Defense-in-Depth a kvantumtörés-álló kommunikációban: *A poszt-kvantum kritptográfia és kvantum alapú kulcselosztás gyakorlati alkalmazása*

Poór Gergely RelNet Technológia Kft · Infrastruktúra rendszermérnök

Poór Gergely (28)

MTCRE, JNCIS-SP, JNCIS-ENT, HEQA & SSH Certified
Szakterület: Linux/BSD, PQC/QKD, gyenge-és erősáramú szerelés
Üzemeltetési tapasztalat: Parkolási és útdíj rendszerek (EU/USA/Ázsia), Gyógyszeripar, Kritikus és Állami infrastruktúra, Logisztika



Kvantumszámítógépek

01 **Kvantum-algoritmusok**

Kulcscsere és titkosítás feltörése

02 **HNDL-jelenség**

Az törés nem azonnal történik

03 **Létező védelmi módok**

PQC, QKD, AES256/SHA512

A kihívások

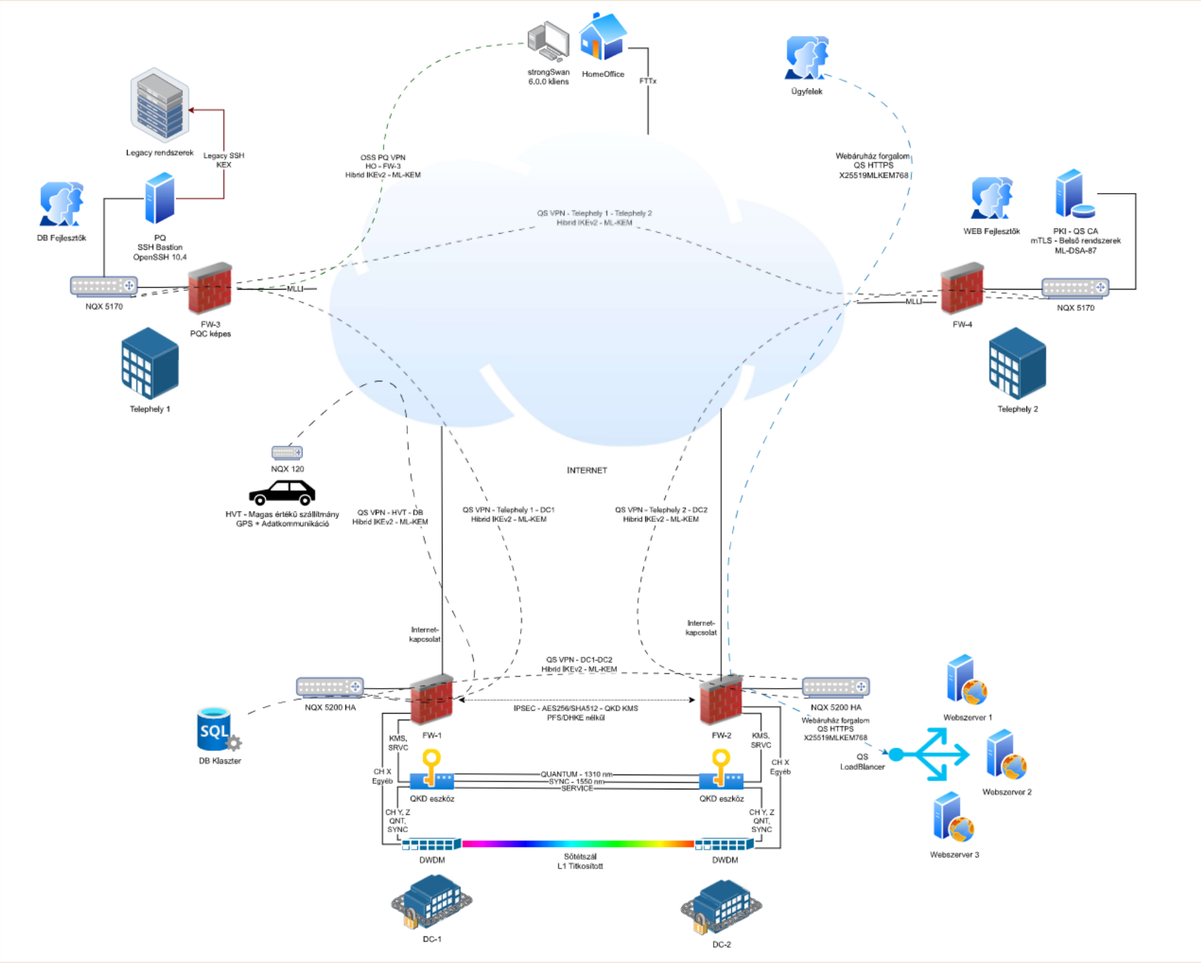
- Tervezés során többrétegű védelem (Defense-in-Depth)
  - Core: QKD
    - Fotonokból kulcsok, **fizikai törvények adta biztonság**, xWDM
  - Edge: PQC
    - Átviteli közegtől független, **matematikai biztonság**, hardveres vagy szoftveres, Layer 3/Layer 7
- Reziliencia, jövőállóság
- Üzemeltethetőség

