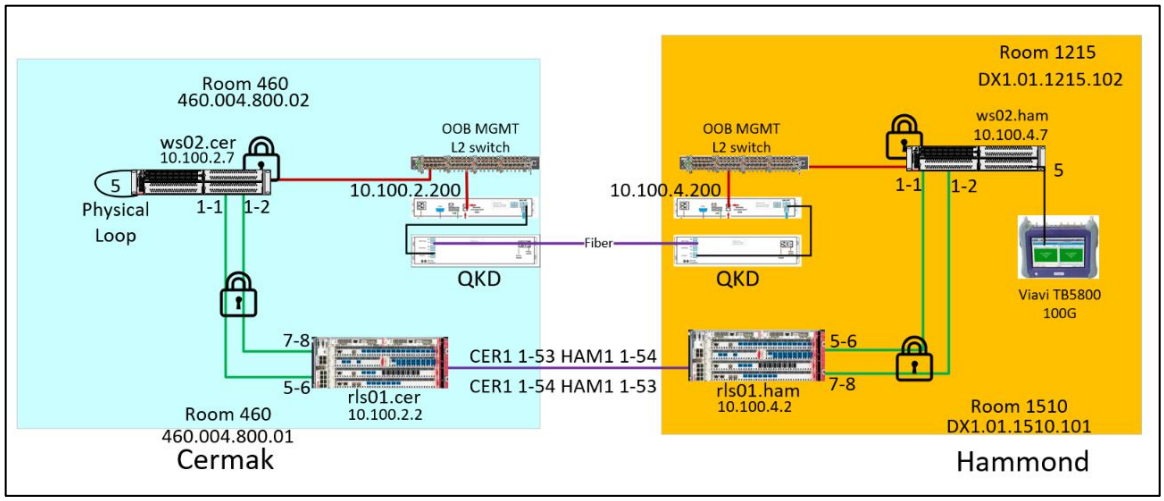


Figure 8 - System Diagram

While a direct connection between the two devices would have offered enhanced security, the Waveserver platform supports only a single management port. To enable simultaneous access for both ETSI GS NFV-IFA 014 REST API integration and general management functions, an intermediary switch was necessary.

With both the QKD system and the encryptors being co-located, and with all equipment consolidated in a single locked cabinet inside a highly secure Tier III data center, this provided a high level of physical security. Additionally, the ETSI 014 interface over which the keys are exchanged is further protected over an authenticated and encrypted communication channel.

Completing the configuration was a Viavi T-BERD/MTS-5800 100GbE network tester located at the Digital Crossroad facility; the ports at the ORD10 facility were looped back. This configuration allowed latency and throughput tests to run across the system over a 48-hour period.

4. Equipment Set-Up and Configuration

4.1. Phase 1 – QKD Installation & Configuration

Both the Toshiba QKD Transmitter (“Alice”) and Receiver (“Bob”), along with their associated Control Servers, were installed in existing locked equipment cabinets at the ORD10 and Digital Crossroad facilities, respectively. The QKD units, Alice and Bob, were connected to the 13.55-

mile, 7.6dB fiber pair between the two locations. Each unit was also connected to their respective Control Server as illustrated in Figure 9.

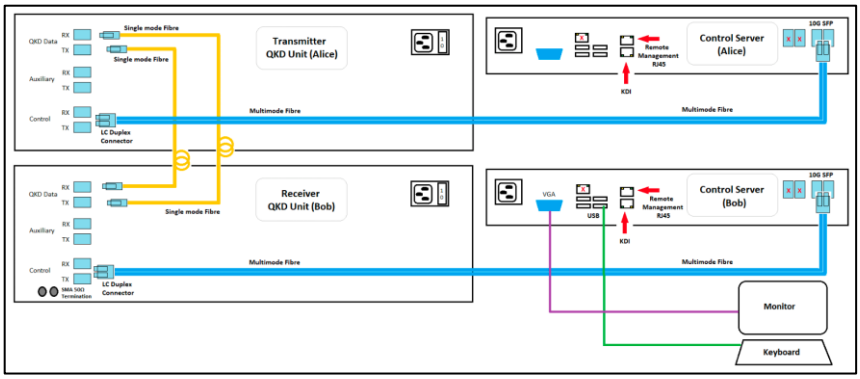


Figure 9 - Overview of Toshiba QKD and Control Servers Connectivity

With all equipment properly connected, the system was powered on and initialized. With the system fully initialized and stable, a GUI was opened on Bob's Control Server and successful key generation was confirmed, measured at 1,830 kbps with a quantum bit error rate of 3.72%.

