Spolufinancovaný Európskou úniou

PROGRAM SLOVENSKO

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodický dokument riadiaceho orgánu pre Program Slovensko č. 2

FORMULÁR ZÁMERU NÁRODNÉHO PROJEKTU

Schválil:
Ladislav Šimko
generálny riaditeľ
sekcia riadenia programu Slovensko a koordinácie fondov EÚ

Verzia: 2.1

Dátum vydania: 22.11.2024

Dátum účinnosti: 22.11.2024

Spolufinancovaný Európskou úniou

Zámer národného projektu[1]

Názov národného projektu (ďalej aj „NP“):

Výskum a vývoj post-kvantových šifrových algoritmov - prvá etapa

Žiadateľ[2]:

Obchodné meno/názov	**Národný bezpečnostný úrad**
Sekcia	Sekcia akreditácie a certifikácie
Právna forma	rozpočtová organizácia
Sídlo	Budatínska 30, 851 06 Bratislava

Poskytovateľ: Ministerstvo školstva, vedy výskumu a športu SR

Partner, ktorý sa bude zúčastňovať na implementácii aktivít NP (ak je to relevantné)

Obchodné meno/názov	**Matematický ústav Slovenskej akadémie vied, v. v. i.**
Právna forma	verejná výskumná inštitúcia
Sídlo	Štefánikova 49, 814 73 Bratislava
IČO	00166791
Zdôvodnenie potreby partnera NP[3]	Nerelevantné
Kritériá pre výber partnera[4]	Nerelevantné
Má partner jedinečné postavenie na implementáciu týchto aktivít? Ak áno, na akom základe?	Matematický ústav SAV má dlhodobú expertízu v oblasti matematických kvantových štruktúr, ktoré boli študované ešte pred vznikom výskumnej oblasti kvantovej informácie, v ktorej našli svoje uplatnenie. Na ústave sa systematicky venujú praktickej kryptografii a, s rozvojom kvantových technológií, sa výskumne zúčastňujú na projektoch zameraných na štandardizáciu post-kvantovej kryptografie – kryptografie schopnej odolať (budúcim) kvantovým počítačom.

V prípade viacerých partnerov, doplňte údaje za každého partnera.

Sumárne informácie o NP

Celkové oprávnené výdavky NP (v EUR)	19 982 400,- €
Miesto realizácie projektu (na úrovni kraja, resp. celé územie Slovenskej republiky)	celá SR
Identifikácia hlavných cieľových skupín (ak relevantné)	subjekty verejnej správy a nimi zriadené subjekty, vrátane subjektov územnej samosprávy; sektor výskumných organizácií; vedecko-výskumní a vývojoví zamestnanci; akademický sektor; podnikateľský sektor;

[1] Formulár zámeru NP predstavuje minimálny obsahový štandard, ktorý je poskytovateľ oprávnený dopĺňať a rozširovať na základe svojich potrieb.

[2] Uviesť aj názov sekcie, ak je to relevantné. Žiadateľom je osoba, ktorá žiada o poskytnutie príspevku do nadobudnutia účinnosti zmluvy o poskytnutí nenávratného finančného príspevku alebo právoplatnosti rozhodnutia podľa § 13 ods. 2 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, alebo osoba, ktorá predkladá zámer NP.

[3] Pod partnerom sa rozumie partner ako je definovaný v § 3, písm. t) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[4] Uveďte, na základe akých kritérií bol partner vybraný, alebo ak boli kritériá zverejnené, uveďte odkaz na internetovú stránku, kde sú dostupné. Ako kritérium pre výber partnera môže byť tiež uvedená predchádzajúca spolupráca žiadateľa s partnerom, ktorá bude náležite opísaná a odôvodnená, avšak nejde o spoluprácu, ktorá by v prípade verejných prostriedkov spadala pod pôsobnosť zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Projekt so špecifickým určením pre marginalizované rómske komunity[5]	nie

Začlenenie národného projektu v štruktúre Programu Slovensko[6]

Cieľ politiky súdržnosti[7]	1 Konkurencieschopnejšia a inteligentnejšia Európa vďaka presadzovaniu inovatívnej a inteligentnej transformácie hospodárstva a regionálnej prepojenosti IKT
	Vyberte položku.
	Vyberte položku.
Priorita	1P3. Platforma strategických technológií pre Európu (STEP)
	Vyberte položku.
	Vyberte položku.
Špecifický cieľ	RSO1.6. Podpory investícií, ktoré prispievajú k cieľom Platformy strategických technológií pre Európu uvedeným v článku 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/795 (EFRR)
	Vyberte položku.
	Vyberte položku.
Opatrenie (ak relevantné)	Vyberte položku.
	Vyberte položku.
	Vyberte položku.
Súvisiace typy akcií[8]	podpora rozvoja postkvantovej kryptografie a bezpečnosti

Zákonné požiadavky

§ 23 ods. 3 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

NP bude realizovaný v súlade s horizontálnymi princípmi s povinnosťou dodržania súladu projektu s Chartou základných práv Európskej únie, rodovou rovnosťou , nediskrimináciou a prístupnosťou osôb so zdravotným postihnutím, ktoré sú definované v Partnerskej dohode SR na roky 2021 – 2027 a v čl. 9 nariadenie o spoločných ustanoveniach, berúc do úvahy Chartu základných práv Európskej únie a povinnosti vyplývajúce z Dohovoru OSN o právach osôb so zdravotným postihnutím a zabezpečenia prístupnosti v súlade s jeho článkom 9, ako horizontálne základné podmienky. Pri implementácii plánovaných aktivít projektu sa budú dodržiavať všetky články Charty ZP EÚ s dôrazom najmä na

[5] Zo zoznamu sa vyberie:
- "**áno**" – ak, projekt bude financovaný výhradne z alokácie so špecifickým určením pre marginalizované rómske komunity (ďalej len „MRK“) uvedenej v Programe Slovensko,
- "**nie**" - ak, projekt nebude v žiadnej miere financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko,
- "**čiastočne**" – ak, projekt bude z časti financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko.

[6] V prípade zámeru NP, ktorý sa plánuje financovať z viacerých cieľov politiky súdržnosti / priorít / špecifických cieľov / opatrení sa vyberú zo zoznamu viaceré položky.
Zákon č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Rámec implementácie fondov a metodický dokument č. 2 riadiaceho orgánu pre Program Slovensko neobmedzujú, resp. nevylučujú možnosť spojiť dva schválené zámery národných projektov do jednej výzvy, resp. na jeden schválený zámer národného projektu vyhlásiť dve výzvy na predloženie národných projektov. V takýchto prípadoch bude riadiaci orgán posudzovať výzvu tak, aby boli splnené všetky parametre schváleného/schválených zámeru/zámerov národného projektu berúc na zreteľ povolené odchýlky.
[7] V prípade Fondu na spravodlivú transformáciu sa vyberie "-".
[8] V súlade s informačným monitorovacím systémom.

články Charty ZP EÚ, ktoré sa najviac vzťahujú k plánovaným intervenciám, aktivitám a cieľovým skupinám.

V súvislosti so všetkými plánovanými aktivitami bude zohľadnený v rámci NP princíp rovnosti mužov a žien a princíp nediskriminácie tak, aby nedochádzalo k znevýhodneným podmienkam pre akúkoľvek skupinu osôb a aby boli vytvorené podmienky prístupnosti aj pre osoby so zdravotným postihnutím k fyzickému prostrediu, k informáciám a komunikácii vrátane informačných a komunikačných technológií a systémov, ako aj k ďalším prostriedkom a službám dostupným alebo poskytovaným verejnosti.

1. Dôvod určenia prijímateľa NP[9]

Jednoznačne a stručne zdôvodnite výber prijímateľa NP ako jedinečnej osoby oprávnenej na realizáciu NP (napr. odkazom na Program Slovensko, v ktorom je priamo uvedený prijímateľ; odkazom na platné predpisy, podľa ktorých má prijímateľ osobitné, jedinečné / unikátne kompetencie na implementáciu aktivít NP priamo zo zákona; odkazom na národnú stratégiu, ktorá odôvodňuje jedinečnosť prijímateľa NP a pod.).

Šifrová ochrana informácií predstavuje jednu z kľúčových súčastí národnej bezpečnosti, technologickej suverenity a ochrany spoločnosti pred neoprávneným prístupom k osobným údajom, citlivým informáciám a súkromiu ako takému. V prostredí rýchlo sa vyvíjajúcich digitálnych technológií a neustále sa zvyšujúcej komplexnosti hrozieb v kybernetickom priestore je nevyhnutné, aby štát zabezpečil vývoj a implementáciu vlastných kryptografických riešení, odolných voči moderným prostriedkom prelomenia. Tieto musia byť navrhované s ohľadom na aktuálne aj budúce hrozby, medzi ktoré dnes jednoznačne patrí aj príchod kvantových technológií.

Jednou z najzásadnejších výziev v oblasti kryptografie je nástup kvantových výpočtových technológií, ktoré majú potenciál prelomiť väčšinu dnes používaných asymetrických šifrovacích algoritmov (napr. RSA, ECC). Tieto algoritmy tvoria základ nielen pre bezpečnú komunikáciu, ale aj pre digitálne podpisy, autentifikáciu a integritu dát v rámci štátnej správy, obrany, súdneho systému, zdravotníctva ale aj súkromných firiem a podnikov. V reakcii na tieto výzvy prebieha na medzinárodnej úrovni výskum a štandardizácia tzv. post-kvantovej kryptografie (PQC), teda kryptografických algoritmov, ktoré odolávajú výpočtovej sile kvantových počítačov.

Pre Slovenskú republiku je nevyhnutné, aby sa v tejto oblasti nielen pasívne prispôsobovala zahraničným štandardom, ale aby sa aktívne podieľala na výskume, vývoji a testovaní vlastných post-kvantových riešení. To umožní nielen lepšiu ochranu kritických systémov, ale aj vyššiu mieru nezávislosti od externých dodávateľov.

V oblasti šifrovej ochrany informácií zohráva Národný bezpečnostný úrad kľúčovú úlohu pri nastavovaní národných bezpečnostných štandardov, identifikácii rizík a pri zabezpečovaní bezpečnostnej kompatibility kryptografických riešení. Národný bezpečnostný úrad zodpovedá za tvorbu a realizáciu štátnej politiky pre oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti, šifrovej služby a dôveryhodných služieb. V súlade s § 70 ods. 1 písm. a) bod 14 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností Národný bezpečnostný úrad vykonáva a zabezpečuje výskum a vývoj v oblasti bezpečnosti informačných technológií, podľa § 70 ods. 1 písm.

[9] V prípade, ak ide o prijímateľa, ktorý nie je určený v Programe Slovensko, alebo ktorého kompetencie nevyplývajú z osobitných predpisov podľa zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, príslušná komisia pri Monitorovacom výbore pre Program Slovensko schválením zámeru NP schvaľuje aj prijímateľa NP. V opačnom prípade sa prijímateľ NP neposudzuje.

c) bod 9 cit. zákona vykonáva a zabezpečuje výskum a vývoj v oblasti kryptológie ako aj výskum a výrobu prostriedkov šifrovej ochrany informácií a podľa § 5 ods. 1 písm. x) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov Národný bezpečnostný úrad koordinuje výskum a vývoj v oblasti kybernetickej bezpečnosti.

Národný bezpečnostný úrad takisto zabezpečuje správu a realizáciu prevádzky zverených informačných systémov úradu vrátane správy používateľských účtov, zabezpečuje správu a prevádzku systémov utajovaného vládneho a utajovaného zahraničného spojenia a vykonáva bezpečnostný dohľad sieťových a aplikačných parametrov komunikačných a informačných systémov na ochranu utajovaných skutočností.

V oblasti šifrovej ochrany informácií úrad plní úlohy ústredného šifrového orgánu Slovenskej republiky. Vykonáva certifikáciu jej prostriedkov, vydáva bezpečnostné štandardy a koordinuje výskum a vývoj prostriedkov šifrovej ochrany. V neposlednom rade plní úlohu garanta národnej autority v medzinárodnej spolupráci a zabezpečuje funkciu Národnej distribučnej autority, ktorá je vstupným a kontaktným bodom Slovenskej republiky pri výmene a distribúcii prostriedkov šifrovej ochrany informácií a šifrových materiálov prostredníctvom Národnej distribučnej autority a plní úlohy Národ- nej distribučnej autority pre distribúciu COMSEC materiálu.

Ako národný garant pre oblasti ochrany informácií, kybernetickú bezpečnosť a šifrovú službu je Národný bezpečnostný prirodzeným centrom pre úlohy výskumu a vývoja v oblasti post-kvantových šifrových algoritmov a ich aplikácie praktickej aplikácie na riešenie výziev súčasného sveta. Prínosom je pokračovanie a kontinuita v podpore výskumu a vývoja v tejto oblasti a posilňovanie strategických partnerstiev domácich výskumníkov so zahraničnými výskumnými a vzdelávacími inštitúciami, podpore slovenskej vedy na európskej úrovni a podpore účasti slovenských výskumníkov v európskych projektoch a v neposlednom rade aj vo vyššej integrácii slovenského výskumu v spoločných európskych aktivitách. Zámer národného projektu reflektuje tieto výzvy vo svojich aktivitách.