Minta *hálózat*

Fiktív webáruház, **többszintű védelemmel** ellátva:

HW PQC, SW PQC, QKD, DWDM titkosítás

Több adatközpont, több telephely, távmunka, kiszállítás



Poszt-Kvantum Kriptográfia

- Szoftveres vagy dedikált hardveres megoldás, új algoritmusok
- Layer3-Layer7
- **FIPS-203**, **FIPS-204**, **FIPS-205** szabványok
  - 203: ML-KEM
    - Kulcscsere
  - 204-205: ML-DSA és SLH-DSA
    - Digitális aláírás
- **Hibrid-PQC** – gyors adaptáció, hagyományos és PQ algoritmusok

SSH NQX

01 **Webes felület**

Verziókezelt házirendekkel

02 **L2-L3 IPSec VPN**

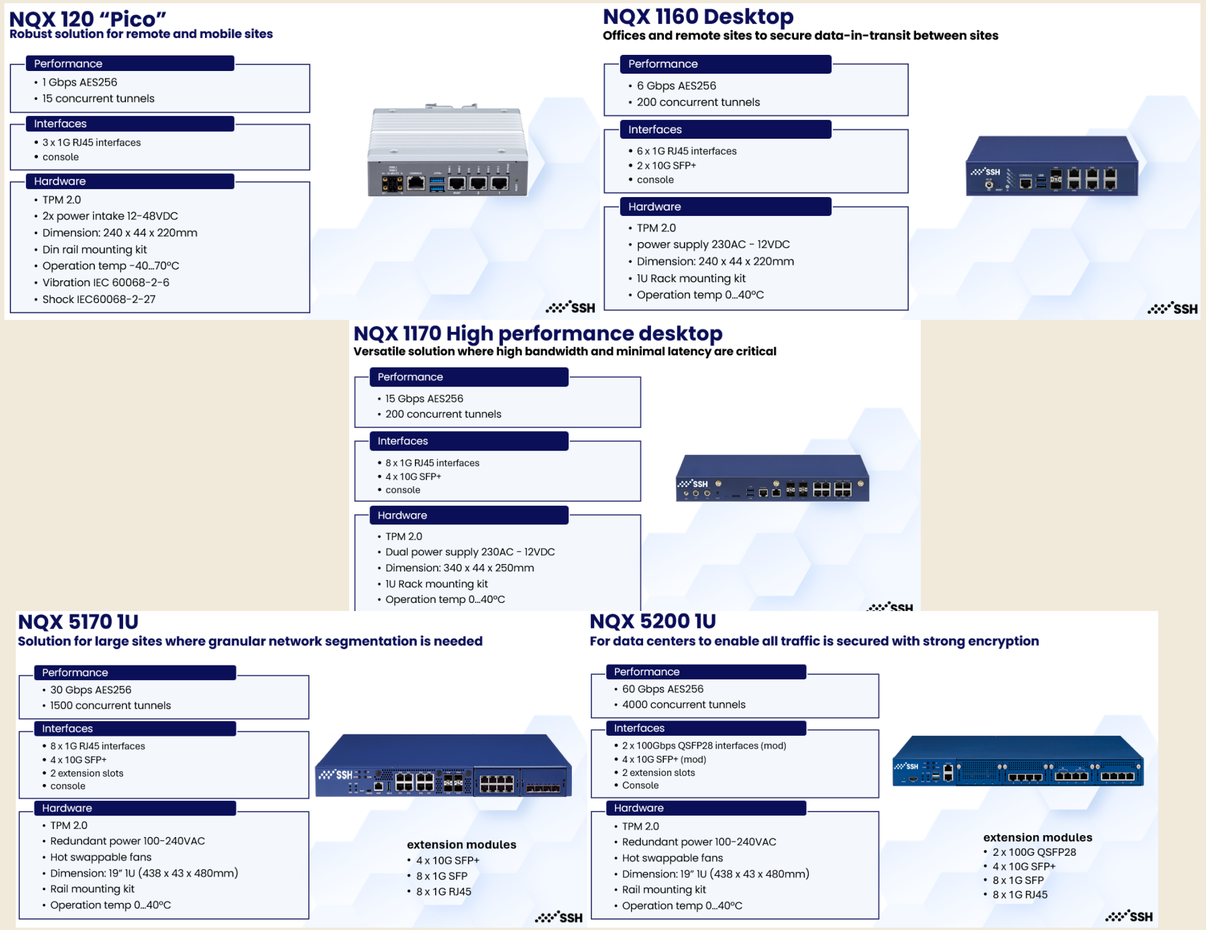
ML-KEM és RFC8784 PPK

03 **Központi vezérlő egység**

Teljes HW életciklus-követés

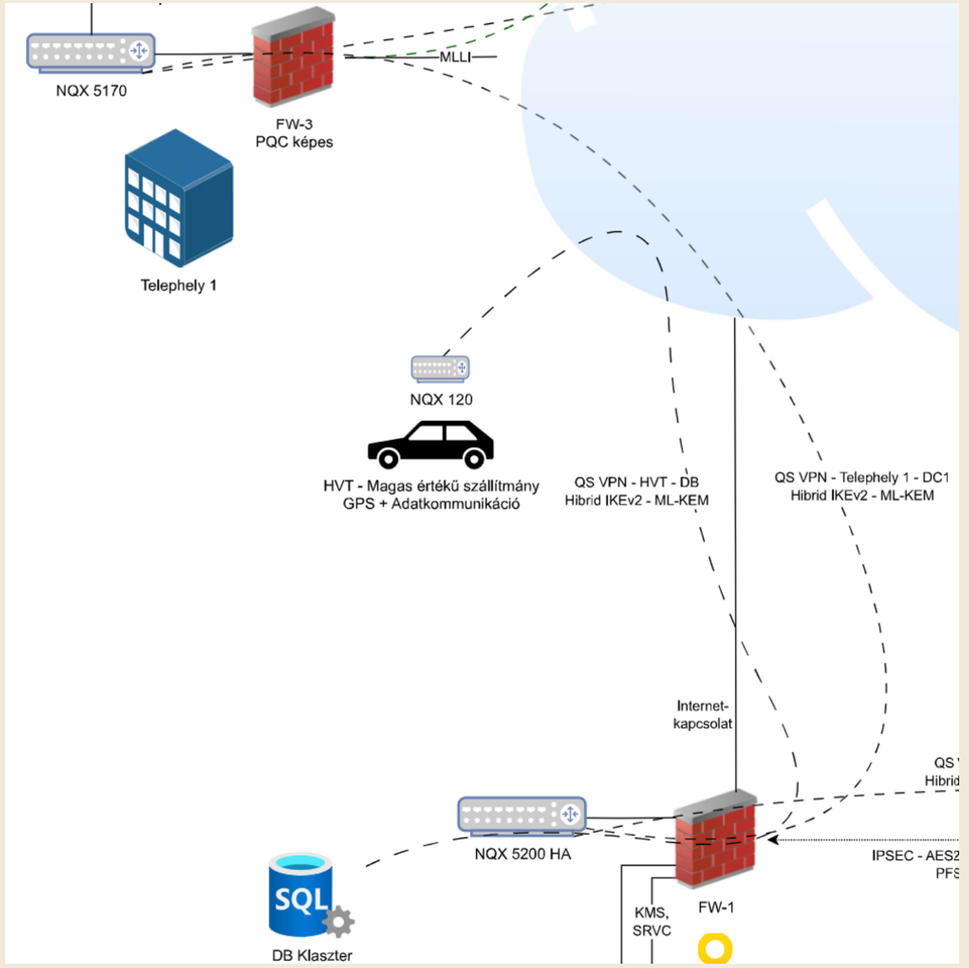
Modellek

IoT-tól a telephelyeken át az adatközpontig



Minta *hálózat*

- NQX 120 – járművek
- NQX 5170 – telephelyek
- NQX 5200 – adatközpontok



PQC Szabad szoftverekkel

- OpenSSL 3.5
  - TLS, PKI
- OpenSSH 9.0
  - Távoli elérés + IP forgalom titkosítása
- strongSwan 6.0.0
  - IPSec