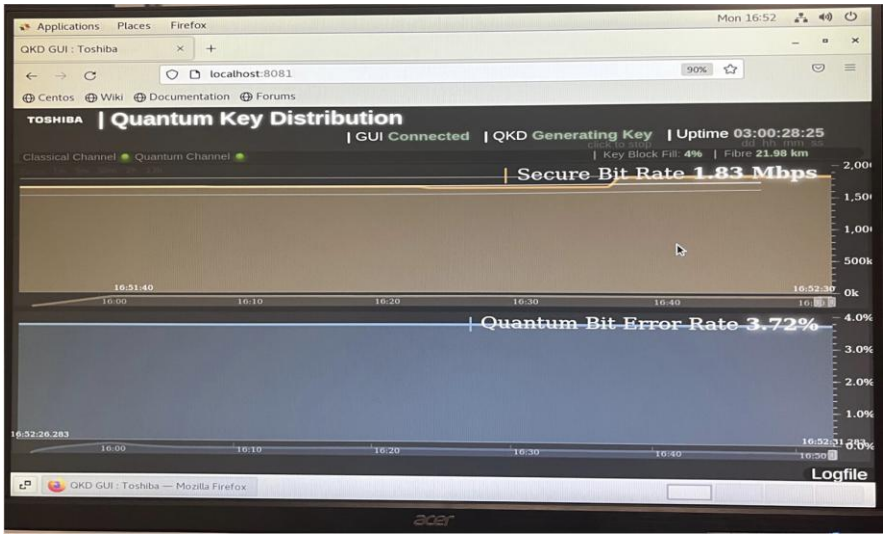
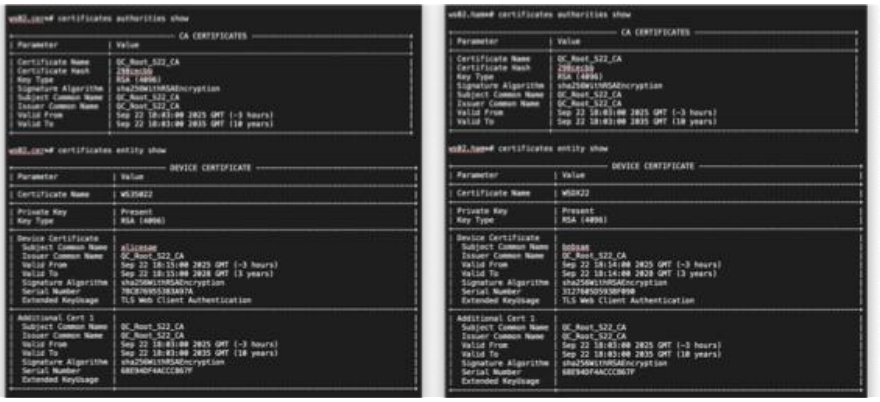


Figure 10 - Toshiba QKD GUI Showing Secure Key Rate and QBER

4.2. Phase 2 – Integration with Ciena Encryptors

The ETSI 014 key delivery API requires a mutually authenticated TLS session for secure key exchange. The initial step to implementing the key exchange interface is thus to generate the required authentication certificate. Although test certificates could be self-generated on the Toshiba servers, new certificates for both the Toshiba QKD Control Servers and the Ciena Waveserver 5 chassis were created using Quantum Corridor's Certificate Authority (CA) infrastructure to demonstrate the solution's integration into a commercial network. The

certificates were then loaded onto the various devices as shown in Figure 11 (note that there are no similar interfaces on the Toshiba units).



