MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

cesnet

VŠB TECHNICKÁ UNIVERZITA OSTRAVA

# NESPOQ

## Kybernetická bezpečnost sítí v postkvantové éře

Projekt výzvy MVČR Impakt VJ01010008

Etapa 5:Návrh bezpečnostní koncepce systému, upřesnění požadavků případů užití ve spolupráci s NÚKIB

NÚKIB

# BEZPEČNOSTNÍ KONCEPCE SYSTÉMU

## Popis etapy

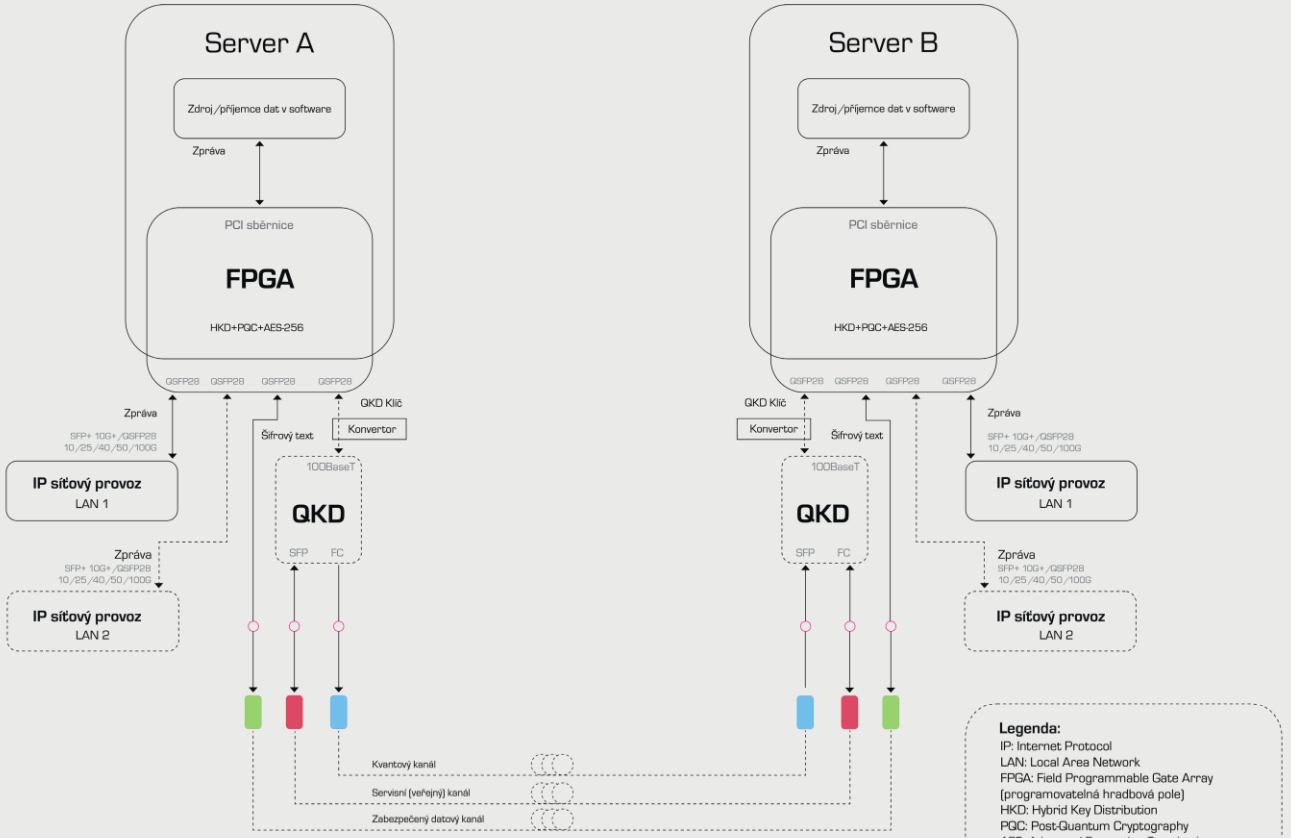
- Číslo: 1.5
- Doba trvání: 07 – 12/2021
- Řešitelé: VUT v Brně + CESNET
- Popis: Návrh bezpečnostní koncepce systému, upřesnění požadavků případů užití ve spolupráci s NÚKIB

# BEZPEČNOSTNÍ KONCEPCE SYSTÉMU

## BLOKOVÉ SCHÉMA ŠIFRÁTORŮ ODOLNÝCH VŮČI KVANTOVÝM ÚTOKŮM

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY




**Legenda:**
IP: Internet Protocol
LAN: Local Area Network
FPGA: Field Programmable Gate Array (programovatelná hradbová pole)
HKD: Hybrid Key Distribution
PQC: Post-Quantum Cryptography
AES: Advanced Encryption Standard
QKD: Quantum Key Distribution
FC: Fixed Connection
SFP: Small Form-Factor Pluggable
QSFP: Quad Small Form Factor Pluggable

Tento projekt „Kybernetická bezpečnost sítí v postkvantové éře" č. VJ01010008 byl podpořen Ministerstvem vnitra ČR z Programu Impakt 1.

