1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
info@relnet.hu

A RelNet átfogó poszt-kvantumtitkosítási megoldásai

Törvényi háttér – Kötelező a PQC!

2024-ben a Parlament elfogadta a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényt, amely 2025. január 1-jén lépett hatályba és a NIS2 irányelv hazai implementációjáról rendelkezik. A törvény egyebek mellett kötelezővé teszi a poszt-kvantumtitkosítás (PQC) alkalmazását bizonyos létfontosságú szervezetek számára. Ide tartoznak többek között a kormányzati célú hálózatot használó intézmények és számos kritikus közműszolgáltató is. A törvény elvárja, hogy az érintett szervezetek IT-hálózati kommunikációjukat olyan poszt-kvantumtitkosítási alkalmazással védjék, amely a hagyományos kriptográfián felül biztosítja egy kvantumszámítógép általi támadások elleni védelmet. A jogszabály további feltételeket határoz meg a poszt-kvantumtitkosítási megoldások szolgáltatóira és azok tanúsítására is.

Ez a törvényi előírás egyértelmű üzenetet közvetít: a kvantumszámítógépek jelentette új fenyegetésre időben fel kell készülni, méghozzá szabályozott keretek között. A jogalkotó ösztönzi a magyarországi szervezeteket, hogy mihamarabb kezdjék meg a kvantumbiztos titkosításra való átállást, és ne várják meg, míg a kvantumtechnológia gyakorlati támadóereje utoléri őket. Aki nem lép időben, az nemcsak támadási kockázatnak teszi ki magát, hanem szabályozói szankciókra is számíthat. A törvény betartását hazánkban a Szabályozott Tevékenységek Felügyeleti Hatóságának (SZTFH) kiberbiztonsági osztálya felügyeli. A hatóság ellenőrizheti, alkalmaz-e az adott szervezet kvantumbiztos titkosítást, és ha nem, súlyos bírságokat helyez kilátásba az előírásokat elmulasztó szereplők számára. Ráadásul a PQC hiánya jövőbeni auditoknál a megfelelőség hiányaként jelenhet meg (akár GDPR vagy ISO 27001 kontextusban is).

Összhangban az Európai Unió cselekvési ütemtervével, 2030 végéig a magas kockázatú területeken (pl. kritikus infrastruktúrák) a poszt-kvantumtitkosítást (PQC) teljessé kell tenni. A hazai szervezetek számára tehát már most valós követelmény a kvantumbiztos átállás.

A kvantumfenyegetés és a „Harvest Now, Decrypt Later” probléma

A kvantumszámítógépek rohamos fejlődése alapjaiban fenyegeti a ma használatos nyilvános kulcsú titkosítási algoritmusokat. Az aszimmetrikus titkosítás – mint az RSA, ECC stb. – biztonságát olyan matematikai problémák adják (pl. faktorizáció), amelyeket a klasszikus számítógépek gyakorlatilag megoldhatatlannak tartanak. Egy megfelelően erős kvantumszámítógép azonban a Shor-algoritmus révén viszonylag gyorsan feltörheti ezeket a titkosításokat. Mivel a szakértők szerint 5-10 éven belül realitássá válhat egy titkosítások feltörésére képes kvantumszámítógép, már most stratégiai fontosságú felkészülni erre a veszélyre.

1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
info@relnet.hu

Az egyik legaggasztóbb jelenség a szakmában a **„Harvest Now, Decrypt Later" (gyűjtsd be most, fejtsd vissza később)** támadási modell. Ennek lényege, hogy egy támadó már ma begyűjtheti és eltárolhatja a célpont titkosított kommunikációját vagy adatforgalmát, bízva abban, hogy néhány év múlva – a kvantumszámítógépek megjelenésekor – képes lesz visszafejteni azt. Tehát amit ma biztonságosnak gondolunk, holnap feltörhetővé válhat. Az EU szakmai útmutatásai is hangsúlyozzák, hogy ez a fenyegetés az egyik legsürgetőbb ok a poszt-kvantumtitkosítás (PQC) mielőbbi bevezetésére. Különösen azon szervezetek számára kritikus ez, amelyeknél az adatok hosszútávon, 5-10 év múlva is érzékenyek maradnak, például egészségügyi adatok, diplomáciai vagy hírszerzési információk, pénzügyi tranzakciók stb.