Vzhľadom na všetky tieto skutočnosti je žiaduce, aby projekty v oblasti šifrovej ochrany informácií boli strategicky riadené garantom šifrovej služby a podporené vedecko-výskumnými kapacitami Slovenskej akadémie vied. Len tak možno zabezpečiť nielen ochranu národných záujmov, ale aj technologickú pripravenosť na výzvy budúcnosti, ktoré so sebou prináša kvantová éra. Investície do vlastného kryptografického výskumu nie sú výdavkom, ale investíciou do bezpečnosti, dôveryhodnosti a stability moderného štátu.

2. Odôvodnenie využitia NP

Vysvetlite, prečo je nevyhnutné realizovať NP, prípadne ako budú využité výstupy projektu.

Tento zámer národného projektu sa bude realizovať v rámci RSO1.6. Podpory investícií, ktoré prispievajú k cieľom Platformy strategických technológií pre Európu uvedeným v článku 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/795 (EFRR). Náplň a ciele projektu sú definované v oblasti platformy STEP - konkrétne do cieľa „Digital technologies and deep technology innovation – Artifical intelligence, quantum technologies and advanced connectivity“. Výsledky projektu zameraného na výskum a vývoj post-kvantových šifrových algoritmov prinášajú na trh inovatívny, nový a špičkový prvok s významným hospodárskym potenciálom pre jednotný trh, alebo prispievajú k znižovaniu alebo predchádzaniu strategickej závislosti EÚ.

V súčasnosti, kedy sa informácia považuje za jednu z najdôležitejších devíz, ktorou verejné a súkromné spoločnosti disponujú, sa stáva zaistenie bezpečnosti informácií prvoradou úlohou. V súvislosti so zabezpečeným prenosom informácie, ako aj s jej zabezpečeným uložením, je šifrovanie základom bezpečnosti celého digitálneho sveta a kľúčovým faktorom informačnej bezpečnosti. Bez dôveryhodného šifrovania, by samotný štát, ale aj väčšina moderných organizácií, nemohla bezpečne

fungovať. V akademickej, odbornej ale aj v oblasti politík existuje konsenzus, že kryptograficky relevantná kvantová výpočtová technika s najväčšou pravdepodobnosťou spôsobí stav, kedy šifrovanie, ktoré dnes bežne používame na ochranu informácií, či už v komerčnej, alebo nekomerčnej sfére, nebude viac dostatočne bezpečné (ODPORÚČANIE KOMISIE z 11. 4. 2024 o Pláne koordinovaného vykonávania prechodu na post-kvantovú kryptografiu: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography) alebo (REPORT ON POST-QUANTUM CRYPTOGRAPHY: https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf). Čas potrebný na prelomenie bežného asymetrického algoritmu na výmenu kľúčov, by sa mohol skrátiť z tisícov rokov výpočtového výkonu na dni, a to za použitia vhodného kvantového počítača, respektíve kvantového výpočtového systému.

Jedným z prístupov pri riešení kvantovej hrozby pre kryptografiu je tzv. post-kvantová kryptografia – úprava existujúcich šifrovacích algoritmov a schém za účelom ich zodolnenia voči predpokladaným útokom prostredníctvom kvantových algoritmov, ako je napr. Shorov algoritmus. Výhodou tohto prístupu je budovanie na doposiaľ známych a preverených technológiách, pričom sa dá považovať za akýsi medzi krok, ktorý zabezpečí šifrovanú komunikáciu voči očakávaným kvantovým útokom.

Post-kvantová kryptografia je oblasť kryptografie, v ktorej sa kryptografické schémy a algoritmy študujú za predpokladu, že útočník disponuje kryptograficky relevantným kvantovým počítačom. V roku 2017 požiadal Národný inštitút pre štandardy a technológie Spojených štátov amerických o predloženie návrhov na nových potenciálnych adeptov na šifrovacie a podpisové algoritmy s verejným kľúčom, ktoré by boli bezpečné aj za predpokladu že už existuje kvantový počítač. Táto súťaž prebiehala podobne ako v prípade známeho AES a SHA-3 v minulosti. V priebehu posledných rokov sa tak hromadili návrhy od akademikov a výskumných tímov, ktoré boli následne predstavené celej odbornej verejnosti a podrobené analýzam. Počet predložených návrhov sa postupne zužoval v niekoľkých kolách až nakoniec zostali 3 hlavní adepti : CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS+. Na základe týchto algoritmov sa budú vytvárať nové kryptografické schémy a pripravovať ich praktické nasadenie (NIST Releases First 3 Finalized Post-Quantum Encryption Standards: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards).

Zohľadňujúc vyššie uvedené, je preto najefektívnejšie nadviazať na citované medzinárodné výskumné úlohy a už zverejnené štandardy ako napríklad FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard), FIPS 204 (Module-Lattice-Based Digital Signature Standard), FIPS 205 (Stateless Hash-Based Digital Signature Standard), FIPS 206 (Falcon FN-DSA Standard) alebo AC/322(CP/4)WP(2024)0024 (NATO Crypto Toolbox). Budovanie na už existujúcom medzinárodnom výskume je vzhľadom na reálne personálne možnosti na Slovensku jediné efektívne riešenie, nebude sa plytvať čas na overovanie už existujúcich výsledkov na ktorých sa niekoľko rokov podieľali početné medzinárodné tímy, ale prejde sa do ďalšej fázy – aplikácie výskumu. Pre reálne a praktické nasadenie je potrebné tieto matematické konštrukty aplikovať do kryptografických knižníc, ktoré bude následne možné priamo implementovať v zdrojových kódoch bežných programovacích jazykov. Jedná sa najmä o knižnice pre IPSec, TLS a podobne. Najefektívnejšia sa javí podpora výskumných a vývojových úloh so zapojením akademikov pôsobiacich v oblastiach matematiky a aplikovanej matematiky s cieľom vytvorenia týchto knižníc. Jedná sa o nevyhnutnú podmienku pre ďalší vývoj v oblasti kryptografie v podmienkach Slovenskej republiky ako aj celkového Európskeho hospodárskeho priestoru.

V modernej spoločnosti je zabezpečenie informačnej a komunikačnej bezpečnosti jednou z kľúčových úloh pre plynulý chod štátu. Krajina je iba vtedy bezpečná, ak je schopná efektívne ochraňovať informácie na úrovni štátnych inštitúcií a jej bezpečnostných zložiek, zdravotníckeho systému,

finančných inštitúcií, leteckého riadenia, výroby a distribúcie energií či dopravného systému a logistiky.

Očakáva sa, že v blízkej budúcnosti dôjde k rozvinutiu kvantových počítačov na úroveň, ktorá umožní prelomiť súčasné systémy šifrovania založené na asymetrických šifrách s verejným kľúčom. Kvantovo šifrovaná komunikácia bude mať mimoriadne závažný hospodársky potenciál. Európska únia zaradila rozvoj kvantovej komunikačnej infraštruktúry medzi vlajkové iniciatívy nevyhnutné na zachovanie schopnosti poskytovať bezpečnú komunikáciu.

Vývoj kvantových počítačov v posledných dvoch dekádach zrýchľuje a existuje konsenzus v akademickej aj odbornej oblasti, ktorý predpokladá, že už v priebehu 30. rokov 21. storočia dosiahnu kvantové počítače s nezanedbateľnou pravdepodobnosťou dostatočnú úroveň a výpočtový výkon, aby predstavovali reálnu hrozbu pre kryptografické systémy, ktoré sú aktuálne využívané naprieč všetkými civilnými i štátnymi oblasťami. Tento druh výskumu napreduje najmä v veľkých krajinách s geopolitickými ambíciami ako USA a Čína a je obtiažne presne stanoviť úroveň ich pokroku, nakoľko presnejšie informácie sú úzkostlivo chránené. Rozvoj na národnej a rovnako aj európskej úrovni je tak nevyhnutný ak si chceme zachovať suverenitu v oblasti kryptografie a informačnej bezpečnosti.

Post-kvantová kryptografia navyše prináša celý rad nových technických aj organizačných výziev. Ide napríklad o otázky kompatibility s existujúcou IT infraštruktúrou, zabezpečenie dostatočnej výpočtovej efektivity, spracovanie veľkých objemov dát, ale aj potrebu výmeny kľúčových komponentov v dlhodobo fungujúcich systémoch. Dôležité je zároveň zdôrazniť, že bezpečné kryptografické riešenia nie sú určené výlučne pre štátnu správu. Ich využitie je kriticky dôležité aj pre súkromný sektor – napríklad v bankovníctve, zdravotníctve, výrobe, logistike či v oblasti správy osobných údajov. Vytvorením dôveryhodných a odolných kryptografických štandardov na národnej úrovni možno podporiť aj súkromné subjekty pri zvyšovaní ich odolnosti voči moderným kybernetickým hrozbám. Zároveň sa tým posilňuje celková kybernetická odolnosť spoločnosti, a to vrátane občanov, ktorí majú právo na bezpečnú komunikáciu a ochranu svojich údajov.

Prechod od klasických spôsobov šifrovania k post-kvantovým predstavuje absolútnu nutnosť v kontexte rastúcich kybernetických hrozieb. Aktéri kybernetických útokov, medzi ktorými sú aj niektoré štátom sponzorované skupiny, využívajú stratégiu „harvest now, decrypt later“ — teda zhromažďovanie a archivovanie dnes šifrovaných údajov s očakávaním, že ich budú schopní dešifrovať v budúcnosti, keď sa objavia funkčné kvantové počítače. Tento scenár predstavuje zvlášť vážnu hrozbu pre dáta s dlhodobou životnosťou – napríklad zdravotné, finančné alebo štátne — pretože ich dôvernosť môže byť ohrozená ešte predtým, než budú k dispozícii kvantové prostriedky. O tom, že takéto riziko reálne existuje, hovoria výzvy aj odporúčania od európskych kyberbezpečnostných orgánov; konkrétnym cieľom je začať migráciu na PQC do rokov 2030–2035, aby včas ochránili kritickú infraštruktúru a verejné služby.

Výskum a vývoj kvantových počítačov je v globálnom meradle rozbehnutý s vysokými investíciami. Spojené štáty, Čína a Rusko vynakladajú miliardy na vývoj kvantového hardvéru. Európska únia reaguje prostredníctvom iniciatív ako Quantum Technologies Flagship, EuroHPC a EuroQCI, ktoré disponujú rozpočtom približne jednej miliardy EUR na budovanie infraštruktúry a laboratórií. Vedci z európskych univerzít a inštitútov, vrátane tých slovenských, majú významný podiel na vývoji štandardizovaných post-kvantových algoritmov. Napríklad CRYSTALS-Kyber a CRYSTALS-Dilithium, ktoré boli vybrané americkou organizáciou pre štandardizáciu (NIST) ako globálne štandardy, majú pôvodné spoluautorské zapojenie európskych tímov z Holandska, Francúzska či Švajčiarska. Na Slovensku prebieha bohatá akademická činnosť – množstvo bakalárskych a magisterských prác rieši

algoritmy ako McEliece, Kyber, Dilithium, UOV, HFE, QSTS, kódovanie MDPC a rôzne vylepšenia určené pre praktické nasadenie.

Európska Komisia 11. apríla 2024 vydala odporúčanie, aby členské štáty vytvorili koordinovaný implementačný plán pre PQC a začali s jeho realizáciou do dvoch rokov. Odporúča tiež založiť pracovnú skupinu pod NIS Cooperation Group, zapojiť príslušné národné agentúry a expertné tímy na hodnotenie, výber a implementáciu európskych algoritmov a prípravu legislatívnych a štandardizačných rámcov. Tento krok má za cieľ posilniť spoločný európsky postoj a harmonizovanú migráciu.

Z obchodného a priemyselného pohľadu má post-kvantová kryptografia obrovský potenciál. Vyvíjajú sa pilotné implementácie v bankovom sektore, telekomunikáciách a zdravotníctve. Vývoj a sprístupňovanie riešení PQC môže slovenským a európskym organizáciám priniesť konkurenčnú výhodu na globálnom trhu. Okrem toho by sa mali rozvíjať kompetencie v oblasti flexiblity protokolov tzv. „cryptographic agility“, teda schopnosť jednoducho meniť kryptografické schémy bez zásahu do architektúry systémov, čo je už súčasťou odporúčaní ENISA a európskych odborníkov.

Z pohľadu národnej bezpečnosti je nevyhnutné chrániť dôverné komunikácie vládnych inštitúcií, ako aj kritické systémy a občianske dáta. Štátne systémy, poskytujúce verejné služby, PKI infraštruktúra, ale aj nemocnice, energetické spoločnosti či doprava sú veľmi zraniteľné voči prelomeniu šifrovacích algoritmov, čo by viedlo k nenapraviteľným prevádzkovým, reputačným a aj finančným dopadom. Ak tieto systémy nebudú migrovať, dôvernosť a autenticita dát bude ohrozená.

Slovensko má výskumný potenciál aj projekty, no chýba mu širšia systémová koordinácia, zapojenie priemyslu a silnejší tlak na edukáciu nových odborníkov. Práve predkladaný projekt je vhodnou príležitosťou začať napravať tento stav a zapojiť širokú bázu odborníkov v oblasti PQC a vytvoriť tak utilizovaný systém postupného prechodu na nové šifrovacie algoritmy a vytvorenie nástrojov, v ktorých budú tieto algoritmy implementované.

