

Závazné parametry řešení projektu

1. Název projektu

Budování kapacit a podpora spolupráce v postkvantové kryptografii

2. Doba zahájení a ukončení projektu

Datum zahájení projektu: 1. září 2024

Datum ukončení projektu (lhůta, v níž má být účelu dosaženo): 31. 8. 2025

3. Cíl(e) projektu (účel projektu)

Návrh projektu „Budování kapacit a podpora spolupráce v postkvantové kryptografii“ (DeCaPoQ) je zaměřen na rozšíření národní expertizy a rozvoj mezinárodní spolupráce v oblasti zvyšování odolnosti vůči kvantovým hrozbám, zejména pomocí prostředků postkvantové kryptografie. Cílem je udržet a dále rozšířit národní expertní základnu, který je schopna navrhovat, implementovat, hodnotit a provozovat systémy využívající postkvantovou kryptografii; rozvinout spolupráci mezi akademickým, privátním a veřejným sektorem a propojit klíčové instituce také na mezinárodní úrovni. Dílčím cílem je dále zvýšit povědomí o kvantových hrozbách a možných řešení u širší odborné veřejnosti a doplnit vzdělávání v této oblasti do studijních programů zaměřených na kybernetickou bezpečnost. Realizací projektu dojde k významné podpoře procesu přechodu na kvantově odolnou kryptografii, která je v současné době díky dokončující se standardizaci velmi aktuálním tématem.

4. Klíčová osoba řešitelského týmu



5. Plánované výstupy/výsledky projektu

Výstup/výsledek:

Číslo výstupu/výsledku: V001

Název výstupu/výsledku: Workshop I: Postkvantová kryptografie: strategie a roadmapping

Popis výstupu/výsledku: Jedná se o výsledek typu RIV-W, tedy uspořádání mezinárodního workshopu, který bude určen pro profesionály a širší odbornou veřejnost k tématům v oblasti postkvantové kryptografie a odolnosti vůči kvantovým hrozbám. Na workshopu bude probrán

aktuální stav kvantových hrozeb, vývoj postkvantové kryptografie a strategie přechodu na kvantově odolné řešení. Přednášky budou zajištěny zástupci z akademického a státního sektoru z ČR i zahraničí. Účelem workshopu bude propojit zástupce státního a akademického sektoru a diskutovat aktuální problémy spojené s přechodem na postkvantovou kryptografii. Přínosem tohoto výsledku bude posílení spolupráce státního a akademického sektoru v oblasti kvantové bezpečnosti a konsensus ve strategii, výzkumu a vývoji v dané oblasti. Předpokládá se dvoudenní program s cca 30 až 50 účastníky. Workshop bude částečně otevřen i širší veřejnosti, avšak bude vyžadována registrace z kapacitních důvodů.

Druh výstupu/výsledku: RIV-W

Výstup/výsledek:

Číslo výstupu/výsledku: V002

Název výstupu/výsledku: Workshop II: Postkvantová kryptografie v praxi

Popis výstupu/výsledku: Jedná se o výsledek typu RIV-W, tedy uspořádání workshopu, který bude zaměřen především na praktické problémy kvantové bezpečnosti a určen pro soukromý a veřejný sektor a odborníky v ICT. Účelem workshopu bude představit postkvantovou kryptografii, benefity a limity PQC, a prezentovat praktické příklady a nástroje pro nasazení PQC do praxe a do současných systémů ICT. V rámci workshopu vystoupí jak zástupci privátního sektoru, tak i akademického a státního sektoru. Přínosem tohoto výsledku bude posílení spolupráce mezi sektory, t.j. propojení soukromého, státního a akademického sektoru v oblasti kvantové bezpečnosti a přímé definování konkrétních problémů a výzev spojených s přechodem na postkvantovou kryptografii v praxi. Součástí akce bude i sekce brokerage, na které bude možné představit a probrat návrhy projektů a sestavit konsorcium. Předpokládá se jednodenní program s cca 20 až 150 účastníky. Převážná část workshopu bude otevřena i širší veřejnosti, avšak bude vyžadována registrace účastníků.