Miért sürgős felkészülni a kvantumkorszakra?

Ha a rendszereink csupán a hagyományos titkosítási algoritmusokra (RSA, elliptikus görbék stb.) támaszkodnak, akkor egy most rögzített adathalmaz a jövőben visszafejthetővé válik. Becslések szerint a „Q-nap", amikor a kvantumgépek feltörik a jelenlegi kriptográfiát, 2030 körül következhet be. Tehát ha például 5 évig kell titokban maradnia az adatoknak, akkor ezeket az adatokat legkésőbb 2025-től poszt-kvantumvédelemmel kellene ellátni.

RelNet előadás az EIVOK-56. konferencián - A poszt-kvantum korszak kihívásai

A halogatás súlyos kockázatokat rejt magában. Ez nem olyan probléma, amit akkor kell majd orvosolni, amikor a kvantumszámítógép megérkezik. A fent vázolt törvényi előírások és fenyegetések egyaránt arra mutatnak, hogy a kriptográfiai paradigmaváltás azonnali cselekvést követel.

A USA Nemzeti Szabványügyi és Technológiai Intézete (NIST) 2022-ben kiválasztotta az első négy poszt-kvantumalgoritmus standardját – ilyen például a CRYSTALS-Kyber és a CRYSTALS-Dilithium –, 2024-ben pedig további digitális algoritmusokat véglegesített a hagyományos kriptográfia leváltására. Az átállás azonban nem megy egyik napról a másikra: nyilvántartásba kell venni a szervezeteknél használt összes protokollt, eszközt, titkosítási modult, és felmérni, melyik kvantumérzékeny közülük. Szükség lehet szoftverfrissítésekre, akár hardvercserére (pl. régi IoT eszközök esetén) is az új algoritmusok támogatása érdekében. Emellett a **kriptoagilitás** elve is kulcsfontosságú: olyan rendszerekre van szükség, amelyek rugalmasan cserélhető algoritmusokkal működnek, és hibrid módon képesek klasszikus és PQC algoritmusokat is futtatni a kompatibilitás érdekében.

Mindezek fényében a szervezeteknek haladéktalanul stratégiai tervet kell készíteniük a posztkvantum átállásra. A kvantumszámítógépek gyors fejlődése miatt elengedhetetlen, hogy már most felkészüljünk a klasszikus titkosítási rendszerek leváltására. Ez nem pusztán technikai feladat, hanem üzletfolytonossági és kockázatkezelési kérdés is. A jó hír, hogy már rendelkezésre állnak azok a megoldások, amelyekkel felvértezhetjük rendszereinket a kvantumkorszak kihívásaival szemben. A RelNet ezek közül kínál teljes körű portfóliót partnerei számára.

Kvantum alapú kulcselosztás (QKD)

A Quantum Key Distribution (QKD) olyan technológia, amely a kvantumfizika törvényeit használja fel titkosítási kulcsok biztonságos megosztására. A QKD lényege, hogy két fél egy kvantumcsatornán – tipikusan optikai szálon, egyesével küldött fotonok segítségével – állít elő és oszt meg egy véletlenszerű titkos kulcsot. A kvantummechanika alapelvei miatt a kommunikáló felek képesek észlelni, ha egy harmadik fél megpróbál belehallgatni a kulcscserébe. Ha valaki megpróbálja elfogni vagy lemásolni a fotonokat, az kimutatható hibát és zajt okoz a monitorozás során. Ilyenkor a kulcsot érvénytelenítik és a kommunikációt biztonsági okból megszakítják. A QKD különlegessége abban rejlik, hogy előre garantálja a kulcs bizalmasságát, szemben a hagyományos algoritmusokkal, ahol csak feltételezzük a nehéz visszafejthetőséget.

A **QKD legfőbb előnye**, hogy nincs olyan számítási kapacitás vagy algoritmus (még kvantumszámítógép sem), amely a kvantumfizika törvényeinek megkerülése nélkül megfejthetné a létrejött kulcsot. További előny, hogy a meglévő optikai hálózatokon is használható. Amennyiben rendelkezésre áll sötét szál vagy megfelelő hullámhosszosztásos (WDM) technika, a QKD eszközök integrálhatók az aktuális infrastruktúrába. Ez fontos gyakorlati szempont például telekommunikációs szolgáltatóknál vagy adatközpontok összeköttetésénél.