ORD10 (Alice) Digital Crossroad (Bob)

Figure 11 - Screenshot of Certificate Provisioning on Ciena Waveserver Encryptors

With the certificates properly loaded on the devices, the Ciena Waveserver external key interfaces were configured with the information related to their respective QKD Control Servers, and the key request interval was reduced to 1-minute (lowest available setting), which would force the two 800Gbps encryptors to each request a new QKD key (and configure it on its internal AES encryptor) every minute.

```
ws02.ham*# system encryption key-server show
------------ SYSTEM ENCRYPTION EXTERNAL KEY ETSI STATUS ------------
| Parameter                          | Value                       |
+------------------------------------+-----------------------------+
| Admin State                        | Enabled                     |
| Operational Status                 | Up                          |
| Entity Certificate                 | WSDX22                      |
| Server CA Certificate              | QC_Root_S22_CA              |
| IP/Hostname                        | 10.100.4.150                |
| Secure Application Entity ID       | bobsae                      |
| Key Update Interval                | 1 minutes                   |
| Key Update Completed Log           | Enabled                     |
| Squelch On Key Update Failure      | Disabled                    |
| Key Update Failure Squelch Threshold | 72 hours                  |
+------------------------------------+-----------------------------+
```

```
ws02.cer*# system encryption key-server show
------------ SYSTEM ENCRYPTION EXTERNAL KEY ETSI STATUS ------------
| Parameter                          | Value                       |
+------------------------------------+-----------------------------+
| Admin State                        | Enabled                     |
| Operational Status                 | Up                          |
| Entity Certificate                 | WS35022                     |
| Server CA Certificate              | QC_Root_S22_CA              |
| IP/Hostname                        | 10.100.2.150                |
| Secure Application Entity ID       | alicesae                    |
| Key Update Interval                | 1 minutes                   |
| Key Update Completed Log           | Enabled                     |
| Squelch On Key Update Failure      | Disabled                    |
| Key Update Failure Squelch Threshold | 72 hours                  |
+------------------------------------+-----------------------------+
```

Figure 12 - External Key Interface Provisioning on Ciena Waveserver Encryptors

It was observed that the actual key request interval was closer to 90 seconds (vs. expected 60 seconds), however this was not material as the main purpose was to force a higher key refresh rate for testing purposes.

5. Testing & Validation

5.1. Link Up Confirmation

The initial validation of the configuration was a green indicator on the Viavi Network Test device, confirming that the link was up and transmitting traffic. Successful traffic transmission on the Ciena Wavelogic 5e Encryption Module is an indication that the encryption subsystems are functional and properly configured with confirmed authentication and AES-256-GCM keys as the units first undergo a complete FIPS 140-3 Level 2 secure initialization.

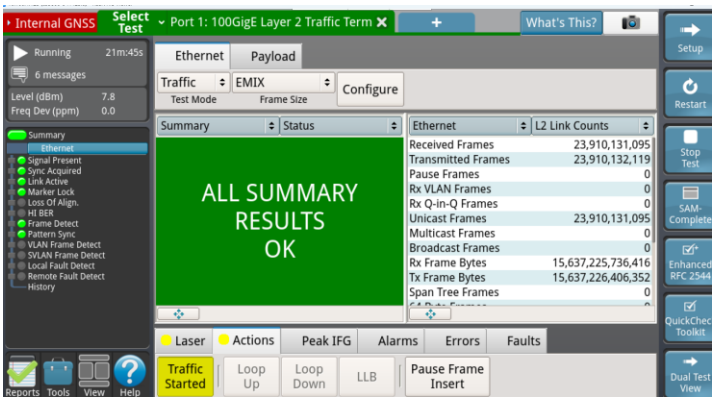


Figure 13 - Viavi Test Set Confirming Traffic Continuity

5.2. ETSI 014 Key Exchange Validation

The next step in validating the system's configuration and operation was to validate that the Wavelogic 5e Encryption Module was receiving and updating its AES key every "minute." The way the ETSI 014 interface is designed to operate, one of the encryptors is designed as the *Master*, issuing the initial key request command to its local QKD device (in this case its local Toshiba QKD Control Server). The Control Server then responds to this initial request with a QKD-generate key and a corresponding Key ID.

The *Master* encryptor then communicates the Key ID (not the QKD key!) over to its encryption peer, the *Slave* encryptor. The Slave then uses its ETSI interface to request the QKD Key that matches the received Key ID from its local Control Server. Once the two encryptors have securely received their (identical) QKD keys, they each load it into their AES encryption engines.

The Ciena Wavelogic 5e Encryption Modules are engineered to update the received QKD keys with no traffic interruption to ensure seamless operations in a commercial production environment.

The following Figures 14 to 16 capture the details of the process for the Waverserver encryptors for three consecutive key request intervals.