Národný projekt bude realizovať Národný bezpečnostný úrad v spolupráci s Matematickým ústavom Slovenskej akadémie vied. Vďaka získaným projektovým výstupom očakávame zlepšenie v oblasti:

- **zvýšenej bezpečnosti citlivých dátových tokov pre verejný aj súkromný sektor**, s dôrazom na komunikáciu v rámci priemyslu, súkromného sektora, štátnych orgánov a kritickej infraštruktúry, pričom sa zabezpečí dlhodobá dôvernosť a integrita informácií aj po nástupe kvantových výpočtových technológií,
- **výskumu** – prínos v podobe novej expertízy a špecializovaných vedeckých kapacít v oblasti kryptografie, kybernetickej bezpečnosti, zvýšenie úspešnosti pri zapájaní sa do prestížnych medzinárodných výziev (napr. Horizon Europe, Digital Europe), vznik nových výskumných smerov ako je napríklad post-kvantová bezpečnosť v zdravotníctve, doprave alebo v smart infraštruktúre, ako aj podpora interdisciplinárneho prepájania vedných odborov – od matematiky cez informatiku až po IT právo,
- **možností použitia overených algoritmov post-kvantovej kryptografie pre verejný a súkromný sektor v existujúcich a nových riešeniach**, čím sa urýchli adopcia bezpečnostných štandardov odolných voči kvantovým útokom v infraštruktúrach ako sú e-Government, digitálna identita, bankovníctvo, IoT alebo cloudové služby,
- **konkurencieschopnosti Slovenska**, najmä v oblasti bezpečnostných technológií, čo umožní slovenským subjektom ponúkať inovatívne riešenia na domácom i medzinárodnom trhu,

zlepšiť ich pozíciu v európskych technologických hodnotových reťazcoch a zároveň posilniť technologickú suverenitu krajiny,

- **zvýšenej odolnosti kritickej infraštruktúry**, kde budú môcť byť post-kvantové algoritmy implementované do riadiacich systémov energetiky, dopravy, telekomunikácií a verejného zdravia s cieľom eliminovať riziko narušenia ich činnosti kvantovými útokmi v budúcnosti,
- **budovania národnej expertnej základne**, čím sa zlepší dlhodobá personálna kapacita Slovenska v oblasti bezpečnosti,
- **posilnenia digitálnej suverenity a geopolitickej bezpečnosti Slovenska**, keďže vlastný výskum a vývoj v oblasti šifrovacích technológií minimalizuje závislosť od mimoeurópskych bezpečnostných riešení a zvyšuje schopnosť samostatne reagovať na kybernetické hrozby aj v prípade globálnych konfliktov alebo prerušenia dodávateľských reťazcov.

Výstupy projektu budú sprístupňované v súlade s princípmi a politikou otvorenej vedy. Akademickí pracovníci SAV budú vykonávať svoju činnosť v zmysle dokumentu „Politika otvorenej vedy v Slovenskej akadémii vied“. Pracovníci spadajúci pod NBÚ budú pri tvorbe softvéru pracovať vo verejne prístupných repozitároch (napr. GitHub). Po ukončení projektu bude na webovej stránke NBÚ zverejnený článok o výstupoch projektu ktorý bude obsahovať odkazy na stiahnutie finálnych verzií inštalačných súborov, obrazov disku, zdrojových kódov, prípadne iných relevantných výstupov.

Projekt zahŕňa konkrétne výskumné úlohy v oblasti výskumu post-kvantovej kryptografie a aplikovaného výskumu (výskum efektívnych implementácií algoritmov, metód manažmentu kľúčov) a podporné aktivity VaV (vytvorenie výskumnej infraštruktúry, vývoj metodík hodnotenia bezpečnosti). Matematický ústav SAV disponuje potrebnou expertízou v oblasti matematických princípov šifrových algoritmov, čo je nevyhnutným predpokladom pre úspešnú realizáciu výskumných aktivít a aplikáciu ich výsledkov do praxe.

V rámci prípravy projektu bola dôkladne zvážená alternatíva riešiť výskum na medzinárodnej úrovni prostredníctvom spoločného výskumu s okolitými štátmi alebo na úrovni EÚ. Táto možnosť bola analyzovaná z hľadiska ekonomickej efektívnosti aj výskumného potenciálu. Dospeli sme k záveru, že národný projekt predstavuje optimálne riešenie z nasledujúcich dôvodov:

- špecifické potreby SR v oblasti kybernetickej bezpečnosti vyžadujú riešenia prispôsobené našej infraštruktúre a legislatívnemu rámcu,
- existujúce medzinárodné iniciatívy v tejto oblasti sú často zamerané na všeobecnejšie aspekty post-kvantovej kryptografie, zatiaľ čo náš projekt sa zameriava na konkrétne implementácie,
- budovanie domácej expertízy v tejto strategickej oblasti je kľúčové pre dlhodobú kybernetickú suverenitu SR.

Napriek tomu projekt počíta s intenzívnou medzinárodnou spoluprácou formou zapojenia zahraničných expertov a zdieľania výsledkov, čím sa dosiahne synergia medzi národným prístupom a medzinárodnou expertízou. V prípade úspechu projektu plánujeme v budúcnosti iniciovať širšiu medzinárodnú spoluprácu na úrovni V4 alebo EÚ, kde by Slovensko mohlo prispieť už vybudovanou expertízou a konkrétnymi výsledkami.

3. Zdôvodnenie vylúčenia „súťažného postupu“ výberu projektu prostredníctvom výzvy

Zdôvodnite, prečo je vhodnejšie realizovať NP ako využitie „súťažného postupu“ prostredníctvom výzvy (napr. porovnanie oboch spôsobov realizácie projektu, efektívnejšie a hospodárnejšie využitie finančných prostriedkov, efektívnosť služby poskytovanej cieľovej skupine, zabezpečenie štandardov kvality a pod.).

Spolufinancovaný Európskou úniou

Problematika výskumu a vývoja v oblasti kvantovej kryptografie a bezpečnosti je vysoko komplexná a vyžaduje si koordináciu na národnej úrovni zo strany autority na to poverenej, najvhodnejším nástrojom na zabezpečenie stanovených cieľov v tejto oblasti je práve národný projekt. NBÚ má ako ústredný orgán štátnej správy zodpovedný za šifrovú službu a oblasť kybernetickej bezpečnosti všetky predpoklady na efektívne riadenie takéhoto projektu – disponuje odbornou autoritou, legislatívnymi nástrojmi a schopnosťou zabezpečiť spoluprácu s vedeckými inštitúciami. V spolupráci so Slovenskou akadémiou vied môže garantovať vysokú kvalitu výskumu, technickú objektivitu a dôsledné overovanie navrhnutých riešení. Navyše, štátne riadenie projektu zabezpečuje aj lepšiu pripravenosť na zapojenie výsledkov do budúcich právnych a technologických rámcov a minimalizuje riziko závislosti od externých subjektov, čo je pri kľúčových bezpečnostných technológiách zásadné. Táto nezávislosť je predpokladom technologickej suverenity, ktorá je v ére kvantovej výpočtovej revolúcie čoraz dôležitejším prvkom národnej stability a bezpečnosti.

Výskum post-kvantových šifrovacích algoritmov je strategickou prioritou, ktorá ovplyvňuje nie len hospodársky vývoj štátu, ale aj národnú bezpečnosť. Preto je dôležité, aby túto problematiku zastrešoval garant šifrovej služby, a to Národný bezpečnostný úrad. Tento projekt predstavuje dlhodobý proces vyžadujúci systematickú koordináciu, strategické plánovanie a rozhodovanie zohľadňujúce širší rámec národnej bezpečnosti. Zverenie jeho manažmentu inému (súkromnému) subjektu by mohlo viesť k tomu, že projekt bude riadený skôr podľa obchodných a krátkodobých cieľov než podľa dlhodobých strategických záujmov. Post-kvantová kryptografia sa totiž netýka len jedného produktu alebo riešenia, ale komplexnej transformácie bezpečnostnej infraštruktúry štátu, vrátane výmeny kľúčových algoritmov, štandardov a spôsobu správy dôvery.

Ďalej je potrebné uviesť, že uplatnením súťažného postupu by mohli dôjsť k situácii, že by nebolo možné nájsť subjekt, ktorý by projekt realizoval v takej forme a kvalite, ako je požadované, nakoľko v Slovenskej republike sa momentálne nachádza veľmi málo subjektov, ktoré sa venujú danej problematike a to len v rovine riešenia parciálnych problémov.

4. Uplatnenie princípu partnerstva pri príprave zámeru národného projektu

V prípade uplatnenia princípu partnerstva pri príprave zámeru NP[10] podľa článku 8 NSU, uveďte v tejto časti informáciu o partneroch, ktorí sa na jeho príprave podieľali.

Za partnerov zapojených do prípravy zámeru národného projektu sa považujú:

- *regionálne, miestne, mestské a ostatné orgány verejnej správy;*
- *hospodárskych a sociálnych partnerov;*
- *subjekty, ktoré zastupujú občiansku spoločnosť;*
- *v náležitom prípade výskumné organizácie a univerzity.*

Ak nezapojíte do prípravy zámeru NP niektorého z partnerov podľa článku 8 nariadenia o spoločných ustanoveniach[11], zdôvodnite ich nezapojenie. V prípade, ak ste princíp partnerstva pri príprave zámeru NP uplatnili, uveďte informáciu zapojení v tejto časti.

Do projektu bude priamo ako partner zapojený Matematický ústav Slovenskej akadémie vied, v. v. i.

[10] Zapojenie, resp. nezapojenie partnera ako je definovaný v § 3, písm. t) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov do implementácie projektu nie je predmetom vypĺňania tejto časti zámeru NP.

[11] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1060 z 24. júna 2021, ktorým sa stanovujú spoločné ustanovenia (ďalej len „NSU“).

Spolufinancovaný Európskou úniou

Slovenská akadémia vied (SAV) predstavuje jedinečného partnera pre výskum a vývoj post-kvantovej kryptografie v Slovenskej republike predovšetkým vďaka svojej dlhodobej odbornej tradícii, interdisciplinárnej výskumnej základni a preukázaným výsledkom v oblasti kvantových technológií a teoretickej informatiky. Na rozdiel od iných výskumných inštitúcií má SAV priame zastúpenie v relevantných európskych iniciatívach, ako sú projekty EuroQCI, EuroHPC a EPIQ, a prostredníctvom Inštitútu pre výskum kvantových technológií (QUTE) už dnes systematicky buduje infraštruktúru na vývoj kvantovo odolných komunikačných sietí a algoritmov. Vzhľadom na prepojenie medzi kvantovou fyzikou, kryptografiou a informačnou bezpečnosťou je výskum PQC typicky vysoko špecializovaný, čo si vyžaduje špičkový vedecký potenciál, aký SAV ako jediná slovenská inštitúcia v tejto oblasti sústavne rozvíja.

Zároveň, na rozdiel od univerzít a komerčných subjektov, má SAV schopnosť vykonávať dlhodobý aplikovaný výskum bez tlaku na okamžitú komercializáciu, čo je kľúčové pre technológie s vysokým nárokom na bezpečnosť, štandardizáciu a dôkaznú overiteľnosť. Kombinácia akademickej integrity, prístupu k medzinárodným výskumným sieťam a skúseností so zabezpečovaním technických riešení robí zo SAV ideálneho partnera Národného bezpečnostného úradu pri budovaní post-kvantovo bezpečnej infraštruktúry Slovenska. V synergii s NBÚ môže SAV zabezpečiť nielen výskumné zázemie, ale aj technologickú validáciu a prípravu odporúčaní pre legislatívne a technické štandardy, čím Slovensko môže okrem iného napĺňať svoje záväzky v rámci európskych plánov kybernetickej a kvantovej bezpečnosti.

Popis národného projektu

5. Východiskový stav

a. Uveďte východiskové dokumenty na regionálnej, národnej a európskej úrovni, ktoré priamo súvisia s realizáciou NP:

- *Odporúčanie Európskej komisie C(2024) 2393 z 11.4.2024 o Pláne koordinovaného vykonávania prechodu na post-kvantovú kryptografiu* - odporúčanie sa zaoberá potrebou koordinovaného prístupu k prechodu Európy na kvantovo bezpečnú digitálnu infraštruktúru. Pomôže členským štátom vypracovať konzistentnú stratégiu pri prechode na bezpečnejšie spôsoby ochrany svojich digitálnych infraštruktúr.

- *Správa Európskej agentúry pre kybernetickú bezpečnosť (ENISA) o post-kvantovej kryptografii na medzinárodnej úrovni* - štúdia poskytuje prehľad aktuálneho stavu procesu štandardizácie post-kvantovej kryptografie. Predstavuje 5 hlavných skupín algoritmov PQ, a to algoritmy založené na kóde, genetické algoritmy, hešové algoritmy, mriežkové algoritmy a viacrozmerné algoritmy. Opisuje tiež finalistov 3. kola NIST pre šifrovacie a podpisové schémy, ako aj alternatívne kandidátske schémy.

- *BSI a NIS Cooperation Group – „Transitioning to Post-Quantum Cryptography" (2024)* - Spoločné stanovisko nemeckého federálneho úradu BSI a európskych národných bezpečnostných agentúr (napr. Francúzsko, Nizozemsko, Švédsko), ktoré odporúča základné fázy migrácie, nastavenie riskovej analýzy, hybridné fázovanie („store now, decrypt later") a deadline pre magistrálne systémy do konca roku 2030.

- *EU PQC Workstream Roadmap (sympózium december 2024)* - Výstup pracovnej skupiny členských štátov (Nemecko, Francúzsko, Holandsko a ďalšie), ENISA, EÚ

Komisie a priemyslu, ktorá načrtla dokument „Concept Paper“ ku koordinovanému postupu pre PQC s cieľom zverejniť ju do roku 2027.