A QKD **hátrányai közé tartozik** azonban, hogy jelenleg igen költséges. Ráadásul nagy hálózat esetén sok eszközt igényel (lézer, detektorok, optikai stabilizáció stb.). Emellett a QKD-nak

fizikai korlátai is vannak: az optikai csatorna távolságával exponenciálisan csökken a kulcselosztás sebessége, ezért ismétlők beiktatására lehet szükség.

Összességében a QKD jelenleg elsősorban ott indokolt, ahol kritikus adatokat kell mozgatni két pont között, elfogadható a magas költség, és nem elégszünk meg a poszt-kvantumalgoritmusok „feltételezett" biztonságával, hanem fizikai garanciát akarunk. Ilyenek lehetnek például az állami vagy katonai gerinchálózati összeköttetések, bankok közötti kommunikáció stb.

A RelNet kvantumbiztos megoldásportfóliója

A RelNet Technológia Kft. felismerte a kvantumkorszak kihívásait, és átfogó kínálatot alakított ki a kvantumbiztos hálózatok terén. Mérnökeink vezető gyártók poszt-kvantumtitkosítási termékei tekintetében rendelkeznek mélyreható kompetenciával, így egy kézből tudunk teljes körű védelmet nyújtani partnereinknek. Legyen szó kvantum alapú kulcselosztásról (QKD) vagy poszt-kvantumalgoritmusokra épülő titkosító eszközökről, a RelNet a tervezéstől a megvalósításon át a támogatásig biztosítja a szükséges szakértelmet. Az alábbiakban áttekintjük a portfóliónk megoldásait ezen a téren.

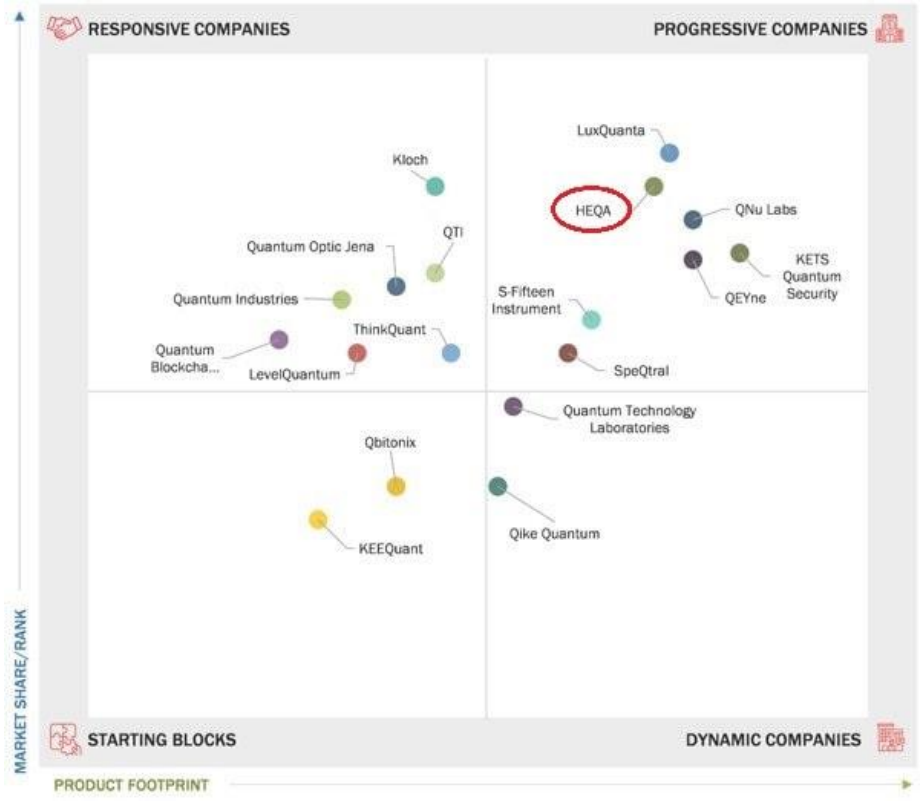
HEQA Security – QKD nagyvállalati hálózatokhoz