Logs from Waveserver @ DX
Requesting and Refreshing QKD Key Every ~Minute from Bob

Key Request #1	21:02:50.969784 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B..@.?.u.d..e...n.....<30>1 2025-09-18T21:02:50+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-2 (Key_ID is 0ad70325-7583-49ed-a9a3-993d376c7503) 21:02:50.969849 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B..@.?.u.d..e...n....=<30>1 2025-09-18T21:02:50+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-1 (Key_ID is 645955b6-3898-4871-b40a-283ea497bc4b) 21:03:08.595336 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 F..8.."@.?.h.d..e...n..$..<28>1 2025-09-18T21:03:08+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemFxternalKeyUpdateComplete [CienaWOS@1271.3 TIMF-FORMAT="UTC" FVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:03:08.595416 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 F..8.#@.?.h.d..e...n..$..<28>1 2025-09-18T21:03:08+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemFxternalKeyUpdateComplete [CienaWOS@1271.3 TIMF-FORMAT="UTC" FVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete
Key Request #2	21:04:20.969202 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B..@.?.._.d..e...n....1.<30>1 2025-09-18T21:04:20+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-1 (Key_ID is ec07f73c-af44-44ae-b4c5-29b09a266856) 21:04:20.969258 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B..@.?.._.d..e...n....|.<30>1 2025-09-18T21:04:20+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-2 (Key_ID is e080c01b-9738-476d-9409-aaff6e491500) 21:04:39.617687 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?.]'d..e...n...$..<28>1 2025-09-18T21:04:39+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:04:39.617738 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 F..8..@.?.]&d..e...n...$..<28>1 2025-09-18T21:04:39+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemFxternalKeyUpdateComplete [CienaWOS@1271.3 TIMF-FORMAT="UTC" FVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete
Key Request #3	21:05:50.969000 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B.h@.?.#cd..e...n....N.<30>1 2025-09-18T21:05:50+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-1 (Key_ID is 290acf5c-8db6-47fc-8ed6-7581b149791c) 21:05:50.969072 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.info, length: 294 E..B.i@.?.#bd..e...n.....<30>1 2025-09-18T21:05:50+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 KeyRetrieval [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-063" EVENT-NAME="KeyRetrieval" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval complete for Modem 1-2 (Key_ID is d964cdb5-4fb3-43be-970d-41e36d22dd54) 21:06:08.562323 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?...d..e...n...$..<28>1 2025-09-18T21:06:08+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:06:09.272721 IP 10.100.4.7.40558 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?...d..e...n...$..<28>1 2025-09-18T21:06:09+00:00 10.100.4.7 Ciena-Waveserver-5-R2.4.52 7616 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete

Figure 14 - External Key Interface Logs on Bob's Waveserver

Logs from Waveserver @ 350 Cermak
Requesting and Refreshing QKD Key Every ~Minute from Alice

Key Request #1	21:03:05.778789 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 E..`..@.?.p.d..e...^...L..<30>1 2025-09-18T21:03:05+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-1 (Key_ID is 645955b6-3898-4871-b40a-283ea497bc4b) 21:03:05.778867 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 E..`..@.?.p.d..e...^...LjH<30>1 2025-09-18T21:03:05+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-2 (Key_ID is 0ad70325-7583-49ed-a9a3-993d376c7503) 21:03:08.777610 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?.o@d..e...^...$..<28>1 2025-09-18T21:03:08+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:03:08.777671 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?.o?d..e...^...$..<28>1 2025-09-18T21:03:08+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete
Key Request #2	21:04:35.778115 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 F..`..>@.?.;od..e...^...L..<30>1 2025-09-18T21:04:35+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIMF-FORMAT="UTC" FVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-1 (Key_ID is ec07f73c-af44-44ae-b4c5-29b09a266856) 21:04:35.778173 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 F..`..=@.?.;pd..e...^...L..<30>1 2025-09-18T21:04:35+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIMF-FORMAT="UTC" FVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-2 (Key_ID is e080c01b-9738-476d-9409-aaff6e491500) 21:04:39.463860 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 F..8..@.?.7.d..e...^...$..<28>1 2025-09-18T21:04:39+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" FVENT-NAMF="ModemExternalKeyUpdateComplete" FVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:04:39.463912 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?.7.d..e...^...$..<28>1 2025-09-18T21:04:39+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" FVENT-NAMF="ModemExternalKeyUpdateComplete" FVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete
Key Request #3	21:06:05.777386 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 E..`..@.?.#.d..e...^...L..<30>1 2025-09-18T21:06:05+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-1 (Key_ID is 290acf5c-8db6-47fc-8ed6-7581b149791c) 21:06:05.777456 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.info, length: 324 E..`..@.?.#.d..e...^...LF.<30>1 2025-09-18T21:06:05+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 KeyRetrievalwithKeyID [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-064" EVENT-NAME="KeyRetrievalwithKeyID" EVENT-ORIGIN="dpe" TARGET-DS="running"] Key Retrieval with Key ID complete for Modem 1-2 (Key_ID is d964cdb5-4fb3-43be-970d-41e36d22dd54) 21:06:08.776902 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8.9@.?.#.d..e...^...$..<28>1 2025-09-18T21:06:08+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-2: external key update complete 21:06:09.676732 IP 10.100.2.7.46174 > syslog.syslog: SYSLOG daemon.warning, length: 284 E..8..@.?.#.d..e...^...$..<28>1 2025-09-18T21:06:09+00:00 10.100.2.7 Ciena-Waveserver-5-R2.4.52 8986 ModemExternalKeyUpdateComplete [CienaWOS@1271.3 TIME-FORMAT="UTC" EVENT-ID="75-043" EVENT-NAME="ModemExternalKeyUpdateComplete" EVENT-ORIGIN="dpe" TARGET-DS="running"] Modem 1-1: external key update complete