- *EPC: A Quantum Cybersecurity Agenda for Europe (2023)* - Strategický dokument think-tanku European Policy Centre, ktorý popisuje PQC ako prioritu európskej suverenity a odporúča prioritu vývoja a kompatibility s QKD a národnými politikami, pričom PQC je vnímaná ako aktuálna a praktická cesta k odolnosti.

- *Vyjadrenia ANSSI, BSI a ETSI (2022-2023)* **-** Francúzska ANSSI, nemecké BSI a ETSI zverejnili pozície a technickú podporu na hybridné nasadenie PQC a na kombináciu s QKD, pričom zdôraznili význam existujúcich a pokrytých riešení a okamžitého nasadenia pre citlivé systémy.

- *Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde C 286/76 z 16.7.2021* – dokument popisujúci stratégie EÚ v oblasti kybernetickej bezpečnosti a v podmienkach rastúcich kybernetických hrozieb. V stratégii sa zdôrazňuje potreba spoľahlivých opatrení kybernetickej bezpečnosti v kritických odvetviach, ako sú energetika, zdravotníctvo a financie.

- *Legislatíva SR na úrovni ústredného orgánu štátnej správy* – jedná sa najmä o Zákon 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a Zákon 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

- *Stratégia rozvoja Národného bezpečnostného úradu v rokoch 2019- 2026* – dokument popisujúci okrem iného aj zámery Národného bezpečnostného úradu rozširovať spôsobilosti a reagovať na trendy vývoja v bezpečnostnom prostredí a implementovať poznatky z aplikačnej praxe.

- *Národná stratégia a akčný plán kybernetickej bezpečnosti* – prijatá uznesením vlády Slovenskej republiky č. 5/2021, ide o východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Na základe jasných princípov určuje strategické ciele a má ambíciu moderným spôsobom reagovať na aktuálne a perspektívne bezpečnostné hrozby.

b. Uveďte predchádzajúce výstupy z dostupných analýz, na ktoré nadväzuje navrhovaný zámer NP (štatistiky, analýzy, štúdie,...):

- *Secure Implementation of Post-Quantum Cryptography – projekt NATO* – tento projekt navrhuje, analyzuje a implementuje kryptografický protokol na bezpečnú skupinovú komunikáciu v distribuovaných hybridných sieťach, ktorý integruje post-kvantovú kryptografiu a kvantovú distribúciu kľúčov, ktoré sú k dispozícii v infraštruktúre distribuovanej siete. Explicitne sa zaoberá kritickou úlohou správy kľúčov a školením mladých vedcov v rámci výskumných komunít post-kvantovej kryptografie a kvantovej výmeny kľúčov.

- *NIST Post-Quantum Cryptography StandardizationSecure* – V roku 2023 Národný inštitút pre štandardy a technológie (NIST) vybral po šiestich rokoch a viacerých kolách medzinárodných súťaží štyri šifrovacie algoritmy ktorých návrh bol zameraný tak, aby odolali útokom kryptograficky relevantných kvantových počítačov. NIST teraz začal s procesom štandardizácie aby bolo možné plnohodnotné sprístupnenie týchto algoritmov pre organizácie na celom svete. Ide o CRYSTALS-Kyber FIPS 203, CRYSTALS-Dilithium FIPS 204, SPHINCS+ FIPS 205 a FALCON FIPS 206.

c. Popíšte problémové a prioritné oblasti, ktoré rieši zámer NP. (Zoznam známych problémov, ktoré vyplývajú zo súčasného stavu a je potrebné ich riešiť):

- **Národná bezpečnosť:** Post-kvantová kryptografia predstavuje nevyhnutný základ pre ochranu národnej bezpečnosti v kybernetickom priestore. Kvantové počítače môžu v horizonte niekoľkých rokov narušiť klasické kryptografické mechanizmy používané nie len na ochranu dôverných informácií a komunikačných kanálov, ale aj bežných údajov občanov či firiem. Projekt bude priamo podporovať budovanie post-kvantovo odolnej bezpečnostnej architektúry štátnych inštitúcií, vrátane obrany, diplomacie a bezpečnostných zložiek, čím sa znižuje riziko kybernetickej špionáže, sabotáže alebo kompromitácie kritických systémov.
- **Informačná a kybernetická bezpečnosť:** projekt sa primárne zameriava na vývoj v oblasti asymetrickej kryptografie ktorá sa používa na výmenu šifrovacích kľúčov a dôveryhodné podpisy. Vývojom nového a bezpečného spôsobu distribúcie a výmeny šifrovacích kľúčov sa výrazne znižujú viaceré riziká pre asymetrickú kryptografiu a zároveň sa zachová možnosť využitia aktuálne používaných symetrických algoritmov. Projekt priamo podporuje zvyšovanie odolnosti spoločnosti v širokom meradle, vrátane podnikateľského prostredia, priemyslu a kritickej infraštruktúry.
- **Dlhodobá ochrana a dôvernosť dát:** Útočníci dnes môžu zaznamenávať šifrované dáta a v budúcnosti ich spätne dešifrovať pomocou kvantových technológií (tzv. „harvest now, decrypt later“ stratégia). Projekt rieši potrebu ochrany celého radu údajov, vrátane tých citlivých, ako sú zdravotné záznamy, osobné údaje, duševné vlastníctvo a strategické dokumenty, ktoré musia zostať dôverné desiatky rokov. Implementácia PQC je kľúčom k zabezpečeniu tejto dlhodobej dôvernosti.
- **Kryptografická agilita:** Súčasné systémy často používajú pevne zabudované algoritmy, ktoré sa ťažko menia. V prípade prelomenia klasickej kryptografie by takýto systém zostal zraniteľný. Projekt pomáha vytvoriť riešenia umožňujúce flexibilnú a rýchlu výmenu kryptografických algoritmov – čo je nevyhnutné na prechod k novým štandardom, ako aj na priebežné reagovanie na nové hrozby.
- **Kompatibilita:** Pre úspešné nasadenie musí byť PQC integrovaná do existujúcich bezpečnostných protokolov, ako TLS (internetová bezpečnosť), VPN, digitálne podpisy či e-mailová komunikácia. Projekt umožní návrh riešení, ktoré budú kompatibilné s existujúcou infraštruktúrou, čo zníži náklady na migráciu a zabezpečí interoperabilitu medzi systémami v rôznych fázach prechodu na PQC.
- **Budovanie expertízy a vzdelávacej základne:** Slovensko má obmedzený počet špecialistov na kryptografiu, kvantové technológie a kybernetickú bezpečnosť. Projekt bude aktívne podporovať vzdelávanie a odborný rozvoj v týchto kľúčových oblastiach. Výstupy projektu budú zahŕňať odborné publikácie a podporu výskumu, čím sa zabezpečí udržateľná vedecká a technická kapacita do budúcnosti.

- **Medzinárodná spolupráca a technologická suverenita:** Projekt má potenciál prispieť k nezávislosti Slovenska a EÚ v oblasti kybernetickej bezpečnosti a šifrovej ochrany. Súčasne sa podporí tvorba domácich technológií a riešení, čím sa zníži závislosť od mimoeurópskych dodávateľov, čo je kľúčové z pohľadu bezpečnostných záujmov EÚ aj jednotlivých členských štátov.
- **Inovačný, ekonomický a trhový potenciál:** Post-kvantová kryptografia predstavuje budúci priemyselný štandard v oblastiach ako bankovníctvo, zdravotníctvo, obrana, digitálne technológie či moderný priemysel. Projekt má potenciál vytvárať inovácie, ktoré budú komerčne využiteľné. Výstupy projektu budú viesť k tvorbe produktov vhodných na export, čím sa podporí konkurencieschopnosť slovenského high-tech sektora a vznik nových pracovných miest.

d. Uveďte, na ktoré z ukončených a prebiehajúcich národných projektov[12] zámer NP priamo nadväzuje, v čom je navrhovaný NP od nich odlišný, resp. na ktoré NP čiastočne nadväzuje / prelína sa s nimi v istej časti a ako sú v ňom zohľadnené (čiastkové) výsledky/dopady predchádzajúcich NP (ak je to relevantné)
Projekt čiastočne nadväzuje na projekt APVV 19-0220-Ontologická reprezentácia pre bezpečnosť informačných systémov riešený na Matematickom ústave SAV (2022-2024) v spolupráci s FGEI STU, FMFI UK a ÚI SAV. Ďalej riaditeľ MÚ SAV a riešiteľ tohto projektu koordinoval sériu post-kvantových projektov v NATO ISEG s priamym dozorovaním projektov (SK+US+Spain+Malta+Finland, 2016-2025). Jeden z týchto projektov bol vyhlásený za najlepší projekt NATO desaťročia v oblasti kybernetickej bezpečnosti.
V centrále NATO v Bruseli spoluorganizoval dve vedecké konferencie so zameraním na post-kvantové technológie a riadil Výzvu NATO pre kybernetickú bezpečnosť.

e. Popíšte administratívnu, finančnú a prevádzkovú kapacitu žiadateľa a partnera (v prípade, ak je v projekte zapojený aj partner):

Národný bezpečnostný úrad (NBÚ) disponuje nielen odborným a personálnym zázemím, ale aj dostatočnou administratívnou a finančnou kapacitou na zvládnutie náročných výskumných a inovačných projektov. Vo svojej organizačnej štruktúre má vyčlenený špecializovaný Odbor projektového a finančného riadenia, ktorý je systematicky zameraný na správu komplexných projektov z domáceho i zahraničného financovania. Tento odbor má preukázateľnú prax s úspešnou realizáciou viacerých národných projektov financovaných z európskych štrukturálnych a investičných fondov, ako aj skúsenosť so zapojením do medzinárodných aktivít v oblasti kybernetickej bezpečnosti. NBÚ ako ústredný orgán štátnej správy garantuje transparentnosť, bezpečnostnú dôveryhodnosť a schopnosť zabezpečiť projektovo-finančné riadenie na úrovni požiadaviek grantových schém EÚ, vrátane prísnych pravidiel auditu a kontroly.

Matematický ústav Slovenskej akadémie vied (MÚ SAV) patrí dlhodobo medzi vedecko-výskumné pracoviská s vysokou mierou medzinárodnej projektovej aktivity. Disponuje vlastným technicko-hospodárskym úsekom, ktorý zabezpečuje kompletnú administratívnu a ekonomickú podporu projektov financovaných z domácich aj zahraničných grantových mechanizmov, vrátane programov ako Horizon Europe, COST či Visegrad Fund. Výskumníci ústavu sa pravidelne zapájajú do výskumných konzorcií na európskej úrovni a majú skúsenosti

[12] V prípade, ak je to relevantné, uveďte aj ukončené národné projekty z programového obdobia 2014 – 2020.

nielen ako riešitelia, ale aj ako koordinátori náročných interdisciplinárnych projektov. V oblasti kryptografie a matematickej analýzy majú odborníci z MÚ SAV vybudované stabilné siete spolupráce s poprednými akademickými a výskumnými inštitúciami v EÚ, čo výrazne zvyšuje schopnosť ústavu plniť aj tie najambicióznejšie projektové ciele.

6. Hlavné ciele NP (stručne):

V tejto časti popíšte očakávané ciele a očakávané výstupy / výsledky projektu. Popíšte prínos projektu pre napĺňanie cieľov a výsledkov príslušnej priority / špecifického cieľa / opatrenia Programu Slovensko, ako aj súvisiacich strategických dokumentov na národnej úrovni (ak je to relevantné).

Cieľom projektu je uskutočniť hlboký výskum a vývoj post-kvantových šifrovacích algoritmov, ktoré budú schopné odolávať útokom potenciálnych kvantových počítačov. Tento výskum sa zameria na analýzu, výber a optimalizáciu algoritmov schválených v rámci medzinárodných štandardizačných procesov, pričom dôraz sa bude klásť na ich bezpečnostné vlastnosti, výpočtovú efektivitu a vhodnosť pre rôzne typy komunikačných a dátových scenárov. Súčasťou vývoja bude aj adaptácia týchto algoritmov do konkrétneho systémového prostredia, ako aj tvorba referenčných implementácií, ktoré zohľadnia nároky na výkon, pamäťovú stopu a kompatibilitu s existujúcou infraštruktúrou informačnej bezpečnosti.

Na tieto algoritmy nadväzuje praktická úloha – ich integrácia do riešenia zabezpečenej pracovnej stanice, ktorá bude predstavovať komplexnú platformu pre bezpečnú komunikáciu, spracovanie a uchovávanie dát. Okrem samotnej šifrovacej vrstvy bude projekt klásť dôraz na bezpečný a post-kvantovo odolný manažment kryptografických kľúčov, vrátane ich generovania, distribúcie, rotácie a archivácie. Cieľom je vytvoriť funkčné, testované a modulárne riešenie, ktoré bude schopné nasadenia v prostredí s vysokými bezpečnostnými nárokmi – napríklad v štátnej správe, obranných zložkách alebo kritickej infraštruktúre. Výsledkom bude produkt, ktorý preukáže nielen technologickú životaschopnosť, ale zároveň položí základ pre ďalší rozvoj a nasadzovanie kvantovo odolných systémov v slovenskej a európskej kybernetickej infraštruktúre.