# BEZPEČNOSTNÍ KONCEPCE SYSTÉMU

## POŽADAVKY NA SYSTÉM A JEJICH ŘEŠENÍ

| ID | Název požadavku | Popis požadavku | Vliv na bezpečnost |
|---|---|---|---|
| N01 | Šifrování ze zdroje aplikace/síť | Zdrojem zprávy pro šifrování může být jak aplikace v OS serveru, tak síťové rozhraní šifrátoru. | Definuje zdroje otevřené zprávy. |
| N02 | Autonomní FPGA | Soustředit co nejvíce funkcí do FPGA, v ideálním případě zajistit samostatnou funkčnost bez serveru. | Snižuje riziko útoků využívající zranitelnosti na OS serveru. |
| N03 | 1 optická linka pro QKD/PQC/Data | Pokud to bude realizovatelné za přiměřeného úsilí, vyzkoušet možnost použití 1 optické linky pro potřeby ustanovení klíče (QKD i PQC) i pro datový přenos. | Zvyšuje efektivitu a snižuje počet vláken, které jsou útočníkovi k dispozici, ale také negativně ovlivní bezpečnost - zavedení jednoho bodu chyby, vyšší riziko narušení. |
| N04 | Optimalizace na rychlost | Optimalizace pro výkon a rychlost, nikoliv velikost a zdroje čipu. | Důraz na rychlost se může negativně projevit ve zvýšené složitosti aplikace ochran před PK. |
| N05 | PQC algoritmy dle NIST | Preference algoritmů standardizovaných v rámci NIST (AES, NISTIR 8309). | Volba standardních schémat pozitivně ovlivní budoucí kompatibilitu a měla by mí pozitivní vliv na bezpečnost z důvodu použití známých a ověřených algortitmů. |
| N06 | Návrh pro páteřní spoje | Předpoklad dvoubodového spoje v rámci několika kilometrů, případné testování v KII. | Jednoduší topologie, menší riziko útoků z různých stran. |
| N07 | Ochrana před postranními kanály | Kde to bude možné, volit prvky odolné vůči analýze postranními kanály. | Mitigace útoků PK zvýší celkovou bezpečnost. |
| N08 | Důraz na autentičnost stran | Ustanovení klíče musí být autentizované, nutnost použití PQC podpisů či schémat pro ustanovení klíče zajišťující autentičnost stran. | Jedná se o zásadní požadavek na bezpečnost. |
| N09 | Minimální délka optického spoje: 40 km | Délka je dána dynamickým rozsahem systému, který by měl být min 12 dB. | Požadavek má jen částečný vliv na bezpečnost, hrozí ale vyšší chybovost QKD. Nutné brát v potaz bezpečnost COW na větší vzdálenosti. |
| N10 | Centrální vlnová délka kvantového kanálu: C pásmo, DWDM kanál | Standardní telekomunikační optické vlákno vykazuje nejmenší měrný útlum v C pásmu, proto je pro přenos kvantového kanálu nejvhodnější. Podmínkou rovněž byla centrální vlnová délka v DWDM gridu z důvodu možnosti následné multiplexace kanálů. | Požadavek nemá přímý vliv na bezpečnost. |
| N11 | Servisní kanály s flexibilní vlnovou délkou | Vlnové délky servisních kanálů by mělo být možné snadno měnit, ideálně pomocí SFP modulů. | Požadavek nemá přímý vliv na bezpečnost. |

# Bezpečnostní koncepce systému

## Hlavní prvky bezpečnostní koncepce:

Modularita:

- Systém je složen z více prvků, které jsou vyměnitelné.
- QKD – ID Quantique Clavis 3,
  - aktuálně jediný dostupný systém na trhu plnící bezpečnostní a funkční požadavky.
- PQC – CRYSTALS-Kyber, možná aktualizace po etapě 10
  - finalista Round 3 NIST PQC Competition (další: NTRU, SABER, McEliece).
- Symetrická kryptografie – AES256 GCM na FPGA.
- UI minimální, Linux OS.

Moderní kryptografie:

- Použití standardizovaných algoritmů, pokud je to možné,
- Reflektování doporučení NÚKIB, NIST, ENISA, E-CRYPT, BSI, ANSSI.
- CRYSTALS-Kyber, AES256 GCM, OTP/SHA3 pro kombinaci klíče?