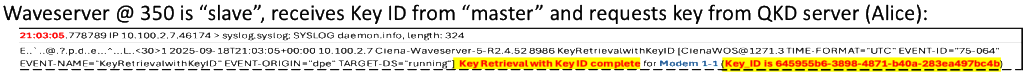
Figure 15 - External Key Interface Logs on Alice's Waveserver

QKD Key Synchronization between Waveserver Encryptors

From previous two charts, let's analyze in more details the key retrieval and updating sequence for 1 encryptor (modem):

Waveserver @ DX is "master", requests key from QKD server (Bob) and transmits Key ID to Waveserver @ 350:

Waveserver @ 350 is "slave", receives Key ID from "master" and requests key from QKD server (Alice):



Both Waveservers update their external key:

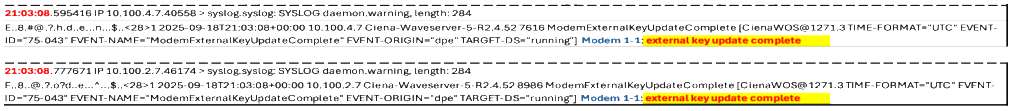


Figure 16 - QKD Key Synchronization Logs between Waveserver Encryptors

Similarly, Figure 17 shows the logs from the Toshiba Control Servers indicating they were providing two keys (one for each encryptor) at the same interval:

Key Exchange Logs from Toshiba QKD Servers

Bob is connected to "master" Waveserver encryptor, thus receiving initial key request.

Bob provides two keys (one for each modem) every minute:

```
Sep 19 15:12:49 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
Sep 19 15:12:49 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
Sep 19 15:14:19 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
Sep 19 15:14:19 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
Sep 19 15:15:49 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
Sep 19 15:15:49 localhost.localdomain qkd-kms[2248]: INFO:    enc_keys: 1 key(s), each with 256 bits, from bobsae to alicesae
```

Alice provides two keys (one for each modem) every minute:

```
Sep 19 15:12:56 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
Sep 19 15:12:56 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
Sep 19 15:14:26 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
Sep 19 15:14:26 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
Sep 19 15:15:56 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
Sep 19 15:15:56 alice qkd-kms[2271]: INFO:    dec_keys: 1 key(s) from bobsae to alicesae
```

Note: The 5 seconds difference between the Bob and Alice is explained by the fact the older software version running on the Toshiba devices did not allow for synchronization to an NTP server.

Figure 17 - Toshiba QKD Control Server Logs

5.3. QKD Channel Status

The next validation activity was to verify the suitability of the secure key rate and the reported Quantum Bit Error Rate (QBER). The Toshiba MU QKD System documentation outlined a baseline 300 kbps for a 10 dB link. Since the link used in the PoC had a measured loss of 7.6 dB, a higher secure key rate was expected. In fact, secure key rates averaging 1,675kbps and a QBER averaging 3.54% over a 24-hour period were observed. Figure 18 on the right provides a sample of the data provided by the Toshiba QKD servers.