7. Merateľné ukazovatele NP a iné údaje

V tabuľke nižšie uveďte merateľné ukazovatele projektu a iné údaje. Poskytovateľ v spolupráci so žiadateľom uvádzajú povinne minimálne jeden merateľný ukazovateľ projektu – výstup a minimálne jeden merateľný ukazovateľ projektu - výsledok[13].
Merateľné ukazovatele projektu musia byť definované tak, aby odrážali výstupy/výsledky projektu a predstavovali kvantifikáciu toho, čo sa realizáciou aktivít za požadované výdavky dosiahne[14].

[13] Povinnosť uvádzať minimálne jeden merateľný ukazovateľ výsledku neplatí pre nasledovné výnimky:
- projekty technickej pomoci (okrem aktivít technickej pomoci zameraných na financovanie informačných systémov, Centrálneho plánu vzdelávania, vzdelávania administratívnych kapacít a materiálovo-technického zabezpečenia),
- projekty návratnej finančnej pomoci,
- projekty v rámci, ktorých je cieľová skupina:
  a) totožná s účastníkmi projektu,
  b) bude monitorovaná prostredníctvom spoločných merateľných ukazovateľov programu – výsledku v súlade s prílohou I nariadenia EP a Rady (EÚ) 2021/1057 o ESF+ (karta účastníka) a súčasne platí jedna z dvoch nasledujúcich pod podmienok: projekty sú financované z ESF+, alebo projekty sú financované FST v súlade s čl. 8 písm. k) až m) nariadenia EP a Rady (EÚ) 2021/1056 o FST.
- typy akcií, pre ktoré neboli stanovené výsledkové merateľné ukazovatele programu a pre ktoré nie je zmysluplné stanovovať kvantifikované výsledky t. j. merateľné ukazovatele projektu. Popis cieľa projektu predstavujúci výsledok. Ide napríklad o intervencie zamerané na obstaranie štúdií alebo projektovej dokumentácie a pod. Riadiaci orgán pre Program Slovensko osobitne posudzuje potenciál zámeru národného projektu generovať kvantifikovateľné výsledky v podobe merateľných ukazovateľov projektu, ktorých definovanie je preferované.

[14] V odôvodnených prípadoch sa uvedená tabuľka nevypĺňa, pričom je nevyhnutné do tejto časti uviesť podrobné a jasné zdôvodnenie, prečo nie je možné uviesť požadované údaje.

Zoznam merateľných ukazovateľov projektu

Typ merateľného ukazovateľa projektu	Kód merateľného ukazovateľa projektu[15]	Názov merateľného ukazovateľa projektu	Merná jednotka merateľného ukazovateľa projektu	Indikatívna cieľová hodnota[16]
výstup	PO005	Počet zavedených a zlepšených služieb, nástrojov a aplikácií	počet	6
výsledok	PR016	Publikácie z podporovaných projektov	publikácie	3 (2+1)

Výstupmi projektu PO005 v počte 6 budú samotné softvérové riešenia a knižnice zabezpečenej pracovnej stanice: upravený podkladový operačný systém, VPN klient, VoIP klient, softvér celodiskového šifrovania / alebo šifrovania súborov v kontajneroch, ďalším výstupom bude celková integrácia všetkých služieb do jedného funkčného celku a softvérová verzia verzia Key Management centra pre generovanie a distribúciu dôveryhodného šifrového materiálu. Súčasne so softvérovým budú súčasťou výstupov aj dokumenty popisujúce spôsob použitia. Dokumentácia bude zameraná najmä na popis správneho postupu pri implementácii a nasadzovaní výsledkov projektu – návody a postupy pre správcov a užívateľov, bezpečnostné mechanizmy a kritické bezpečnostné nastavenia ktoré sú nevyhnutné pre správnu funkcionalitu softvéru a jeho bezpečnú prevádzku. Všetka dokumentácia bude verejne prístupná a bude slúžiť na podporu ďalšieho využitia výsledkov projektu či už priamo v informačných systémoch, alebo ako podklad pri modifikácii výsledkov a ich implementácie do iných riešení komerčných subjektov. Časť dokumentácie bude zameraná primárne na technické odporúčania pre implementáciu výsledkov projektu pre rôzne prípady použitia. Okrem dokumentov popisujúcich funkcie a správne postupy použitia výstupov projektu budú pre bezpečnostne kritické výstupy pripravené aj dokumenty ktoré sa budú venovať zdôvodneniam a zámerom riešiteľov popisujúcich voľby parametrov a implementačných metód – táto úroveň dokumentácie je určená pre kryptografické algoritmy.

NBÚ vytvorí pracovnú skupinu ktorej účelom bude okrem efektívnejšieho sprístupnenia výsledkov projektu aj hľadanie nových spôsobov ich použitia a integrácie. Do pracovnej skupiny budú prizvaní aj predstavitelia záujmových združení právnických osôb ako napr. IT asociácia Slovenska, Asociácia kybernetickej bezpečnosti, Asociácia kritickej infraštruktúry Slovenskej republiky a podobne. Cieľom pracovnej skupiny bude informovať verejný a súkromný sektor o postupe projektu, jeho smerovaní a čiastkových výstupoch aby sa uľahčil prenos výstupov do spoločnosti. Jedným z cieľov pracovnej skupiny bude v neposlednom rade aj hľadanie spôsobov financovania ďalších etáp projektu, ktoré budú nadväzovať a stavať na výstupoch z tejto prvej fázy.

Výstupy projektu budú sprístupňované v súlade s princípmi otvorenej vedy (Open science). Publikácie budú zverejnené v režime otvoreného prístupu (Open Access) v relevantných vedeckých časopisoch a na repozitároch podobných arXiv.org. Dátové súbory vytvorené počas projektu budú uložené vo verejne dostupných dátových repozitároch (napr. Zenodo, Open Science Framework) s pridelenými DOI identifikátormi. Softvérové knižnice a implementácie algoritmov budú zverejnené na platforme GitHub pod vhodnou open-source licenciou (napr. MIT, Apache 2.0), ktorá umožní ich ďalšie využitie a rozvoj výskumnou komunitou, pri zachovaní bezpečnostných štandardov. Všetky výstupy budú obsahovať informáciu o zdroji financovania a budú prepojené s projektovým webovým sídlom, kde budú dostupné komplexné informácie o projekte a jeho výsledkoch.

[15] Uvádza sa kód merateľného ukazovateľa projektu, nie kód spoločného, resp. špecifického merateľného ukazovateľa programu. Ak merateľný ukazovateľ projektu ešte nemá pridelený kód, uvádza sa „n/a“.

[16] V zmysle zmluvy o poskytnutí nenávratného finančného príspevku sa pre typ merateľného ukazovateľa projektu – výstup štandardne cieľová hodnota nastavuje ku koncu realizácie národného projektu. Pre typ merateľného ukazovateľa projektu – výsledok sa štandardne cieľová hodnota nastavuje na obdobie udržateľnosti národného projektu.

Zoznam iných údajov projektu (ak relevantné)

Kód iného údaja[17]	Názov iného údaja	Merná jednotka iného údaja
DPSK033	Počet nástrojov zabezpečujúcich prístupnosť pre osoby so zdravotným postihnutím	počet
DPSK034	Priemerná hrubá mesačná mzda financovaná z projektu za rok	Eur/rok
DPSK035	Medián priemerných hrubých mesačných miezd financovaných z projektu za rok	Eur/rok

8. Prínosy, ktoré sa dajú očakávať pre cieľové skupiny (ak je to relevantné)

Cieľová skupina	Počet[18]	Prínos
subjekty verejnej správy a nimi zriadené subjekty, vrátane subjektov územnej samosprávy; sektor výskumných organizácií; vedecko-výskumní a vývojoví zamestnanci; akademický sektor; podnikateľský sektor;	Nie je možné špecifikovať presný počet, keďže výstupy a dáta budú otvorenými dátami dostupnými pre všetky verejnej, akademickej a súkromnej sféry	Prínosom pre všetky uvedené cieľové skupiny bude voľne prístupné riešenie pre zabezpečenú komunikáciu a šifrovú ochranu údajov. Žiadny z prvkov zabezpečenej pracovnej stanice nebude licencovaný a všetky výstupy výskumu, vývoja a praktickej aplikácie budú zverejňované v súlade so zásadami otvorenej vedy. Verejný sektor tak môže ponúkané riešenie nasadiť v rámci svojej IT infraštruktúry kde je dôležitá kybernetická bezpečnosť a ochrana údajov. Súkromný sektor bude mať možnosť použiť kryptografické knižnice, alebo časti softvéru vo svojich produktoch, alebo na nich stavať svoje vlastné riešenia.

9. Aktivity národného projektu

a. V tabuľke nižšie uveďte rámcový popis aktivít, ktoré budú v rámci identifikovaného národného projektu realizované.

Názov aktivity	Čo sa má aktivitou dosiahnuť	Spôsob realizácie (žiadateľ a / alebo partner)	Predpokladaný počet mesiacov realizácie aktivity
Matematická podpora kvantových technológií	Výskum post-kvantových algoritmov a protokolov	MÚ SAV NBÚ	1-48
Matematické princípy post-kvantových šifrových algoritmov	Odporúčania pre komunikáciu so zameraním na post-kvantové komunikačné algoritmy	MÚ SAV NBÚ	1-48
Vývoj a vytvorenie prototypu zabezpečenej pracovnej stanice	Vývoj zabezpečeného OS, VPN klienta, VoIP klienta, celodiskového šifrovania alebo šifrovania súborov v	NBU	1-48

[17] Ak iný údaj ešte nemá pridelený kód, uvádza sa „n/a“.
[18] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

	kontajneroch		
Vytvorenie Key Management centra pre generovanie a distribúciu dôveryhodného šifrového materiálu	Navrhnúť nové KMC s implementovanými post-kvantovými algoritmami	NBU	1-48

V prípade viacerých aktivít, doplňte informácie za každú z nich.

b. V tabuľke nižšie uveďte, či v rámci národného projektu bude uplatnený inštitút užívateľa[19] podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Názov aktivity	Využitie inštitútu užívateľa (áno/nie)	Typ užívateľa[20]	Poskytovateľ príspevku užívateľovi (žiadateľ alebo partner)
Matematická podpora kvantových technológií	Nie		
Matematické princípy post-kvantových šifrových algoritmov	Nie		
Vývoj a vytvorenie prototypu zabezpečenej pracovnej stanice	Nie		
Vytvorenie Key Management centra pre generovanie a distribúciu dôveryhodného šifrového materiálu	nie		

V prípade viacerých aktivít, doplňte informácie za každú z nich.

c. Uveďte detailnejší popis aktivít.

Okrem detailnejšieho popisu každej oprávnenej hlavnej aktivity uveďte, ako je v projekte zabezpečené dodržiavanie horizontálnych princípov podľa čl. 9 nariadenia o spoločných ustanoveniach, ako aj podľa uznesenia vlády SR č. 668 z 26. októbra 2022.

Ak po schválení zámeru NP komisiou pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 dôjde k podstatnej zmene v rozsahu hlavných aktivít NP uvedených vyššie (t. j. minimálne jedna hlavná aktivita nebude v rámci NP realizovaná, resp. má dôjsť k výraznému zväčšeniu alebo zmenšeniu rozsahu schválených aktivít, príp. doplneniu novej aktivity), riadiaci orgán / sprostredkovateľský orgán predloží pred vyhlásením výzvy na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 upravený zámer NP. Z dôvodu zabezpečenia overenia dodržania vyššie uvedenej zásady poskytovateľ vo výzve na predkladanie žiadosti o nenávratný finančný príspevok v rámci relevantnej podmienky poskytnutia príspevku zadefinuje hlavné aktivity schváleného zámeru NP ako povinné hlavné aktivity projektu.

[19] Užívateľ sa na rozdiel od partnera nepodieľa na realizácii projektu žiadateľa, ale môže využiť finančný príspevok na realizáciu aktivít definovaných poskytovateľom vo výzve (napr. nákup a inštalácia kotla). Podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, užívateľom je osoba, ktorej prijímateľ alebo partner poskytuje finančné prostriedky z príspevku na základe predchádzajúceho súhlasu poskytovateľa a v súlade so zmluvou uzavretou medzi prijímateľom a užívateľom alebo partnerom a užívateľom alebo iným obdobným právnym vzťahom medzi prijímateľom a užívateľom alebo partnerom a užívateľom.

[20] Uvádza sa typ subjektu/osôb (napr. neverejní poskytovatelia soc. služieb, dlhodobí uchádzači o zamestnanie), alebo právna forma.

Analýza súčasnej situácie

Po položení základov kvantového sveta v 20. storočí, je v 21. storočí rozvoj kvantových technológií veľmi razantný. Po rozvoji reálnych kvantových počítačov sa začala črtať hrozba reálneho rozkladu veľkých čísel na prvočísla pomocou algoritmu P. W. Shora. To by znamenalo zlomenie algoritmov typu RSA, DSA, ECDSA, na ktorých je postavených 95 % protokolov a šifrovacích primitívov dnešných počítačových a komunikačných technológií.

Aj keď ešte dnešné kvantové počítače nedosahujú svojimi parametrami tento prah ich pokrok je veľmi rýchly. Dnešné kvantové procesory firiem Google a IBM majú niečo vyše 100 logických qubitov. Na jeden logický qubit je potrebných 8 až 10 fyzikálnych qubitov. Rozvoj je zameraný jednak na zvýšenie počtu fyzikálnych qubitov a jednak na zlepšenie pomeru fyzikálnych qubitov na jeden logický qubit. Konkrétne IBM predstavila 4. 12. 2023 procesory Condor (1121 qubitov), Heron (133 qubitov). Google zase Wilow (105 qubitov). Viac ako 200 bitové majú väčšiu chybovosť a nie sú použiteľné na výpočty.