A HEQA Security a kvantumbiztos hálózati megoldások úttörője. Termékei a kvantum alapú kulcselosztásra épülnek. A HEQA QKD rendszereit kifejezetten úgy tervezték, hogy nagyvállalatok meglévő optikai infrastruktúráiba és kulcskezelési folyamataiba integrálhatók. Két fő terméke a SceptreDuo és a SceptreLink:

- **SceptreDuo**, az iparág első „all-in-one" QKD megoldása. Adó, vevő és integrált kulcsmenedzsment (KMS) egyetlen 1U méretű hardverben, a költséghatékony telepítés és egyszerűbb üzemeltetés érdekében. A SceptreDuo a meglévő optikai szálakon képes kvantumkulcsokat terjeszteni, akár dedikált sötét szálon, akár a DWDM rendszerbe multiplexálva. A kompakt egyesített kivitel csökkenti a hibalehetőségeket és egyszerűsíti az üzemeltetést. A rendszer „plug-and-play" jelleggel, különleges kvantumfizikai szakértelem nélkül telepíthető.

1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
info@relnet.hu

- **SceptreLink** – egy költséghatékony QKD megoldás, amely szintén a meglévő optikai szálakon működik, de modulárisabb felépítésű, különálló adó és vevő egységgel. Könnyen telepíthető és skálázható, lehetővé téve kvantumkulcsok biztosítását nagyobb távolságú összeköttetések számára is. A SceptreLink ideális választás lehet azoknak, akik lépcsőzetesen vezetnék be a QKD-t: kisebb kezdő beruházással indulva, majd szükség szerint bővítve a hálózat kvantum alapú védelmét.



A MarketsandMarkets a HEQA Securityt a kvantum alapú kulcselosztási (QKD) piac fő szereplői között említi

A HEQA megoldásait világszerte már most alkalmazzák távközlési szolgáltatók, a kormányzati és védelmi szektor, a nagy adatközpontok, bankok és biztosítók, kritikus infrastruktúrák, valamint az egészségügy. Ezen szektorokban a kvantumbiztonság már nem luxus, hanem gyakorlati igény. A HEQA Security jelenleg a leggazdaságosabb és legjobban skálázható nagyvállalati QKD megoldást nyújtja, miközben nem köt kompromisszumot a biztonság terén. A RelNet szakértői csapata rendelkezik a HEQA rendszerek telepítéséhez és integrációjához szükséges know-how-val, így ügyfeleink számára komplett szolgáltatást tudunk biztosítani a tervezéstől az üzemeltetésig.