Sample output from Toshiba QKD server log showing measured values for the Secure Key generation rate and the Quantum bit-error rate (QBER)

Time	QBER	Secure Key Rate (kbps)
2025-09-22T12:02:57	0.0399	1,649
2025-09-22T12:03:13	0.032	1,705
2025-09-22T12:03:28	0.0323	1,878
2025-09-22T12:03:44	0.0321	1,734
2025-09-22T12:03:59	0.035	1,760
2025-09-22T12:04:14	0.0306	1,868
2025-09-22T12:04:30	0.0347	1,625
2025-09-22T12:04:45	0.0329	1,817
2025-09-22T12:05:02	0.0325	1,570
2025-09-22T12:05:17	0.0339	1,791
2025-09-22T12:05:32	0.0314	1,838
2025-09-22T12:05:48	0.0322	1,684
2025-09-22T12:06:03	0.0336	1,653
2025-09-22T12:06:19	0.0332	1,770
2025-09-22T12:06:36	0.0356	1,500
2025-09-22T12:06:51	0.0327	1,783
2025-09-22T12:07:06	0.0327	1,829
2025-09-22T12:07:22	0.0345	1,647
2025-09-22T12:07:37	0.032	1,802

Figure 18 - Sample Logs from Toshiba Servers

5.4. Network Throughput and Latency Measurements

The PoC activity also included performing a 48-hour Enhanced RFC 2544 test using the Viavi 100GbE network test set to validate 100% line-rate throughput and monitor for any frame or packet loss (see Figure 19).

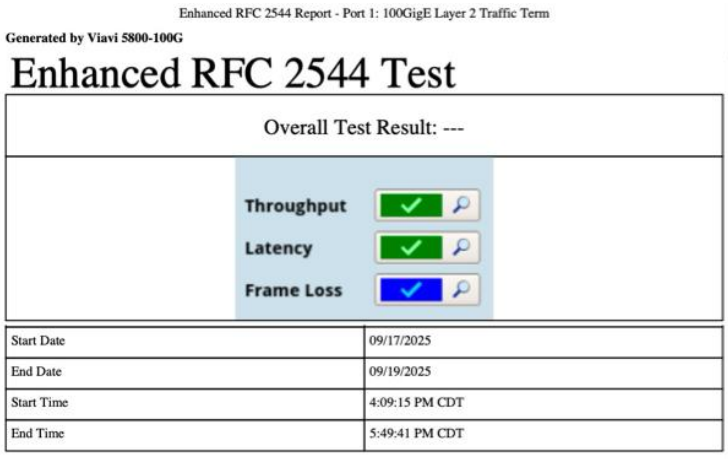


Figure 19 - Viavi Network Tester Enhanced RFC 2544 Report Summary

Overall, the throughput and transparency of the system was confirmed, with 100% throughput and no dropped frames or packets. This test also confirms that the Ciena Wavelogic 5e Encryption Modules maintained this performance while updating its AES-256-GCM encryption key with the key obtained from the Toshiba QKD devices every ~90 seconds.

The overall round-trip latency of the link, including the 800Gbps coherent OTNsec encryptors, was measured at a constant 274.22μs

The detailed measurements are captured in Figure 20.

Enhanced RFC 2544: Throughput Test Results								
Pass/Fail	*Frame Length (Bytes)*	*Measured L1 Rate (Mbps)*	*Measured L2 Rate (Mbps)*	*Measured L3 Rate (Mbps)*	*Measured L4 Rate (Mbps)*	*Measured Rate (frms/sec)*	*Pause Detect*	*Cfg Rate (L1 Mbps)*
Pass	256	99996.0	92749.9	86228.4	78982.3	45,288,042	No	99,996
Pass	1024	99996.0	98080.4	96356.3	94440.7	11,972,701	No	99,996
Pass	9600	99996.0	99788.1	99601.0	99393.1	1,299,325	No	99,996

Enhanced RFC 2544: Latency Test Results						
Pass/Fail	*Frame Length (Bytes)*	*Latency RTD (us)*	*Measured L1 Rate (Mbps)*	*Measured L1 (% Line Rate)*	*Measured Rate (frms/sec)*	*Pause Detect*
Pass	256	274.22	99996.0	99.996	45,288,042	No
Pass	1024	274.22	99996.0	99.996	11,972,701	No
Pass	9600	274.22	99996.0	99.996	1,299,325	No