# Bezpečnostní koncepce systému

## Hlavní prvky bezpečnostní koncepce:

### Redundance:

- Kombinace PQC a QKD, hybridní ustanovení klíče.
- Možnost náhrady algoritmů PQC, zařízení QKD i mechanismu vzniku hybridního klíče.
- Paralelní využití 2 odlišných mechanismů založených na velmi odlišných principech.

### Hardwarová implementace:

- Implementace na FPGA nejen z důvodu zrychlení, ale také bezpečnosti.
- V dalších fázích zohlednění rizik útoků postranními kanály.
- Snaha o nezávislý PCI šifrátor (?další výzkum?).
- Snazší případná certifikace vyloučením OS.

# Bezpečnostní koncepce systému

## Další prvky bezpečnostní koncepce:

### Bezpečná implementace:

- Bezpečné generování náhodných čísel na platformě FPGA (výzkum vhodných postupů).
- Minimalizace použití knihoven třetích stran (případně jejich ověření).

### Klíčový management a autentizace:

- Bezpečný klíčový management - přenos, exspirace a účel klíčů.
- Silná autentizace uživatelů a stran při dohodě klíče.
- Minimalizace uchovávání klíčů v paměti a v OS serveru, přímý transfer klíče z QKD do FPGA.
- Využití čipové karty pro bezpečné uchování klíče a pro certifikáty?

### Testování a kompatibilita:

- Prověření funkčnosti a bezpečnosti dílčích bloků.
- Testování celkového řešení (funkčnost, stabilita, odolnost proti chybám, bezpečnost).
- Ověření kompatibility s jinými zařízeními QKD?

# Požadavky na případy užití

**Laboratorní nasazení**

- Cílem je ověřit základní funkčnost systému.
- Laboratoř FEKT VUT v Brně
- Vzdálenosti 10km, 25km, 50 km.
- Právě probíhá.

**Experimentální nasazení**

- Cílem je ověřit parametry QKD systému na větší vzdálenosti, v reálné síti.
- Nasazení mezi budovami, institucemi v rámci Brna

**Pilotní nasazení**

- Cílem je ověřit funkčnost systému v reálném prostředí, s plnou funkcionalitou (šifrování, sloučení vláken, plná rychlost, atp.)
- Vytvoření mobilního testbedu
- Nasazení u partnerských institucí (NUKIB)
- Využití infrastruktury CESNET.

# POŽADAVKY NA PŘÍPADY UŽITÍ

## LABORATORNÍ NASAZENÍ

- 9/2021 FEKT VUT V BRNĚ


# Požadavky na případy užití

**Požadavky:**

- Infrastructure2Infrastructure (dvoubodové spoje spojující větší sítě)
- Vzdálené lokality, až několik desítek km
- Rychlost 10 – 100Gbps
- Využití minima vláken
- Integrace s IPv4 prostředím
- Snadnost konfigurace, používání
- Stále pilotní nasazení, nikoliv ostrý provoz
- Možnost měření a testování (bezpečnostní, zátěžové, atp.)

# Požadavky na případy užití

**Vychází ze skutečného požadavku na případ užití**

**Požadavky:**

- Datacenter2Datacenter (dva nezávislí poskytovatelé služeb)
  - Zabezpečení ověřování generovaných veličin mezi body a - b
- Metropolitní vzdálenosti, do 30 km
  - 27.7 km odhad délky optické trasy
- Rychlost do 10Gbps
- Využití minima vláken
  - Dostupnost dalších prochází ověřením
- Stále pilotní nasazení, nikoliv ostrý provoz
- Možnost měření a testování (bezpečnostní, zátěžové, atp.)
  - Poskytování součinnosti, sdílení výsledků

# Požadavky na případy užití

**Otevřené pro vstupy od AG během workshopu**

**Omezující požadavky:**

- Lokality vzdálené (fyzický průběh) do 50 km
- Kvantový a klasický (datový) kanál v samostatných vláknech
- Další vstupy z dotazníku, link níže

https://forms.gle/aRS97szi7Xxzjn7x7

# DĚKUJI ZA POZORNOST


CESNET, z. s. p. o.

Ing. Josef Vojtěch, Ph.D.

Zikova 4

160 00 Praha 6

+420 234 680 377

VUT v Brně

doc. Ing. Jan Hajný, Ph.D.

Technická 12

616 00 Brno

+420 608 823 522

VŠB TUO

prof. Ing. Miroslav Vozňák, Ph.D.

17. listopadu 2172/15,

Ostrava-Poruba 708 00

+420 603 565 965