Pre reálne zlomenie RSA je potrebný kvantový počítač s rádove oveľa viac qubitmi, ako máme teraz k dispozícii. Odhady sú, že kryptograficky relevantný kvantový počítač musí mať k dispozícii viac ako 10 tisíc nezašumených qubitov, alebo až 20 miliónov zašumených qubitov na úspešnú aplikáciu Shorovho algoritmu na zlomenie bežne používaných RSA kľúčov.

Napriek tomu sa musíme pripraviť jednak na situáciu, že to môže nastať a jednak na to, že je možný útok – odpočúvaj teraz, dešifruj neskôr (Harvest now, decrypt later). Pritom existujú tajomstvá, ktoré je potrebné chrániť dlhodobo, určite viac ako desaťročia. Napríklad aj úradné záznamy, alebo prísne tajné dokumenty.

Okrem kvantových počítačov má kvantová technológia aplikáciu na možnosť dohody o kľúči. Princípom je použitie spriahnutých fotónov, z ktorých jeden si nechá odosielateľ a jeden sa prenesie cez optické vlákno alebo satelit ku prijímateľovi. Predtým je potrebné mať dohodnutý spoločný kľúč.

Odpočúvanie optického vlákna nie je fyzikálne uskutočniteľné. Navyše stačí poslať jeden fotón a prerušenie prenosu mužom v strede je detekovateľné. Prvý prenos cez optický kábel realizovali prof. A. Zeilinger a prof. V. Bužek na hranici medzi Rakúskom a Slovenskom. Odvtedy vieme túto technológiu nasadiť rutinne do prevádzky. Prvý satelitný prenos sa uskutočnil v roku 2017 medzi Čínou a Rakúskom, pod vedením Prof. A. Zeilingera. A. Zelinger dostal v roku 2022 Nobelovu cenu za fyziku za svoj prínos ku kvantovým technológiám. Napriek tomu má táto technológia má niekoľko problematických bodov.

- Maximálna dĺžka cez optické vlákno prenosu je okolo 100-200 km. Potom je potrebné inštalovať opakovač/repeater. Bezpečnosť takýchto staníc je problematická.
- Pri prenose cez satelit je potrebné použiť laserový zväzok na zameranie a tiež na prenos so štatistickým vyhodnotením. Tu sú znovu bezpečnostné riziká.
- Vzhľadom na to, že pri kvantovom prenosovom kanáli, ktorý slúži na dohodu o kľúči, alebo distribúciu kľúčov, musí byť vopred dohodnutý kľúč je vlastne takáto technológia drahá, nie dokázateľne bezpečná a nie potrebná.

Napriek vyššie uvedenému veľké telefónne spoločnosti budujú siete pozemných staníc a siete satelitov na nízkych dráhach na takúto distribúciu kľúčov.

Z vyššie uvedeného vyplýva jednoznačný záver, že v zhode so závermi nemeckej BSI z roku 2023:

- Systémy musia byť migrované do kvantovo bezpečnej kryptografie tak rýchlo, ako je to možné.
- Algoritmy post-kvantovej kryptografie (Post Quantum Cryptography - PQC) pre dohodu o kľúči a podpisové algoritmy budú čoskoro štandardizované. Migrácia do PQC musí byť prioritou.
- Kvantová distribúcia kľúčov (Quantum Key Distribution - QKD) je vedecky zaujímavá, ale je vhodná iba pre obmedzený počet prípadov. Dokonca aj vtedy, QKD nie je dostatočne zrelá z hľadiska bezpečnostnej perspektívy.

Napriek poslednému záveru BSI mnohé komerčné firmy budú túto verziu ponúkať a budeme musieť riešiť bezpečnosť hybridných systémov.

Úlohy riešené na Matematickom ústave SAV, v. v. i. budú spadať do dvoch oblastí:

Matematická podpora kvantových a šifrovacích systémov

Strategickým cieľom tejto aktivity je prehlbovanie výsledkov v matematických metódach na podporu kvantových a post-kvantových technológií. Tým zabezpečiť existenciu vlastnej expertízy, podporiť rozvoj vlastného výskumu a zapojenie sa do európskych infraštruktúr v oblasti matematickej podpory kvantových a post-kvantových technológií. Je veľmi dôležité, aby sme vytvorili silný tím, ktorý je schopný porozumieť všetkým detailov problematiky. Tým, ktorý bude prehlbovať poznatky v tejto oblasti a nie iba preberať cudzie algoritmy a schémy bez vniknutia do problémov. Táto časť úlohy bude prebiehať do úrovne TRL 4 – laboratórne testovanie.

Už teraz disponujeme silným tímom, ktorý zaručuje dosiahnutie relevantných výsledkov. Túto bázu je potrebné rozvíjať, lebo pokrok v tejto oblasti je veľmi rýchly. Úlohou výskumníkov bude teda primárne naštudovanie si relevantných noriem v ktorých sú popísané princípy a matematické konštrukty. Následne bude potrebné zhodnotenie, ktoré z uvedených noriem sú najvhodnejšie pre potreby projektu s ohľadom na ich budúcu aplikáciu do zabezpečenej pracovnej stanice.

Po zvolení najefektívnejšej cesty sa začne hlavná úloha a to reálna tvorba kryptografických knižníc domácimi akademikmi z Matematického ústavu SAV a zahraničnými kontrahovanými vedeckými pracovníkmi. Počas trvania projektu sa zamerajú na implementáciu návrhov algoritmov do kryptografických knižníc. Táto časť úlohy je vedomostne najnáročnejšou časťou celého projektu. Vzhľadom na obmedzené domáce kapacity vedeckých pracovníkov schopných efektívne pracovať v oblasti post-kvantovej kryptografie bude nevyhnutné využiť zahraničné kapacity a kontakty Matematického ústavu SAV na zazmluvnenie zahraničných vedeckých pracovníkov s potrebnými skúsenosťami. V tejto fáze bude dôležité najmä správne zvolenie módov, parametrov kryptografických premenných a iných dôležitých parametrov za účelom zabezpečenia požadovanej úrovne bezpečnosti. Prioritné zameranie bude kladené na vytvorenie náhrady asymetrickej výmeny šifrovacích kľúčov. Navrhnuté knižnice budú musieť byť naviac dôsledne preskúmané voči nesprávnej implementácii - keďže pôjde o novovytvorené a nepreverené implementácie, bude potrebné zamerať sa aj na celý rad „klasických“ postranných útokov ako napríklad časové útoky, vyvolávanie chýb, neoprávnené zápisy/čítania a iné útoky zamerané na implementáciu dobre známe z dnes bežne nasadených kryptografických schém a algoritmov. Výsledkom tejto časti budú prvotné prototypy kryptografických knižníc spolu s odporúčanými metódami ich použitia.

Úloha je rozdelená do niekoľkých teoretických pod úloh vedených kľúčovými riešiteľmi. Výstupmi budú vedecké práce publikované v odborných a vedeckých časopisoch. Súčasťou úlohy sú aj nové typy post-kvantových algoritmov alebo protokolov, ktoré sa v období riešenia úlohy ukážu ako relevantné.

Matematické princípy post-kvantových šifrovacích algoritmov.

V tejto úlohe sa budeme venovať konkrétnemu rozpracovaniu šifrovacích procesov v našom prostredí.

Základné prístupy, ktoré boli akceptované vo verejnej súťaži NIST ako správne (v podobe konkrétnych algoritmov) sú založené na :

- metódach mrežových bodov (lattice based),
- sústav rovníc s veľa neznámymi,
- odtlačkových funkciách,
- samoopravných kódoch,
- izogénnych grafoch eliptických kriviek,
- a niektorých ďalších.

V úlohe budeme stále sledovať rozvoj týchto metód a vypracovávať prehľadné správy o situácii.

Zameriame na detailný popis pre implementáciu schém na vytvorenie kľúča alebo dohody o kľúči. Takáto dohoda o kľúči potom umožní vytvárať šifrovacie prostredie so symetrickým kľúčom, teda rýchlu a bezpečnú komunikáciu. Mnohé schémy takéhoto typu už boli publikované. Prvým štandardom, ktorý bol prijatý pre KEM – Key Encapsulation Mechanism je FIPS 203. Táto časť úlohy bude prebiehať na úrovni TRL 4 – laboratórne testovanie.

Výstupmi budú (podrobnejší popis je v rozpise na pod úlohy):

- Detailné popisy vybraných algoritmov.
- Odporúčania pre používanie šifrovacích metód.

- Školenia a prednášky pre vybraných poslucháčov.

Strategickým cieľom oboch aktivít je zabezpečiť existenciu vlastnej expertízy, podporiť rozvoj vlastného výskumu a zapojenie sa do európskych infraštruktúr v oblasti post-kvantovej bezpečnosti.

Tieto úlohy budeme riešiť v úzkej spolupráci s účasťou domácich, ale aj zahraničných expertov z akademického prostredia. Súčasne sa podieľame na systematickej výchove našich budúcich absolventov.

V nadväznosti na Odporúčania Európskej komisie a popis úlohy vyššie predpokladáme nasledujúci postup riešenia úlohy Pri riešení sa opierame o základné dokumenty uvedené v časti 5. a. Mnohé postupy boli rozpracované, široko posudzované medzinárodnou vedeckou komunitou v rámci projektu NIST Post-Quantum Cryptography (https://csrc.nist.gov/projects/post-quantum-cryptography) a sérii štandardov NISTu. V priebehu riešenia projektu predpokladáme vznik štandardov Európskej únie a nami navrhované postupy budú v súlade s týmito štandardami. Budeme riešiť nasledujúce pod úlohy:

1. ***Základné princípy, postupy post-kvantových algoritmov a protokolov.***

V tejto časti sa sústredíme na vedecký popis šifrovacích algoritmov a protokolov pre post-kvantovú kryptografiu. Popíšeme tie, ktoré sa zavádzajú do praxe a považujú sa za najvhodnejšie. Rovnako sem zaradíme aj algoritmy, ktoré vzniknú počas riešenia úlohy a budú považované za dôležité. To znamená, že stále budeme sledovať vedecký a praktický rozvoj v tejto oblasti a popisovať aj takéto výsledky.

Popis základných matematických postupov na riešenie úloh. Táto pod úloha má začiatok hneď po štarte projektu. Popisuje matematické základy nevyhnutné pre riešenie úlohy. Má tri etapy so samostatnými výstupmi.

Trvanie T01-T36

Výstupy:

Výstupmi budú správy obsahujúce popisy matematických metód, ktoré postupne pokryjú celú oblasť použitých metód. Úlohy a výstupy pre jednotlivé etapy, 1.1 až 1.3.

Etapa 1.1. Správa 1.1 v čase T12 bude zameraná na popis základných matematických postupov a pracovných oblastí. Sem patria konečné polia, ich konštrukcia a výpočty s príkladmi použitia v jednotlivých štandardoch. Sem patria aj výpočtové metódy ako sú rýchla aritmetika vrátane rýchlej Fourierovej transformácie v jej jednotlivých formách.

Etapa 1.2. Správa 1.2 v čase T24 bude zameraná na post-kvantové metódy založené na metódach teórie čísel. Sem patria aj mrežové body, algoritmy pre výpočty s mrežovými bodmi, LLL redukovaná báza, odtlačkové funkcie

Etapa 1.3. Správa 1.3 v čase T36 bude zameraná na post-kvantové metódy založené na metódach teórie čísel. Sem patria sústavy rovníc, SAT solvery, samoopravné kódy, izogénia eliptických kriviek a ďalšie metódy, ktoré sa v priebehu riešenia úlohy ukážu ako relevantné pre problematiku post-kvantových výpočtov.

2. ***Základné realizačné postupy post-kvantových algoritmov a protokolov.***

V tejto časti sa zameriame na konkrétnu realizáciu postupov v algoritmickej podobe. Budú v nej podrobne algoritmicky popísané niektoré metódy z pod úlohy 1 a základné algoritmy a protokoly pre post-kvantovú kryptografiu

Trvanie T06-T42

Výstupy.

Etapy. Výstupmi budú správy obsahujúce popisy niektorých algoritmov, ktoré budú výstupmi podúlohy 1 a algoritmy a protokoly. Úlohy a výstupy pre jednotlivé etapy, 2.1 až 2.3.

Etapa 2.1. Správa 2.1 v čase T18 bude zameraná na algoritmy popísané vo výstupe 1.1. Sem patria niektoré algoritmy pre konečné polia, rýchlu aritmetiku vrátane rýchlej Fourierovej transformácie v jej jednotlivých

formách. Ďalej bude zameraná na post-kvantové metódy a protokoly typu „Lattice-based“ založené na problémoch mrežových bodov. Sem patria algoriotmy, protokoly a štandardy ako CRYSTALS-Kyber a ML KEM, CRYSTALS-Dilithium a ML-DSA.

Etapa 2.2. Správa 2.2 v čase T24 bude zameraná na post-kvantové metódy založené na odtlačkových funkciách. Sem patria algoritmy a protokoly pre digitálne podpisové štandardy založené na odtlačkových funkciách, ako SPHINC a SLH-DSS.