Enhanced RFC 2544: 9600 Byte Frame Loss Test Results				
Throughput Rate (L1 Mbps)	*Frame Loss Rate (%)*	*Frames Lost*	*Pause Detect*	*Cfg Rate (L1 Mbps)*
99996.1	0.00	0	No	99,996
89996.0	0.00	0	No	89,996

Figure 20 - Viavi Network Tester Enhanced RFC 2544 Detailed Report

6. Outcome & Observations

The PoC activity successfully demonstrated the following:

- Establishing a stable QKD link using the BB84 protocol between two Chicago-area Tier III data centers over a multi-state commercial network. The quantum link over the 13.55-mile fiber connection between the ORD10 and Digital Crossroad remained active and fully operational for over a week. Data collected showed that despite some minor perturbances, the QKD link continuously delivered a steady stream of secure keys well over 1,500 kbps, which is sufficient to power many functions requiring secure keys and/or random numbers.
- Integration of the ETSI QKD 014 standard interface between commercial Generally Available (GA) platforms. While some previous industry tests leveraged commercial QKD and/or encryption devices, many relied on test functions, engineering software and scripts to achieve a successful integration. The activities described herein were conducted using GA versions of hardware and software, and they leveraged only customer-facing interfaces, no

design or backdoor access. Furthermore, the authentication certificates were generated using Quantum Corridor's enterprise CA infrastructure, demonstrating complete integration into a commercial enterprise environment.

Together, these technical demonstrations allowed us to validate the successful implementation of quantum-safe communication links over a metropolitan commercial network. The two 800Gbps encrypted channels were secured using fresh QKD-generated AES key every 90 seconds, showcasing robust and quantum-safe connectivity between two major Midwest data centers across state lines.

This successful demonstration further confirms the commercial readiness of the technologies delivering quantum secure communications over Quantum Corridor's network infrastructure.

6.1. Observations

Since the activity was conducted over a commercial environment with fiber connections going through patch panels in the data centers and through a variety of access points across the metropolitan area, Quantum Corridor reviewed the reported quantum channel performance information provided by the Toshiba QKD system. This led to an initial observation that there appeared to be a somewhat regular perturbation to the fiber connection between the QKD devices taking place over an initial 24-hour monitoring period as illustrated in Figure 21.

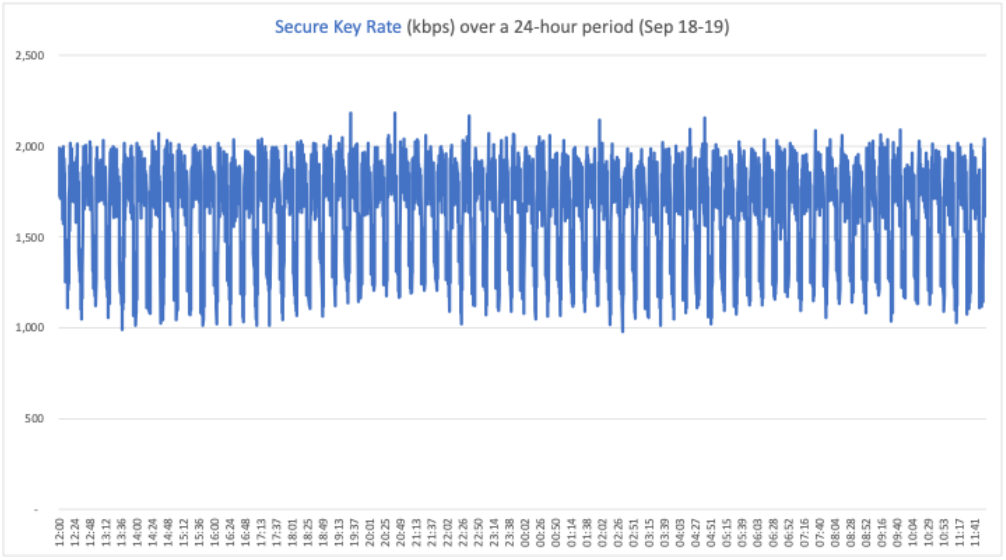


Figure 21 - Secure Key Rate Data over a 24-hour Period

However, despite the perturbations experienced initially on the link, it is worth noting that the Secure Key Rate essentially remained over 1,000kbps and the link remained fully operational.

