Quantum Key Distribution on Metro Fiber:
QKD-Keyed Optical Encryption Between 350 Cermak and SC26

Quantum Foundry and Internet2. SC26 Network Research Exhibition NRE134. Linked infrastructure request: NRI112.

Abstract

This demonstration runs a Quantum Key Distribution (QKD) link over production metro fiber between the Equinix facility at 350 E Cermak and the SC26 exhibit floor at McCormick Place, and uses the keys it produces to encrypt an optical wave on Internet2 transport equipment. A pair of ID Quantique Clavis XG systems exchanges keys over a dedicated dark-fiber strand. Those keys are delivered through a key management system to Internet2 Waveserver 5 encryption on a wave carried on Internet2 Ciena 6500 gear between 350 Cermak and the SCinet NOC. The chassis at both ends carry production traffic; the demo runs on its own module.

The point of the exercise is the quantum channel itself. QKD does not stop someone from tapping the fiber; it makes the tap visible. An IP-controlled attenuation device on the quantum strand in the SCinet Research Hotel lets us introduce loss on demand and show what the QKD system does when the channel is disturbed: the quantum bit error rate rises, the secure key rate falls, key sessions drop, and the encryptor is left without fresh keys. Visitors watch that happen on a display in the Internet2 booth.

Goals

- Run QKD on real Chicago metro fiber, 350 Cermak to McCormick Place, on strands provisioned through SCinet.
- Feed QKD keys into Waveserver 5 encryption through a single management VLAN carrying KMS, key ID and device management.
- Show tamper detection live: attenuate the quantum strand and observe the QKD system and the encrypted wave respond.
- If a second module frees up, run an unencrypted wave alongside the encrypted one for comparison. This is a stretch goal.

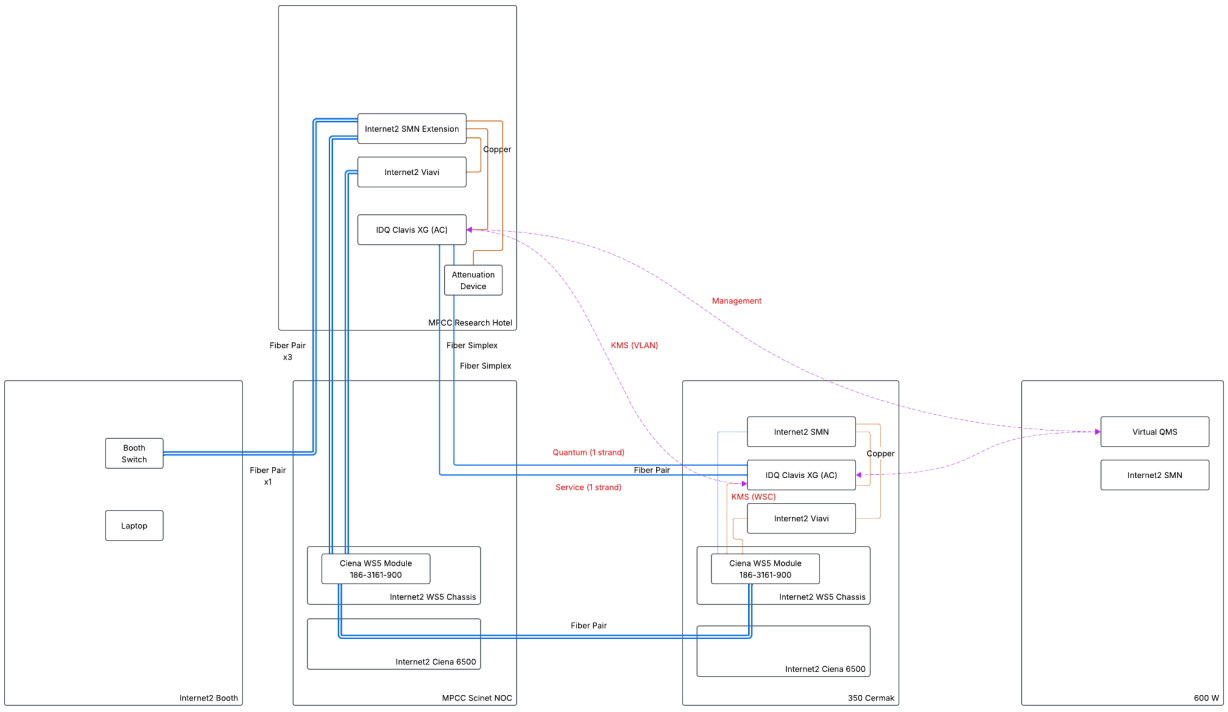
Demonstration design

Equipment is split across four locations. 350 Cermak holds an Internet2 Ciena 6500, a Waveserver 5 chassis with the demo module, one Clavis XG and a VIAVI test set, all reachable over the Internet2 Secure Management Network (SMN). The SCinet NOC holds the matching Ciena 6500 and Waveserver 5 chassis. The SCinet Research Hotel holds the