Etapa 2.3. Správa 2.3 v čase T36 T bude zameraná na metódy založené na samoopravných kódoch. Tiež ďalšie metódy ako izogénia eliptických kriviek a ďalšie metódy, ktoré sa v priebehu riešenia úlohy ukážu ako relevantné pre problematiku post-kvantových výpočtov.

3. Tvorba informačných materiálov

V tejto časti budeme pre sprístupnenie problematiky vytvárať série prezentácií pre sprístupnenie problematiky pre pracovníkov štátnej správy, aby sme rozšírili informovanosť o vážnosti problematiky a priblížili prístupnejšou formou spôsoby riešenia.

Trvanie T12-T48

Vytvorenie Key Management Centra pre generovanie a distribúciu dôveryhodného šifrového materiálu

Každý systém s aplikovanou kryptografickou ochranou ktorý má za cieľ poskytovať reálnu úroveň bezpečnosti musí mať manažment šifrovacích kľúčov a definovaný spôsob ich tvorby, distribúcie a likvidácie. Všetky tieto úlohy sa v reálnom nasadení implementujú do tzv. "KMC - key management centra". Key Management Centrum (KMC) je najdôležitejšou časťou dôveryhodného kryptografického systému. Úlohou bude vytvoriť novú softvérovú implementáciu certifikačnej autority schopnej generovať kľúče použiteľné s novo implementovanými kryptografickými knižnicami. KMC bude musieť mať silný zdroj entropie – tu sa predpokladá použitie existujúceho zdroja entropie ktorý môže byť softvérový alebo aj hardvérový podľa požiadaviek danej aplikácie. Najväčšou výzvou v tejto úlohe bude riešenie bezpečnej distribúcie šifrovacích kľúčov a certifikátov, v prvej fáze bude postačovať aj manuálny prenos šifrového materiálu, ale v momente ako budú dostupné nové kryptografické knižnice bude potrebné prejsť na vzdialenú a automatizovanú distribúciu prostredníctvom zabezpečeného komunikačného kanála – napr. IPSsec tunelom. Prvotná inicializácia kryptografických zariadení bude v dohľadnej dobe musieť stále prebiehať manuálne, keďže zatiaľ ešte nie sú dostupné autentifikačné predmety (tokeny, smart karty) ktoré by podporovali nové algoritmy, avšak následná komunikácia po inicializácii už bude môcť byť automatizovaná. Ďalšou funkcionalitou KMC bude databáza vydaných šifrových kľúčov a certifikátov spolu s riadením ich životného cyklu –t.j. sledovanie doby platnosti a ich deaktivovanie v systéme v pri skončení ich životnosti ale kompromitácii. Aktuálne používané algoritmy na vzdialenú dohodu a výmenu šifrovacích kľúčov založené na asymetrickej kryptografii sú zraniteľné pri príchode kryptograficky relevantného kvantového počítača (Odporúčania ENISA https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation a BSI https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626). Je teda nevyhnutné navrhnúť nové KMC ktoré bude implementovať post-kvantové algoritmy za účelom zabezpečenia generovania a dôveryhodnej distribúcie šifrového materiálu užívateľom. KMC bude musieť implementovať nové kryptografické knižnice ktoré sa budú vyvíjať v prvej aktivite. V tejto fáze projektu sa bude realizovať najväčšia časť vývoja nových kryptografických knižníc, čomu zodpovedajú aj vyššie mzdové náklady na matematikov, kryptológov a bezpečnostných špecialistov z tuzemska a zahraničia ktoré predstavujú vyše 75% nákladov celej úlohy. Výsledkami tejto úlohy budú okrem softvérovej implementácie KMC aj technická dokumentácia popisujúca správnu implementáciu kryptografických knižníc zameraných najmä na problematiku asymetrickej kryptografie, dohode na šifrovacích kľúčoch a elektronického podpisu.

Vytvorenie prototypu zabezpečenej pracovnej stanice

Súbežne s tvorbou kryptografických knižníc bude prebiehať ďalšia fáza výskumnej aktivity a to príprava prvých verzií softvéru použiteľného pre bežné stolné počítače, notebooky a v istých prípadoch aj mobilné zariadenia s operačnými systémami iOS a Android za účelom umožnenia bezpečnej šifrovanej dátovej komunikácie. Tento

softvér bude zameraný na najbežnejšie prípady použitia prítomné vo väčšine IKT systémov a to najmä IPSEC protokol a VoIP protokol. Softvér bude vytváraný takým spôsobom, aby bolo možné v neskoršej fáze vývoja zmeniť kryptografické jadro/modul za nové knižnice bez nutnosti výrazných zmien v ostatných častiach kódu. Cieľom je implementácia novo vyvinutých kryptografických knižníc do softvéru a následné testovanie v laboratórnych podmienkach. Záverečná fáza testovania bude mať za cieľ preukázať splnenie požadovaných parametrov výsledného softvéru či už z pohľadu matematickej odolnosti, štatistických testov alebo implementačnej bezpečnosti. Vytvorenie prototypu zabezpečenej pracovnej stanice bude aplikovať vytvorené kryptografické knižnice v softvérovom prostredí pripravenom pre reálne nasadenie a skončí tak na úrovni TRL 8 – integrovaný pilotný systém preukázaný.

Logicky je tak možné rozdeliť návrh softvéru pre prototyp zabezpečenej pracovnej stanice do niekoľkých logických celkov: 1) návrh zabezpečeného operačného systému 2) návrh VPN klienta 3) návrh VoIP klienta 4) návrh celo-diskového šifrovania alebo šifrovania súborov v kontajneroch. Výhodou prístupu rozdelenia úlohy do niekoľkých samostatných celkov je hlavne flexibilita – jednotlivé časti ako VPN klient alebo zabezpečený operačný systém nebude nutné použiť len ako súčasť zabezpečenej pracovnej stanice, ale aj samostatne v iných produktoch, Na výstupoch tohto projektu tak môžu vznikať nové implementácie, ktoré môžu stavať na jednom alebo viacerých bezpečných prvkoch a doplniť k nim svoje riešenia pre ich konkrétne potreby.

1) Tvorba zabezpečeného operačného systému

Táto časť aktivity bude zameraná na prípravu podkladového operačného systému. Cieľom bude minimalistický a na bezpečnosť zameraný operačný systém použiteľný pre ľubovoľnú pracovnú stanicu. Postačovať bude jadro bez grafického prostredia iba s nevyhnutnými ovládačmi a virtualizačným prostredím, v ktorom sa ako virtuálne stanice budú spúšťať ostatné užívateľské operačné systémy. Návrh sa zameria aj na realizovateľnosť verzie na bootovateľnom médiu (USB kľúč, USB disk) pre maximálnu univerzálnosť. Ako najvhodnejší variant sa javí príprava zabezpečeného operačného systému postavenému na **Ubuntu 24.04 LTS** báze s vlastným desktop prostredím. Cieľom bude vyvinúť bezpečnú pracovnú stanicu, ktorá používateľovi po prihlásení poskytne možnosť výberu medzi spustením lokálneho virtuálneho stroja alebo pripojením ako thin client na vzdialenú infraštruktúru.

Základná architektúra

Systém bude postavený na **Ubuntu 24.04 LTS** s nasledovnými modifikáciami:

- **Hardened Ubuntu kernel** s vlastnými security patches
- **Custom desktop environment** s launcher/selection interface
- **Integrated hypervisor** (KVM/QEMU) pre lokálne VM
- **Thin client stack** pre remote VM pripojenia
- **Post-kvantová kryptografia** integrácia na systémovej úrovni

Podporované architektúry

- **x86_64** (primárna platforma)
- **ARM64** (AArch64) pre moderné workstation riešenia

Kľúčové komponenty

Custom Desktop Environment

Bezpečnostný launcher interface namiesto štandardného Ubuntu desktop:

- **Welcome screen** s používateľskou autentifikáciou
- **Service selection menu** - voľba medzi VM/Thin Client
- **Pre-defined VM templates** (Windows 10/11, Linux distributions, specialized systems)
- **Remote server discovery** a connection management
- **Security status dashboard** s real-time monitoring

- **Session management** s logout/shutdown options

Lokálna virtualizácia (KVM/QEMU integrácia)

- **One-click VM deployment** z pre-pripravených templates
- **Resource allocation management** (CPU, RAM, storage pre VM)
- **VM lifecycle management** (start, stop, pause, snapshot)
- **Shared folder access** medzi host a guest systémami
- **USB device passthrough** pre peripherals
- **Network isolation** pre VM security

Thin Client funkcionality

- **Server auto-discovery** cez LAN/WAN
- **Multiple protocol support** (RDP, VNC, SPICE, custom PQC protocol)
- **Session persistence** a reconnection handling
- **Bandwidth optimization** s adaptive quality settings
- **Local resource sharing** (USB, audio, clipboard)
- **Multi-monitor support** pre thin client sessions

Bezpečnostné komponenty

- **Post-kvantové kryptografické moduly**:
  - **Kyber** pre symmetric key exchange
  - **Dilithium** pre digital signatures
- **Full-disk encryption** s LUKS2 + PQC extensions
- **TPM 2.0 integration** pre hardware attestation
- **Secure boot chain** s custom signing certificates
- **Network security** s built-in firewall a traffic monitoring

Implementačné varianty
Variant A: Inštalovaný systém

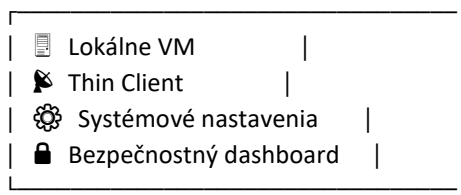
- **Persistent VM storage** s automatic backup scheduling
- **Template management** s version control a rollback
- **Enterprise integration** (Active Directory, LDAP support)
- **Remote management** capabilities pre IT administráciu
- **Automatic updates** s cryptographic verification

Variant B: Live bootovateľný systém

- **USB/DVD bootable** image (8GB target size)
- **RAM-based operation** s optional persistent storage
- **Universal hardware support** s broad driver coverage
- **Secure boot** s integrity verification
- **Emergency tools** pre system recovery a diagnostics

Používateľský workflow
1. Boot a prihlásenie
Ubuntu 24.04 štart → Custom login manager → Používateľská autentifikácia

2. Desktop launcher
Custom desktop interface s výberom:



3A. Lokálne VM workflow
Výber VM template → Resource allocation → VM štart → Full desktop experience
3B. Thin Client workflow
Server discovery → Protocol selection → Autentifikácia → Remote session

Bezpečnostné funkcionality

- **Measured boot** s TPM attestation
- **File system integrity** checking s dm-verity
- **Application signature verification** pre všetky spustené komponenty
- **Runtime security monitoring** s anomaly detection

Komunikačná bezpečnosť

- **VPN integration** s post-kvantovou kryptografiou
- **Network traffic encryption** pre všetky connections
- **Certificate management** s automatic PQC cert rotation
- **Zero-trust networking** principles

Výstup

Výsledkom bude **production-ready zabezpečený operačný systém** obsahujúci:

- **Ubuntu 24.04 ISO** s custom installer
- **VM template library** (Windows, Linux, specialized systems)
- **Management tools** pre system configuration
- **User documentation** pre operation a troubleshooting
- **Administrator guide** pre deployment a maintenance
- **Security audit tools** pre compliance verification
- **Source code package** s build system pre customization

Systém predstavuje **enterprise-grade secure workstation platform** kombinujúcu flexibility lokálnej virtualizácie s ekonomickými výhodami thin client infraštruktúry, zabezpečenú post-kvantovou kryptografiou.

2) Tvorba VPN klienta

Výsledkom tejto pod úlohy bude vytvorenie softvérového VPN klienta s postupným zavádzaním na platformy: Linux → Windows → macOS → Mobile. Primárnymi atribútmi má byť jednoduchosť a ľahkosť nasadenia a použitia – na klientskej strane pôjde o čisto softvérovú aplikáciu. Výhodou takéhoto prístupu bude univerzálnosť použitia, ktorá nebude viazaná na konkrétneho výrobcu alebo špecifický typ služieb na backende.

Postupné zavádzanie podporovaných operačných systémov

VPN klient bude navrhnutý ako multiplatformová aplikácia s postupným zavádzaním platformy:

- **Fáza 1**: Linux (Ubuntu 20.04+, CentOS 8+, Fedora 35+)
- **Fáza 2**: Windows (Windows 10, 11 a novšie)
- **Fáza 3**: macOS (macOS 11 Big Sur a novšie)
- **Fáza 4**: Mobile (Android 8.0 API level 26+, iOS 13+)

Podporované protokoly

VPN klient bude implementovať nasledovné protokoly s hybrid PQC/classical crypto prístupom:

- OpenVPN (s rozšírením pre post-kvantovú kryptografiu)
- WireGuard (modifikovaná verzia s PQC podporou)
- IPSec/IKEv2 (s post-kvantovými kryptografickými algoritmami)
- Vlastný protokol optimalizovaný pre post-kvantovú kryptografiu

Autorizácia a autentifikácia

Systém overenia identity bude podporovať viacero metód:

- Certifikátová autentifikácia (X.509 certifikáty s PQC podpismi)
- Používateľské meno a heslo s MFA (Multi-Factor Authentication)
- Tokeny (JWT s post-kvantovými podpismi)
- Biometrická autentifikácia (na mobilných zariadeniach)
- Smart karty a HSM (v prípade existencie kariet podporujúcich PQC algoritmy)

Post-kvantová kryptografia s hybrid prístupom

Vzhľadom na skutočnosť, že aktuálne používané VPN klienty majú výmenu kryptografických kľúčov založenú na algoritmoch, ktoré sú ohrozené v prípade príchodu kryptograficky relevantného kvantového počítača, bude implementovaný hybrid prístup kombinujúci klasické a post-kvantové algoritmy pre plynulý prechod.