Minta *hálózat*

- Reverse-Proxy és PKI
- PQ SSH Bastion legacy rendszerek elé
- IPSec a távmunkához

```
[root@rhel-wsl ~]# curl https://pq.techsuppoort.com
Your IP is: [redacted]
Your User-Agent is: curl/8.12.1
Your TLS version is: TLSv1.3
You have negotiated this KeyExchange: X25519MLKEM768

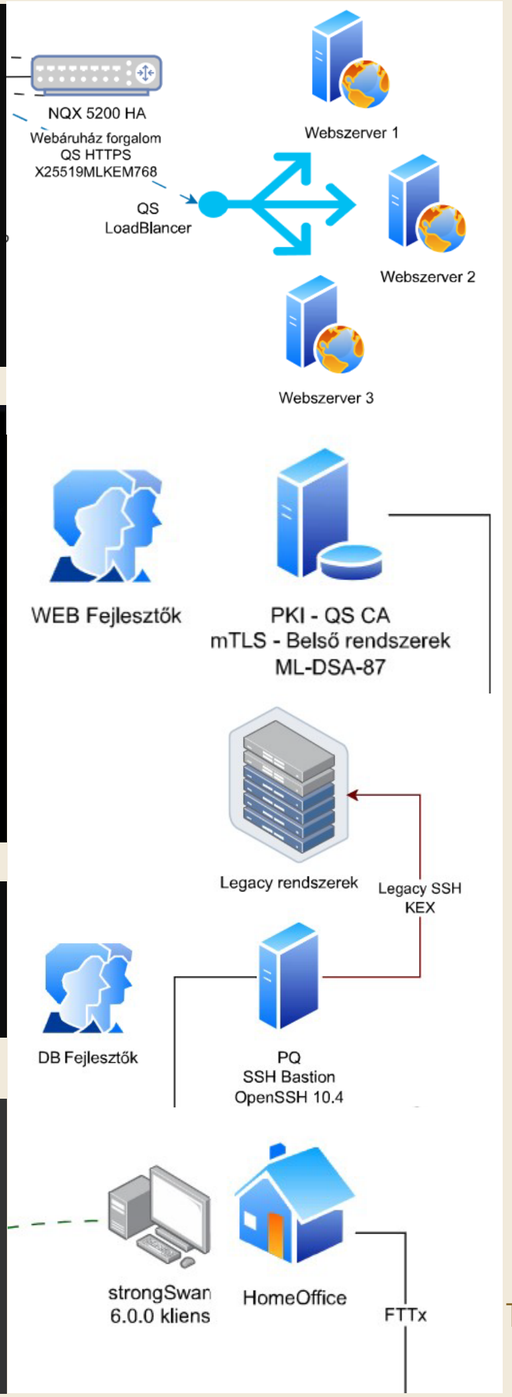
This connection is considered quantum-safe.

Powered by techsuppoort>_
Proudly served on FreeBSD
[root@rhel-wsl ~]#
```

```
Data:
    Version: 3 (0x2)
    Serial Number: 4098 (0x1002)
    Signature Algorithm: ML-DSA-87
    Issuer: O=techsuppoort>_, CN=techsuppoort>_ QUANTUM-SAFE LOCAL mTLS CA
    Validity
        Not Before: Jun  5 12:22:41 2026 GMT
        Not After : Jun  2 12:22:41 2036 GMT
    Subject: CN=                , O=techsuppoort>_
    Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:a8:70:19:17:e1:ea:f6:c5:37:63:0f:c9:b1:4a:
                6a:64:db:ba:3c:aa:6c:b7:f5:f9:3e:60:eb:8a:50:
                0c:78:68:d9:d5:10:89:04:6b:fd:70:f4:28:9a:b2:
                27:f0:d7:79:c7:56:a8:7b:45:48:9b:da:18:73:7c:
                bd:5a:de:0d:3f
            ASN1 OID: prime256v1
            NIST CURVE: P-256
```

```
openbsd# ssh admin@192.168.56.254
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
admin@192.168.56.254's password:
```

```
root@site1-bsd:~ # swanctl --list-sas
site2site: #1, ESTABLISHED, IKEv2, 928e1b816c566952_i* 16b7820121e44798_r
  local  '10.0.0.2' @ 10.0.0.2[4500]
  remote '10.0.0.3' @ 10.0.0.3[4500]
  AES_CBC-256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/ECP_384/KE1_ML_KEM_768
  established 257s ago, rekeying in 12760s
  net-net: #2, reqid 1, INSTALLED, TUNNEL, ESP:AES_GCM_16-256
    installed 257s ago, rekeying in 3056s, expires in 3703s
    in  c692e079,    816 bytes,    10 packets,    10s ago
    out cc15e722,   1356 bytes,    10 packets,    10s ago
    local  192.168.1.0/24
    remote 192.168.2.0/24
root@site1-bsd:~ #
```



