REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
URSIV

Načrt Evropske unije za postkvantno kriptografijo

Pogosta vprašanja

Skupina za sodelovanje NIS
Maj 2026

Kazalo

Seznam kratic

V dokumentu so kratice ob prvi omembi zapisane s slovenskim poimenovanjem. Spodnja tabela povzema najpomembnejše kratice in izraze, uporabljene v besedilu.

PQC	postkvantna kriptografija
NIS	varnost omrežij in informacijskih sistemov
NIS CG	Skupina za sodelovanje NIS
CRQC	kriptografsko relevanten kvantni računalnik
AES	napredni šifrirni standard
PKI	infrastruktura javnih ključev
KEM	mehanizem za enkapsulacijo ključev
KDF	funkcija za izpeljavo ključa
QKD	kvantna distribucija ključev
NIST	Nacionalni inštitut za standarde in tehnologijo ZDA
NCSC	Nacionalni center za kibernetsko varnost
ASD	Avstralski direktorat za signale
NSA	Agencija za nacionalno varnost ZDA
CNSA 2.0	Zbirka algoritmov za komercialno nacionalno varnost 2.0
SDO	organizacija za razvoj standardov
ANSSI	francoska agencija za kibernetsko varnost
BSI	nemški Zvezni urad za informacijsko varnost
NLNCSA	nizozemska nacionalna agencija za varnost komunikacij
ENISA	Agencija Evropske unije za kibernetsko varnost
IKT	informacijske in komunikacijske tehnologije
MSP	Evropska platforma več deležnikov za standardizacijo IKT
NIS 2	Direktiva NIS 2
CRA	Akt o kibernetski odpornosti
GDPR	Splošna uredba o varstvu podatkov
CSA	Akt o kibernetski varnosti
DORA	Akt o digitalni operativni odpornosti
ECSF	Evropski okvir znanj in spretnosti na področju kibernetske varnosti
MOOC	množični odprti spletni tečaji
ITAM	upravljanje sredstev informacijske tehnologije
ERC	Evropski raziskovalni svet
EIC	Evropski svet za inovacije
DIGITAL	Program Digitalna Evropa
RSA	kriptografski algoritem RSA
DSA	algoritem digitalnega podpisa
ECC	kriptografija eliptičnih krivulj

1 Uvod

Ta dokument vsebuje odgovore na pogosto zastavljena vprašanja v zvezi z objavo usklajenega načrta izvajanja za prehod na postkvantno kriptografijo (Načrt EU za PQC), ki ga je pripravila Skupina za sodelovanje NIS. Dokument predstavlja neuradni prevod gradiva Evropske komisije: EU Roadmap on PQC – Frequently Asked Questions.

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) priporoča, da vsi zavezanci po Zakonu o informacijski varnosti (ZInfV-1), kot tudi entitete, ki niso neposredno zavezane temu zakonu, začnejo z aktivnostmi za prehod na post-kvantno kriptografijo (PQC). Glede na naraščajoča tveganja, povezana z razvojem kvantnega računalništva, ter možnost scenarijev »shrani danes, dešifriraj kasneje«, je zgodnje načrtovanje in postopno uvajanje kvantno odpornih kriptografskih rešitev ključnega pomena za dolgoročno zaščito podatkov in storitev. URSIV zato spodbuja vse organizacije k izvedbi pregledov obstoječe uporabe kriptografije, pripravi načrtov uvajanja in dopolnjevanja obstoječih kriptografskih sistemov s PQC, kar bo omogočilo varno in zanesljivo digitalno okolje v prihodnosti.

2 Ocenjevanje kvantnega tveganja, mejniki in določanje prednostnih nalog

2.1 Kako je grožnja, ki jo predstavljajo napadi po načelu "shrani zdaj, dešifriraj pozneje", zajeta v modelu tveganja, predstavljenem v poglavju 5 "Ocenjevanje kvantnega tveganja" Načrta EU za PQC?

O: Pri napadu po načelu "shrani zdaj, dešifriraj pozneje" lahko napadalci že danes pridobijo šifrirane podatke in jih shranijo za poznejše dešifriranje, tj. za čas, ko bo na voljo dovolj zmogljiv kvantni računalnik. To je tveganje za vse informacije, ki morajo ostati zaupne daljše obdobje, zlasti po letu 2035. Izračun ocene kvantnega tveganja lahko organizacijam pomaga oceniti ranljivost za grožnje kvantnega računalništva ter določiti prednostne strategije za zmanjšanje tveganj v njihovih kriptografskih sistemih.

Na podlagi slike 2.7 iz Priročnika za prehod na PQC se ocena kvantnega tveganja izračuna s kombinacijo posameznih ocen ranljivosti, vpliva in zahtevnosti prehoda.