Druh výstupu/výsledku: RIV-W

Výstup/výsledek:

Číslo výstupu/výsledku: V003

Název výstupu/výsledku: Workshop III: Postkvantová kryptografie: principy a výzvy

Popis výstupu/výsledku: Jedná se o výsledek typu RIV-W, tedy uspořádání workshopu, který bude určen především pro studenty a další zájemce o problematiku kvantové bezpečnosti. Účelem workshopu bude atraktivně představit postkvantovou kryptografii od teoretických základů po praktické ukázky existujících nástrojů. Na workshopu vystoupí nejen zkušení akademici, ale i zástupci soukromého sektoru, kteří představí aktuální problémy z praxe. Cílem bude zvýšit povědomí o problematice kvantové bezpečnosti a zaujmout talentované studenty pro další studium a výzkum v této oblasti. Dalším přínosem akce bude možné propojení studentů a firem při řešení konkrétních problémů spojených s nasazením PQC v praxi a možností vytvoření stáží pro studenty. Předpokládá se jednodenní program s cca 20 až 150 účastníky. Workshop bude otevřen i pro širší veřejnost a nebude vyžadována registrace.

Druh výstupu/výsledku: RIV-W

Výstup/výsledek:

Číslo výstupu/výsledku: V004

Název výstupu/výsledku: Audiovizuální tvorba: Postkvantová kryptografie

Popis výstupu/výsledku: Jedná se o výsledek typu RIV-A, tedy audiovizuální tvorbu. Výsledek sdružuje kvalitní veřejné prezentace, které byly představeny během workshopu III, případně předchozích. Prezentace budou sloužit jako ucelený materiál v rámci problematiky postkvantové kryptografie a budou veřejně dostupné širší veřejnosti prostřednictvím webových stránek. Některé prezentace budou rovněž zařazeny jako nový výukový materiál v rámci některých předmětů studijního programu Informační bezpečnost na VUT v Brně.

Plánovaným dodatečným výstupem tohoto projektu je vytvoření nového konsorcia a příprava projektu do vhodné národní nebo EU výzvy v rámci kvantově-odolné bezpečnosti. Vzhledem k termínům výzev, které mohou být až po skončení projektu (tj. od 9/2025), není tento výsledek plánován jako závazný.

Druh výstupu/výsledku: RIV-A

6. Identifikační údaje účastníků

Hlavní příjemce: Vysoké učení technické v Brně

Role uchazeče na projektu: Hlavní řešitel

IČ: 00216305

DIČ / VAT-ID: CZ00216305

Obchodní jméno/název organizace: Vysoké učení technické v Brně

Právní forma: Veřejná vysoká škola

7. Náklady

Náklady - Souhrn		2024	2025
Osobní náklady [Kč]	448 452,00	149 484,00	298 968,00
Osobní náklady [Kč]	448 452,00	149 484,00	298 968,00
Úvazek [člověko-rok]		0,11	0,22
Průměrné osobní náklady na úvazek [Kč / člověko-rok]		1 379 852,31	1 379 852,31
Ostatní přímé náklady [Kč]	205 000,00	115 000,00	90 000,00
Cestovní náklady	65 000,00	25 000,00	40 000,00
Nákup služeb, materiálu, drobného hmotného a nehmotného majetku	140 000,00	90 000,00	50 000,00
Další přímé náklady	0,00	0,00	0,00
Nepřímé náklady [Kč]	45 742,00	18 514,00	27 228,00
Náklady celkem [Kč]	699 194,00	282 998,00	416 196,00
Zdroje			
Podpora [Kč]	699 194,00	282 998,00	416 196,00
Neveřejné zdroje [Kč]	0,00	0,00	0,00
Zdroje celkem [Kč]	699 194,00	282 998,00	416 196,00
Intenzita podpory [%]	100,00%	100,00%	100,00%