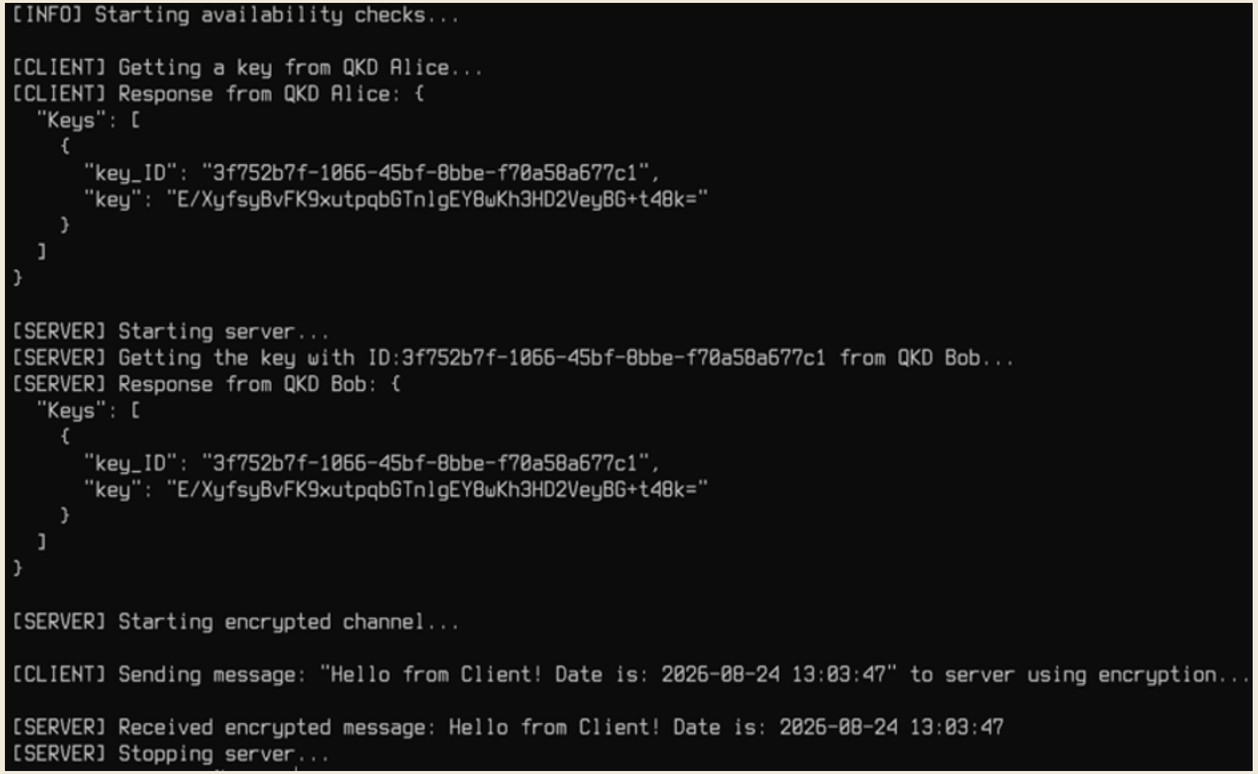
Kvantum-Kulcselosztás

- Fotonok manipulációja optikai linkeken
- Szimmetrikus kulcsok, **PFS/DHKE kiváltása**
- Nem csak hálózati eszközök számára hasznos
  - ETSI GS QKD API
- ~ 100km két eszköz között
- BB84/E91 protokoll
- xWDM – akár L1 titkosítással