second Clavis XG, the attenuation device, an SMN extension and, if needed, a second VIAVI. The Internet2 booth holds a small switch, the demo laptop and a display. A single VLAN carries KMS, key ID and Clavis management end to end over the SMN, so nothing has to be routed through SCinet's own infrastructure. The QMS runs either on the Internet2 virtualization cluster or on a laptop in the Research Hotel.

Fiber between sites: one pair for the 6500 line side between 350 Cermak and the NOC; two simplex strands (quantum and service) between the Clavis units at 350 Cermak and the Research Hotel; three pairs between the NOC and the Research Hotel; one pair from the Research Hotel to the booth. Most of the build can be staged at 350 Cermak starting 21 October, with the Waveserver 5 and 6500 chassis configured and upgraded in the Internet2 lab before shipping to McCormick Place. The Research Hotel equipment goes in during setup week.

At the booth, the walkthrough is short. A VIAVI in loopback keeps test traffic running over the encrypted wave, which also keeps key consumption high enough that a disturbance shows quickly. We add loss to the quantum strand from the laptop and watch the QKD dashboards: QBER climbs, secure key rate drops, key sessions fall over, and the encryptor's key supply stalls. Remove the loss and the link recovers. Encryption on a Waveserver is always on and invisible from the line side, so the story is the quantum channel rather than a before-and-after of the encryptor. Scheduled sessions in the Research Hotel are available as well.



Impacts

Importance to the participating institutions and the R&E community. Internet2 has been working through what Post-Quantum Cryptography (PQC) and MACsec mean for the network it operates for the research and education (R&E) community. QKD is the other half of that question, and there is very little operational experience with it on North American R&E fiber. This is a chance to get some, on real metro spans with real transport gear, in front of the operators who would have to run it. For Quantum Foundry it is a test of whether commercial QKD can be integrated into an existing carrier-class optical platform without a purpose-built network around it.

What SCinet makes possible. The quantum channel needs a dedicated, unamplified strand between two sites several kilometers apart. SCinet's dark fiber between 350 Cermak and the convention center gives us that, and the Research Hotel gives us a secured place to put the far-end QKD device where it can be reached from the booth. Neither is something we could improvise on the exhibit floor.

Next steps. The immediate follow-on is a technical write-up of what the QKD link did on this span: key rates over the week, how the system responded to the induced loss, and what the key-management plumbing looked like in practice. That record is what Internet2 and Quantum Foundry need to judge whether QKD-keyed transport is worth carrying further on R&E fiber, and what encryptor and key-delivery interfaces (ETSI GS QKD 014 among them) would have to be supported to do it.

Resources requested from SCinet (see NRI112)

- Two simplex dark-fiber strands, 350 Cermak to the SCinet Research Hotel, one each for the quantum and service channels.
- One fiber pair, 350 Cermak to the SCinet NOC, for the Ciena 6500 line side, if not already in place on the Internet2 side. (already accounted for)
- One wave on the Internet2 Waveserver 5 between 350 Cermak and the SCinet NOC; a second unencrypted wave if a module becomes available. (I2 will supply)
- Three fiber pairs NOC to Research Hotel; one fiber pair Research Hotel to the Internet2 booth.
- Rack space and power in the Research Hotel (Clavis XG, attenuation device, SMN extension, possibly a VIAVI) and in the NOC (Ciena 6500, Waveserver 5 chassis). One AC circuit in the Research Hotel; DC preferred at 350 Cermak if IDQ confirms the Clavis supports it.
- One VLAN for KMS, key ID and management between the Research Hotel and 350 Cermak, carried over the Internet2 SMN extension.

- Secured rack access in the Research Hotel.

Involved parties

- Vincent Celindro, Quantum Foundry, vince@quantumfoundry.ai (primary contact); Bob Reinert, Quantum Foundry
- Chris Wilkinson, Internet2, cwilkinson@internet2.edu; Robert Sears, Brenna Meade, JoAnne Bender, Matt Hoffman, Jim Lookabaugh and Christian Todorov, Internet2
- ID Quantique: Clavis XG QKD systems
- Ciena: Waveserver 5 and 6500 platforms
- IonQ: Clavis