Data collected over two separate 24-hour periods in the following days pointed to the source of the original perturbation being no longer present as illustrated by Figures 22 and 23, but that punctual disturbances are noted from time to time as shown in Figure 22.

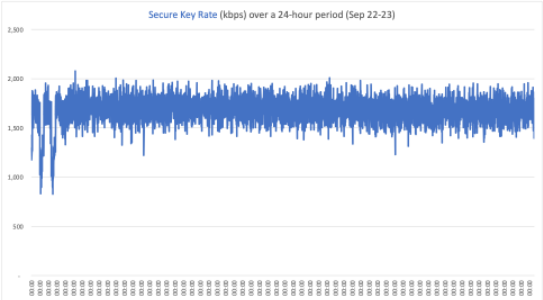


Figure 22 - Sep 22-23 Data

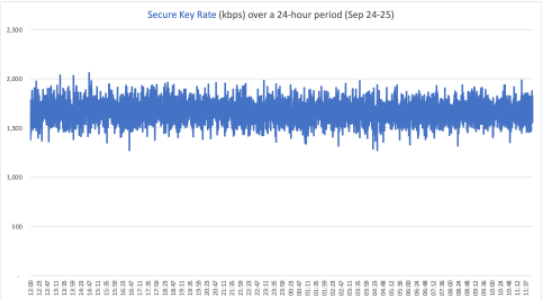
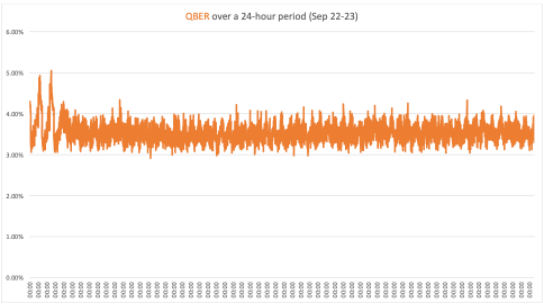
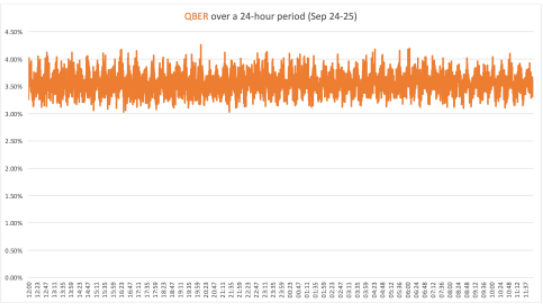


Figure 23 - Sep 24-25 Data





In summary, the data collected over the week-long activity confirms that although one can expect to experience external disturbances across a commercial metropolitan network, the overall stability of the system was never in jeopardy as the quantum channel remained up at all times and maintained a high Secure Key Rate – over 1,500 kbps most of the time – to secure the encrypted traffic between the two end points.

7. Summary, Conclusion and Future Work

The successful implementation of quantum-secure communication over Quantum Corridor's live, commercial metropolitan network through the integration of Toshiba's QKD system with Ciena's high-speed encryption equipment demonstrated consistent, high-rate key generation and stable, 800 Gbps encrypted data transfer between two interstate Tier III data centers.

This proof-of-concept marks a key milestone toward operational quantum-safe communication infrastructure over Quantum Corridor's commercial network. The results demonstrate that QKD can be deployed over commercial fiber with production-grade encryption systems, paving the way for future quantum-resilient critical infrastructure and enterprise services.

These results make way for the network to move forward with testing additional building blocks for quantum communication, including but not limited to quantum memories, timing distribution and quantum repeaters.

8. Acknowledgements

Quantum Corridor would like to thank the following key partners for their collaboration and support of this successful PoC demonstration: the QKD servers were graciously loaned to Quantum Corridor by the ***University of Chicago*** and ***Chicago Quantum Exchange***, extending their existing loan from ***Toshiba***. ***Toshiba*** additionally provided technical support for the configuration, operation and troubleshooting of the QKD servers. Project management, installation and engineering support for the planning and execution of this PoC demonstration were performed through Quantum Corridor's exclusive partnership with ***Quantum Foundry***.