API

A QKD eszközök bármivel integrálhatóak, amennyiben a kliens képes az alábbiakra:

- HTTPS
- TLSv1.3
- mTLS



HEQA Sceptre termékcsalád

01 **Több modell**

Link, Hub&Spoke, DUO, Moduláris

02 **Fókuszban az üzemeltető**

API, SNMP, LED-ek, Web UI, KMS

03 **exeQtive**

Központi felügyeleti rendszer

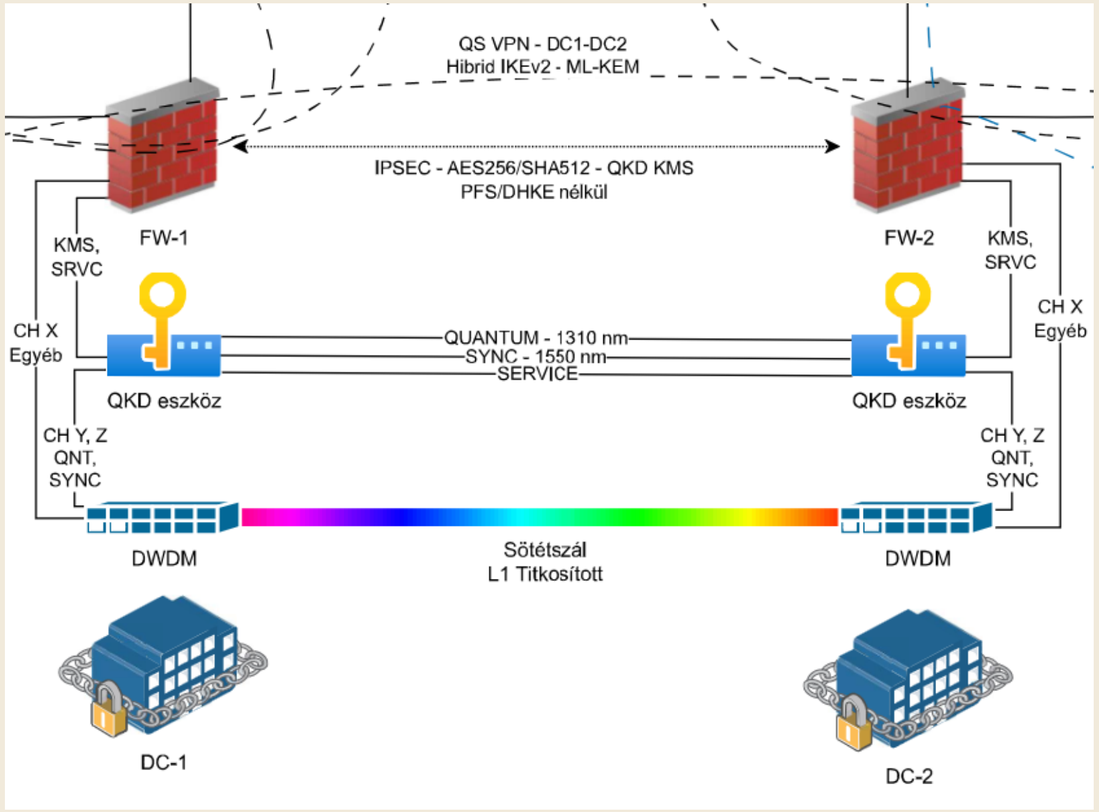
Modellek

- **Link**: Klasszikus Alice-Bob
- **DUO**: Alice és Bob 1U-ban
- **HUB/Spoke**: 1 Bob – 4 Alice
- **MODULAR**: sokoldalú és csak 2U



Minta *hálózat*

- 4 csatorna:
  - DWDM-en keresztül
    - Kvantum – 1310 nm – fotonok
    - Szinkron – 1550 nm – órajel
  - Ethernet-en keresztül
    - Service – DS BB84 – publikus mérések
    - KMS – kulcsok a titkosító eszközöknek



Összefoglaló

01 **Ez nem a jövő!**

A kvantumtechnológia és a védelmi megoldások már itt vannak.

02 **Többrétegű védelem**

QKD – Core, PQC – Edge+App szinten

03 **Te már felkészültél?**

https://pq.relnet.hu

Köszönöm a figyelmet!

Poór Gergely
gpoor@relnet.hu