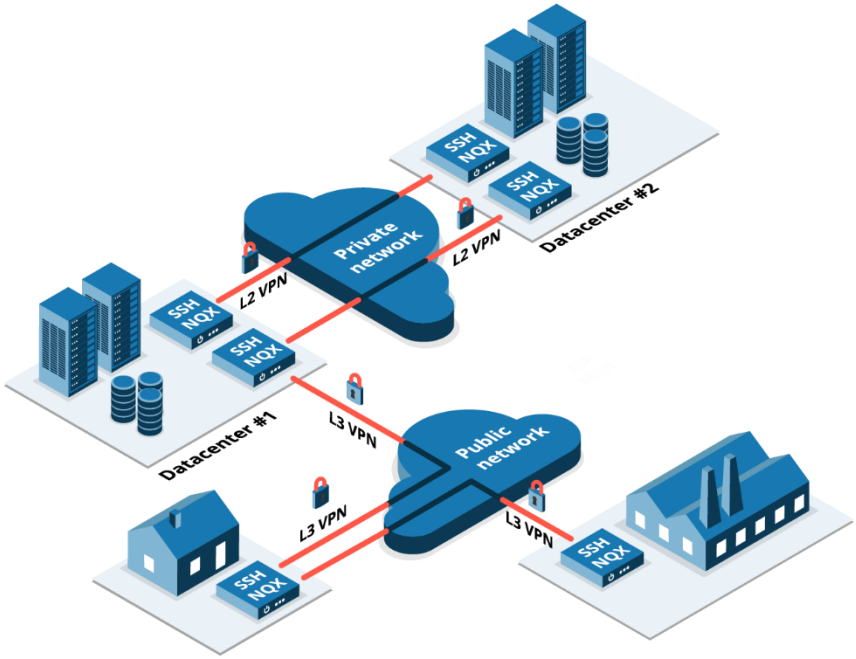
SSH NQX - PQC platform

Az SSH Communications Security mára a kvantumbiztos hálózati titkosítás egyik élharcosa. Legújabb terméke, az NQX titkosító platform, kifejezetten a poszt-kvantumkriptográfiai algoritmusokra (PQC) épül. Az NQX célja, hogy az adatfolyamokat kvantumbiztos módon titkosítsa, legyen szó akár két adatközpont közötti nagy sebességű gerinchálózati linkről,

1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
info@relnet.hu

akár OT és IT környezetek összekapcsolásáról, vagy éppen távoli telephelyek közötti kommunikációról.

Az NQX a legfejlettebb poszt-kvantum algoritmusokat alkalmazza, amelyek ellenállnak a kvantumszámítógéppel végrehajtott támadásoknak. Ráadásul az NQX egy **kriptográfiailag agilis (crypto-agile) platform**, ami azt jelenti, hogy a titkosító szoftver/hardver modulok bármikor frissíthetők az újonnan standardizált algoritmusokra, így mindig naprakész a legújabb PQC szabványokból. Az NQX beépített algoritmuskészlete tartalmazza például azokat a NIST által ajánlott kulcscsere megoldásokat, mint a FrodoKEM vagy a Classic McEliece, melyeket nagy sebességű környezetben is optimalizáltak.

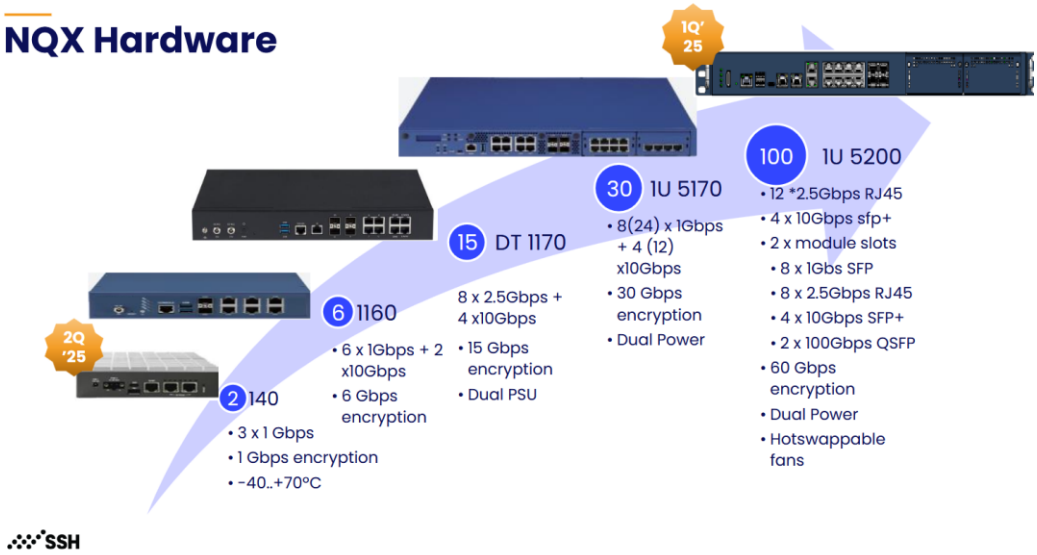


Egy lehetséges NQX architektúra

Az NQX torzítás nélkül képes tartani a gerinchálózatok sávszélességigényének dinamikus növekedését, így ideális például állami intézmények közötti összeköttetések vagy banki adatközpontok között. Fontos kiemelni, hogy egy NQX eszköz egyedülálló módon tud működni Layer 2 módban (Ethernet) és Layer 3 módban (IP) is. Ez nagy előny, mert így egyaránt alkalmazható hagyományos IP-alapú WAN/VPN titkosításra, illetve közvetlen optikai/Ethernet átvitel titkosítására. Az L2-es működésnek köszönhetően zökkenőmentesen beilleszthető akár ipari hálózatokba is.