Implementované PQC algoritmy:

- Kyber (key encapsulation)
- Dilithium (digitálne podpisy)
- SPHINCS+ (alternatívne digitálne podpisy)
- FALCON/BIKE (backup riešenie)

Implementácia

Návrh najprv analyzuje dostupné voľne šíriteľné a modifikovateľné riešenia a identifikuje to, ktoré bude najvhodnejšie na modifikáciu a implementáciu nových kryptografických knižníc. Budú vyhodnotené existujúce open source VPN riešenia ako OpenVPN, WireGuard, strongSwan a SoftEther VPN.

Výstup

Výsledkom tejto časti aktivity bude beta verzia softvérového VPN klienta podporujúca post-kvantovú kryptografiu, vrátane:

- Inštalačných balíkov pre podporované platformy (postupne)
- Konfiguračných nástrojov
- Dokumentácie pre správcov a používateľov
- Testovacích scenárov a benchmarkov výkonu

3) Tvorba VoIP klienta

Výsledkom tejto časti aktivity bude vytvorenie bezpečnej komunikačnej aplikácie založenej na modifikácii Signal/Matrix protokolu s postupným zavádzaním PQC. Aplikácia kombinuje textové správy, hlasové a video hovory s pokročilým end-to-end šifrovaním. Aplikácia bude navrhnutá s dôrazom na súkromie a bezpečnosť používateľov.

Podporované operačné systémy

- Windows 10/11 (64-bit)
- Linux (Ubuntu 20.04+, CentOS 8+, Debian 11+)
- macOS 11.0+ (Big Sur a novšie)
- Android 8.0+ (API level 26+)
- iOS 13.0+

Základné funkcionality

- End-to-end šifrované textové správy
- Bezpečné hlasové hovory
- Šifrované video hovory
- Skupinové konverzácie
- Zdieľanie médií (obrázky, súbory)
- Miznutie správ (disappearing messages)
- Overenie identity kontaktov
- Offline doručovanie správ

Podporované protokoly

- Modifikovaný Signal/Matrix protokol pre správy s post-kvantovým šifrovaním
- WebRTC pre real-time komunikáciu s kvantovo-bezpečnými rozšíreniami
- Double Ratchet Algorithm s post-kvantovými primitívami
- Forward secrecy a post-compromise security

Audio/video kodeky

- **Audio**: G.711 (PCM), G.722 (HD audio), G.729, Opus
- **Video**: H.264, H.265/HEVC, VP8, VP9
- Adaptívna kvalita na základe šírky pásma

Implementácia

Návrh bude vychádzať z analýzy a modifikácie existujúcich open-source bezpečných komunikačných riešení (Signal, Element/Matrix, Briar, Session). Bude identifikované najvhodnejšie riešenie na customizáciu, ktoré už obsahuje všetky potrebné komunikačné funkcie a bezpečnostné mechanizmy.

Kľúčové modifikácie budú zahŕňať:

- Nahradenie existujúcich algoritmov výmeny kľúčov post-kvantovými (CRYSTALS-Kyber)
- Implementácia post-kvantových digitálnych podpisov (CRYSTALS-Dilithium)
- Úprava komunikačných protokolov pre post-kvantové primitívy
- Integrácia hybrid riešenia (klasické + post-kvantové algoritmy) pre prechodné obdobie
- Zachovanie kompatibility s existujúcou infraštruktúrou kde je to možné

Výhody tohto prístupu:

- Využitie existujúceho, prevereného kódu
- Kratší čas vývoja a testovanie
- Lepšia bezpečnosť vďaka existujúcim auditom
- Jednoduchšia údržba a budúce aktualizácie
- Možnosť porovnania s pôvodnou implementáciou

Výsledkom bude post-kvantová verzia bezpečnej komunikačnej aplikácie, ktorá poskytne používateľom ochranu pred súčasnými aj budúcimi kvantovými hrozbami pri zachovaní všetkých funkcionalít modernej komunikačnej platformy.

4) Tvorba celodiskového šifrovania alebo šifrovania súborov v kontajneroch

Existuje niekoľko produktov na celodiskové šifrovanie, niektoré sú voľne šíriteľné s dostupnými zdrojovými kódmi. Cieľom tejto časti aktivity je modifikovať LUKS/dm-crypt riešenie na spoluprácu so zabezpečeným operačným systémom a novými kryptografickými knižnicami založenými na post-kvantovej kryptografii.

Riešenie bude navrhnuté pre široké spektrum úložných zariadení vrátane SSD diskov, hybridných HDD a konvenčných HDD diskov, s dôrazom na optimalizáciu pre rôzne typy úložiska. Implementácia bude zahŕňať podporu pre nasadenie v dátových centrách, NAS systémoch a ďalších podnikových úložných riešeniach, pričom sa zabezpečí kompatibilita s existujúcimi infraštruktúrnymi riešeniami.

Technická implementácia

Modifikácia LUKS/dm-crypt bude zahŕňať:

- Integráciu post-kvantových kryptografických algoritmov
- Zachovanie kompatibility s existujúcimi LUKS kontajnermi
- Optimalizáciu výkonu pre rôzne typy úložných zariadení
- Rozšírenie key derivation funkcií pre PQC algoritmy

Komplexné testovanie

Súčasťou vývoja bude komplexné testovanie odolnosti šifrovania zahŕňajúce:

- Analýzu bezpečnosti implementovaných kryptografických algoritmov
- Penetračné testovanie a hodnotenie zraniteľností
- Výkonnostné testy na rôznych typoch úložných zariadení
- Testovanie kompatibility s rôznymi operačnými systémami a hardvérovými konfiguráciami

Verifikáciu odolnosti voči kvantovým útokom v kontexte post-kvantovej kryptografie

10. Predpokladaný časový rámec

Predpokladaný dátum vyhlásenia výzvy vo formáte mesiac/rok	01/2026
Predpokladaná doba realizácie NP v mesiacoch	48

Termíny v tabuľke nie sú záväzné.

11. Finančný rámec[21]

a) žiadateľa

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[22] (v EUR)	viac rozvinutý región	512 863,00 Eur
	menej rozvinutý región	17 482 337,00 Eur
Zdroj EÚ podľa kategórie regiónu[23] (v EUR)	viac rozvinutý región	512 863,00 Eur
	menej rozvinutý región	17 482 337,00 Eur
Zdroj ŠR podľa kategórie regiónu[24] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Vlastné zdroje prijímateľa[25] podľa kategórie regiónu[26] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Miera spolufinancovania (v %)	Zdroj EÚ	100%
	Štátny rozpočet SR	0%
	Prijímateľ	0%
Uplatňovanie špecifického pravidla financovania[27] (ak relevantné)	neaplikuje sa	
Zdroj pro-rata (v %)	neaplikuje sa	
	neaplikuje sa	
V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.	Neuplatňuje sa	

[21] Finančný rámec je potrebné uvádzať za celý NP spolu a v prípade financovania NP z viacerých priorít/špecifických cieľov, aj v rozdelení podľa špecifických cieľov.
[22] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[23] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[24] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[25] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027
[26] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[27] Uveďte konkrétne číslo tabuľky a jej názvu podľa Stratégie financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027.

b) partnera (ak relevantné)

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[28] (v EUR)	viac rozvinutý región	56 635,00 Eur
	menej rozvinutý región	1 930 565,00 Eur
Zdroj EÚ podľa kategórie regiónu[29] (v EUR)	viac rozvinutý región	56 635,00 Eur
	menej rozvinutý región	1 930 565,00 Eur
Zdroj ŠR podľa kategórie regiónu[30] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Vlastné zdroje partnera[31] podľa kategórie regiónu[32] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Miera spolufinancovania (v %)	Zdroj EÚ	100%
	Štátny rozpočet SR	0%
	Partner	0%
Zdroj pro-rata (v %)	neaplikuje sa	
	neaplikuje sa	
V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.	Neuplatňuje sa	

12.Rozpočet

V tejto časti uveďte, ako bol pripravovaný indikatívny rozpočet a ako spĺňa kritérium „hodnota za peniaze“, t. j. akým spôsobom bola odhadnutá cena za každú položku, napr. prieskum trhu, analýza minulých výdavkov spojených s podobnými aktivitami, nezávislý znalecký posudok. V prípade, ak príprave projektu predchádza vypracovanie štúdie uskutočniteľnosti, ktorej výsledkom je, okrem iného aj určenie výšky alokácie, je potrebné uviesť túto štúdiu ako zdroj určenia výšky finančných prostriedkov. Skupiny výdavkov doplňte v súlade s Príručkou k oprávnenosti výdavkov v platnom znení. V prípade infraštruktúrnych projektov, ako aj projektov súvisiacich s obnovou mobilných prostriedkov, sa do ukončenia verejného obstarávania uvádzajú položky rozpočtu len do úrovne aktivít.

Uveďte, či bude v národnom projekte využité zjednodušené vykazovanie výdavkov a ak áno, ktorá forma. V prípade využitia paušálnej sadzby, ktorej výška je stanovená v nariadení, sa spôsob stanovenia sadzby nepožaduje.

V prípade, že žiadateľ/partner poskytuje finančný príspevok užívateľovi, identifikujte v tabuľke nižšie, o ktoré skupiny výdavkov ide.

Indikatívny rozpočet bol pripravený v súlade so mzdovou politikou NBU a to tak, že pre každú aktivitu a jej časť bola odhadnutá prácnosť a časová náročnosť. Pre odborný personál bolo uvažované s hodinovou mzdou 50 EUR/hod, pre kľúčový odborný personál projektu bolo uvažované s hodinovou mzdou 100 EUR/hod. Zahraničný

[28] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[29] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[30] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[31] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027
[32] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

odborný personál bude hodnotený hodinovou mzdou rovnakou ako mu poskytuje jeho domovská organizácia (indikovaných 200 EUR/hod).

Rozpočet projektu je určený na mzdové náklady odborného personálu. Výskum bude prebiehať na už existujúcej prístrojovej infraštruktúre existujúcej na NBÚ alebo SAV. Prípadný nákup infraštruktúry, alebo softvérových licencií sa bude uskutočňovať jedine z paušálnych výdavkov.

Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu a ich výstižné zdôvodnenie

Predpokladané finančné prostriedky na aktivity NP	Celkové oprávnené výdavky (v EUR)	Plánované vecné vymedzenie
Hlavné aktivity		
Matematická podpora kvantových technológií	728 000	Mzdy na odborný personál, zahraničných a národných expertov z oblasti matematiky a kryptológie počas celého trvania projektu.
Matematické princípy post-kvantových šifrových algoritmov	1 000 000	Mzdy na odborný personál, zahraničných a národných expertov z oblasti matematiky a kryptológie počas celého trvania projektu.
Hlavné aktivity MU SAV	1 728 000	
Podporné aktivity MU SAV (15%)	259 200	
MU SAV spolu	**1 987 200**	
Vytvorenie prototypu zabezpečenej pracovnej stanice	2 000 000	Mzdy na odborný personál, najmä programátorov a IT expertov počas celého trvania projektu. Obsahuje ďalšie 4 samostatné logické celky.
Pod úloha 1 - Tvorba zabezpečeného operačného systému	2 000 000	Mzdy na odborný personál, najmä programátorov a IT expertov počas celého trvania projektu.
Pod úloha 2 - Tvorba VPN klienta	2 000 000	Mzdy na odborný personál, najmä programátorov a IT expertov počas celého trvania projektu.
Pod úloha 3 - Tvorba VoIP klienta	2 000 000	Mzdy na odborný personál, najmä programátorov a IT expertov počas celého trvania projektu.
Pod úloha 4 - Tvorba celodiskového šifrovania alebo šifrovania súborov v kontajneroch	2 000 000	Mzdy na odborný personál, najmä programátorov a IT expertov počas celého trvania projektu.
Vytvorenie Key Management centra pre generovanie a distribúciu dôveryhodného šifrového materiálu	5 648 000	Mzdy na odborný personál, najmä programátorov a matematikov počas celého trvania projektu.
Hlavné aktivity NBU	15 648 000	
Podporné aktivity NBU (15%)	2 347 200	
NBU spolu	**17 995 200**	
PROJEKT CELKOM NBU + MU SAV	**19 982 400**	

V prípade zvýšenia celkových oprávnených výdavkov NP (po jeho schválení komisiou pri Monitorovacom výbore pre Program Slovensko 2021 – 2027) o viac ako 15 % (a nejde o prípad, kedy je určenie alokácie výsledkom realizovanej štúdie uskutočniteľnosti), riadiaci orgán / sprostredkovateľský orgán predloží pred vyhlásením výzvy na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 upravený zámer NP.

Ostatné zmeny v rozpočte projektu (napr. doplnenie novej skupiny výdavkov, vypustenie skupiny výdavkov, zvýšenie alebo zníženie výšky oprávnených výdavkov v rámci skupín výdavkov a pod.) nie je potrebné predkladať na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027.

13.Ďalšie informácie o národnom projekte

Definuje riadiaci orgán / sprostredkovateľský orgán, ak je to relevantné, v nadväznosti na zameranie projektu (napr. v prípade IT projektov odkaz na dokumentáciu projektu dostupnú v Metainformačnom systéme Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky https://metais.vicepremier.gov.sk/).