Integráció és üzembe helyezés szempontjából az NQX nagy előnye, hogy nem igényel speciális új infrastrukturális elemeket. Teljesen kompatibilis a meglévő hálózati topológiákkal: gyakorlatilag egy titkosító eszköz, amit a védeni kívánt összeköttetés két végére kell illeszteni. Mivel standard Ethernet/IP interfészekkel dolgozik, bármilyen switch vagy router mögé beköthető anélkül, hogy a hálózat többi részét érintenénk. **Az NQX költséghatékonyabb megoldás, mint a QKD:** egyfelől olcsóbb eszközökből áll, másfelől a

már meglévő infrastruktúrán fut, így nincs extra telepítési költség. Skálázhatósága kétirányú: vertikálisan, erősebb hardverre cserélve bírja a nagyobb terhelést; horizontálisan pedig tetszőleges számú eszköz telepíthető párhuzamosan a hálózat különböző pontjain. Támogatja a nagy rendelkezésre állást (HA) is, azaz fürtözhető annak érdekében, hogy egy eszköz kiesése ne okozzon szolgáltatásleállást.



Az NQX webalapú kezelőfelületén áttekinthető módon konfigurálhatók a titkosítási kapcsolatok, kulcsbeállítások, hálózati interfészek. A rendszer naplózza és monitorozza a forgalmat, így megfelelés esetén riportokat is lehet készíteni. Fontos megjegyezni, hogy az NQX megszerezte a finn Nemzeti Kiberbiztonsági Központ minősítését „NATO Restricted / EU Restricted" szintre, ami igazolja, hogy megfelel a szigorú kormányzati-biztonsági követelményeknek. Jelenleg folyamatban van a még magasabb „Confidential" szintű tanúsítás is. Az NQX pozícionálása tehát rendkívül széles. Lényegében mindenütt hasznos, ahol bizalmas adatok mozgását kell védeni a kvantumfenyegetések ellen.

A RelNet szakértői csapata az SSH NQX bevezetésében is otthon van. A termék natívan integrálható az SSH egyéb biztonsági szoftvereivel. Az **SSH PrivX PAM** rendszeréhez tartozó Key Manager modul már felkészült a posztkvantum korszakra: képes felmérni egy szervezet kulcsinfrastruktúrájának PQC érettségét, és alapértelmezésben tartalmazza az szükséges szabályrendszereket, metrikákat és riportokat. A PrivX automatikusan kimutatja, mely kulcsok, algoritmusok nem kvantumbiztosak, hol kell őket cserélni, és javaslatokat ad a teendőkre. Ez óriási segítség a kriptográfiai eszközleltár összeállításában és migrációjában, ami az átállás egyik legnehezebb része.

Végül megemlítendő, hogy az SSH kínál úgynevezett **NQX Demo Kit csomagot** is, amely kiválóan alkalmas a technológia kipróbálására éles bevezetés előtt. A demó készlet tartalmaz 2 darab NQX titkosító eszközt és 1 darab Cluster Manager vezérlőt, amelyekkel szimulálható egy két végpontú titkosított hálózat felépítése. A RelNet szakemberei be tudják mutatni az NQX működését „élőben": látható, ahogy a két eszköz között kiépül a

kvantumbiztos kapcsolat, és a Cluster Manager felületen nyomon követhető a forgalom titkosítása, a kulcscsere folyamata és a rendszer teljesítménye. Ez a gyakorlati bemutató sok ügyfelünknek segített megérteni a technológia előnyeit és egyszerű integrálhatóságát.

SSH NQX Demo Kit kicsomagolási videója a RelNet szakembereitől

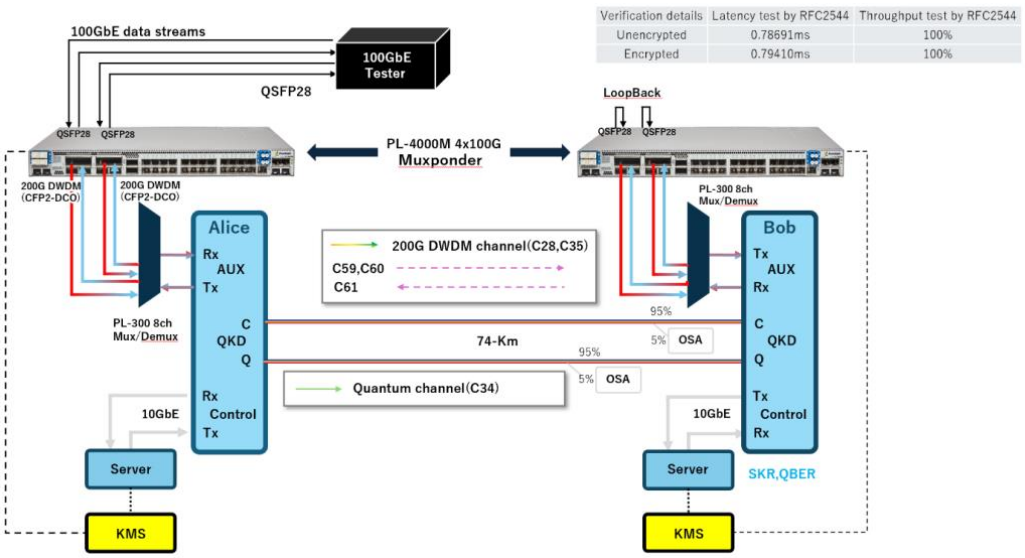
PacketLight Networks – QKD integráció optikai hálózatokban

A PacketLight Networks elsősorban DWDM/OTN megoldásairól ismert. Az utóbbi években e gyártó nagy hangsúlyt fektetett arra, hogy eszközei beépített titkosítási funkciókkal rendelkezzenek, és felkészültek legyenek a QKD technológia integrációjára. Ez azt jelenti, hogy a PacketLight DWDM/OTN berendezései – melyek tipikusan az adatközpontok közötti nagysebességű optikai összeköttetések fő aktív elemei – képesek fogadni a kvantumkulcs-elosztó rendszerek által generált kulcsokat, és azokat felhasználva titkosítani a rajtuk áthaladó adatot (ún. Layer 1 szintű, azaz optikai csatorna titkosítás).

A kvantumszámítógépek fejlődése az optikai hálózatokat is veszélyezteti, ami szükségessé teszi a biztonság növelését és a kulcscserék megerősítését. Az IT-szakemberek hajlamosak kevésbé törődni a optikai hálózatok biztonságával, hiszen fizikailag védett kábelekről van szó. Azonban egy tenger alatti kábel vagy bármilyen gerinchálózati szál lehallgatható speciális eszközökkel anélkül, hogy azt a tulajdonos észrevenné. A PacketLight szerint a megoldás kulcsa a kvantumkulcs-elosztás integrálása az optikai titkosításba. A QKD segítségével a két végponti eszköz feltörhetetlen titkosítási kulcsokat tud megosztani egymással, kvantumszintű védelmet nyújtva a kommunikációban.

1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
info@relnet.hu

A PacketLight eszközök ennek érdekében kompatibilisek olyan QKD rendszerekkel, mint a HEQA Security, a Toshiba vagy az ID Quantique megoldásai. A PacketLight Networks és a Toshiba Digital Solutions már 2024-ben sikeresen demonstrálta a kvantumkulcsok DWDM kapcsolatokon keresztül történő elosztását, melyet a HEQA Security eszközeivel is megvalósítottak.



A PacketLight-Toshiba QKD integráció részletes taglalása a RelNet weboldalán

A RelNet kínálatában a PacketLight azért stratégiai fontosságú, mert így olyan „kulcsrakész" optikai titkosító megoldást tudunk adni, amely a lehető legmagasabb szintű kvantumbiztonságot nyújtja, ugyanakkor kihasználja a meglévő optikai összeköttetéseket. Például egy országos banki összeköttetés esetén be tudunk építeni PacketLight DWDM berendezéseket, amelyek egyrészt elvégzik a szükséges multiplexelést, másrészt titkosítják a teljes forgalmat. E titkosítás kezdetben lehet nem kvantumbiztos AES-256 alapú, majd, amikor az ügyfél készen áll, hozzá lehet adni a rendszerhez a QKD eszközöket (pl. HEQA Security QKD-t vagy más gyártót), és onnantól kezdve a PacketLight automatikusan a QKD által generált kulcsokkal frissíti a titkosító kulcsait, a hálózat teljesítményének csökkenése, valamint kompatibilitási problémák nélkül.

A PacketLight a Toshibával közösen 400 Gbps DWDM linken sikeresen mutatta be a QKD integrációt nagy sebességen. A HEQA Security-vel folytatott együttműködésével pedig meglévő telekom hálózatok utólag kvantum-biztossá tehetők. A RelNet szakértői e projektek tanulságait ismerik és készen állnak magyarországi környezetben is adaptálni a megoldást (pl. szolgáltatói DWDM hálózat kvantumbiztossá tétele a törvényi megfelelés érdekében). A RelNet számára kiemelten fontos, hogy a PacketLight és a HEQA Security hivatalos disztribútoraként egy kézből tudja kiszolgálni a DWDM és QKD igényeket.

RelNet innováció és tapasztalat

A fenti gyártói megoldásokon és a megszerzett tapasztalatokon túl a RelNet szakemberei évek óta részt vesznek innovatív kísérletekben és eszköztesztelésekben a kvantumbiztos kriptográfia terén. Egy említésre méltó példa, hogy a 2010-es évek közepén Orosz Nándor, a RelNet jelenlegi projekt- és szolgáltatásigazgatója, akkoriban a **T-Systems Magyarország vállalatban tagja volt annak a csapatnak, amely sikeresen valósított meg titkosítást egy 12.288 bites RSA kulccsal.** Ez a kísérlet felhívta a figyelmet a kvantumkockázatokra, és az akkori technológiai adottságokat a korlátukig feszítve keresett védelmet a futurisztikusnak tűnő támadások ellen. Összehasonlításként: ma a legtöbb HTTPS weboldal 2048 bites RSA kulcsokat használ, a katonai alkalmazásokban esetleg 4096 bites kulcsokat találunk. A 12 kbit hosszúságú RSA kulcs extrém méretű, a biztonsága elméletileg meghaladja még a kvantumszámítógépek feltörési kapacitását is. A kísérlet érdekessége, hogy egy ekkora kulcshoz tartozó tanúsítvány kiállítása közel egy teljes napig tartott, mivel a számítási igénye óriási. Bebizonyosodott, hogy a kvantumkorszak előtt rendszerek határait is feszegetni lehet a fenyegetések kivédése érdekében. Kiderült azonban az is, hogy a klasszikus algoritmus bitméretének drasztikus növelése nem járható út, mert műszakilag gazdaságtalan és nehézkes. A jövő inkább a szabványosított PQC algoritmusoké és a kvantumtechnológiáké, amelyek hatékonyan és szabványosan biztosítják a védelmet.

Összegzés

A kvantumkorszak eljövetele a kibertér védelmezőitől proaktív választ követel. A RelNet – felismerve a fenyegetést és a lehetőséget – egyedülállóan széles megoldásportfóliót épített ki a poszt-kvantumtitkosítás terén, magában foglalva a kvantum alapú kulcselosztást és a kvantumbiztos algoritmusokra épülő hálózatbiztonságot is. Legyen szó törvényi megfelelésről, üzleti titkok hosszú távú védelméről a „harvest now, decrypt later" fenyegetéssel szemben, vagy éppenséggel technológiai versenyelőny megszerzéséről – mi készen állunk segíteni. A bemutatott HEQA, SSH és PacketLight megoldások mind azt szolgálják, hogy az Ön szervezete már ma biztonságban tudhassa adatait a holnap támadóival szemben. A RelNet felkészült csapata tanácsadással, tervezéssel és implementációval áll rendelkezésre, hogy a kvantumváltás zökkenőmentes és eredményes legyen.

Készüljön fel velünk a kvantumkorszakra! Védje adatait már ma a jövő fenyegetéseitől!

PQC és QKD témájú képzések a RelNet eLearning programban

Az SSH.COM megoldásai a kvantuminformatika korában

NQX: Az SSH kvantumbiztos megoldása

PacketLight – DWDM hálózatok építése 800G és 1,6T adatátvitelhez

EIVOK – A poszt-kvantum korszak kihívásai