Na primer:

- če eden ali več uporabljenih algoritmov ni varnih pred kvantnimi napadi, je ocena kvantne ranljivosti 2;
- če bi napadalec lahko izvedel napad po načelu "shrani zdaj, dešifriraj pozneje" na podatke, katerih zaupnost mora ostati zaščitena po letu 2035, je ocena vpliva 3;
- na podlagi slike 2.7 v Priročniku za prehod na PQC iz tega izhaja, da je ocena kvantnega tveganja 3 ali 4, odvisno od ocene zahtevnosti prehoda;
- ocena kvantnega tveganja 3 ali 4 ustreza "visoki" stopnji kvantnega tveganja, kot je določeno v poglavju 5 "Ocenjevanje kvantnega tveganja" v Načrtu EU za PQC.

2.2 Ali je pravilno, da se uporaba naprednega šifrirnega standarda AES-128 za zaščito dolgoročne zaupnosti obravnava kot srednje tveganje in se zato prednostno obravnava na isti ravni kot prehod "enostavnih" primerov, ki ne zahtevajo veliko napora, npr. v primerjavi s kompleksnimi infrastrukturami javnih ključev (PKI), za preverjanje pristnosti?

O: Načrt EU za PQC se osredotoča na prehod kriptografije z javnim ključem, saj je tveganje pri njem bistveno večje kot pri kriptografiji s simetričnim ključem. Priporočilo načrta je, da se jasna prednost nameni prehodu kriptografije z javnim ključem. Pri tem je treba upoštevati nekatere praktične omejitve preprostih modelov za ocenjevanje tveganja. Res je, da bo uporaba modela za ocenjevanje kvantnega tveganja iz Priročnika za prehod na PQC v obeh primerih dala enako oceno kvantnega tveganja in s tem enako stopnjo kvantnega tveganja. Glejte tudi odgovor na naslednje vprašanje.

2.3 Ali kriptografsko relevantni kvantni računalniki (CRQC) vplivajo na simetrično kriptografijo? Če vplivajo, ali to spremeni določanje prednostnih nalog?

O: Ker je jasno, da bo kriptografsko relevanten kvantni računalnik (CRQC) močno vplival na kriptografijo z javnim ključem, napadi na najsodobnejše kriptografske algoritme s simetričnim ključem, kot je napredni šifrirni standard AES, pa se v bližnji prihodnosti ne zdijo praktično izvedljivi niti pri 128-bitnih ključih, se Načrt EU za PQC osredotoča na prehod kriptografskih sistemov z javnim ključem.

To ne spreminja prednostnih nalog glede na stopnjo kvantnega tveganja, lahko pa v praksi vpliva na izbiro rešitve. Na splošno se priporoča uvedba kriptografske prilagodljivosti, da se po potrebi omogočijo hitre spremembe algoritmov in/ali dolžin ključev.

2.4 V poglavju 5 Načrta EU za PQC je na primeru navedeno, da je stopnja kvantnega tveganja visoka, če prehod traja več kot osem let in je vpliv napada velik. Glede na časovnico je potrebno primere z visokim tveganjem prenesti do konca leta 2030, do takrat pa je manj kot osem let. Ali to ni protislovno?

O: Ker je opisani primer zahteven in nanj ni enostavnega odgovora, je treba upoštevati nekaj ključnih vidikov:

- V nekaterih primerih je lahko prepozno, da bi se organizacija osredotočila samo na dolgoročno rešitev. Prehod s tradicionalne asimetrične kriptografije na PQC bi lahko za določen primer uporabe trajal predolgo, zato je potrebno razmisliti o kratkoročnih alternativah, na primer o dodajanju vnaprej deljenih simetričnih ključev.
- Čeprav popoln prehod infrastrukture javnih ključev (PKI) do konca leta 2030 morda ne bo izvedljiv, je mogoče pred rokom leta 2030 poleg stare, kvantno ranljive PKI uvesti novo PKI, ki podpira PQC.
- Tveganja je potrebno stalno ocenjevati in spremljati razvoj kvantnega računalništva, hkrati pa pripraviti rezervni načrt za primer, da bi se kriptografsko relevanten kvantni računalnik pojavil v manj kot osmih letih.
- Pomembno je razumeti, zakaj je prehodno obdobje za posamezen primer uporabe tako dolgo. Eden od razlogov je lahko običajna življenjska doba naprav ali obdobje veljavnosti certifikatov. Prilagajanje teh časovnic je za organizacije lahko zahtevno, vendar lahko pospeši prehod.

2.5 Kako se pri določanju prednostnih nalog uravnotežijo grožnje zaupnosti na eni strani ter celovitosti in pristnosti na drugi strani?

O: Poglavje 5 Načrta EU za PQC z naslovom "Ocenjevanje kvantnega tveganja" navaja, da lahko izvedba ocene kvantnega tveganja pomaga pri določanju prednostnih nalog v procesu prehoda. Metodologija za izvedbo analize kvantnega tveganja je določena v Priročniku za prehod na PQC.

Organizacije bi morale s to metodologijo izračunati oceno kvantnega tveganja za vsak svoj primer uporabe. Nato se lahko na podlagi poglavja 5 Načrta EU za PQC določi stopnja kvantnega tveganja, povezana z oceno posameznega primera uporabe: nizka, srednja ali visoka.

Časovnica za prehod na PQC na strani 7 Načrta EU za PQC določa časovni okvir za vsako stopnjo kvantnega tveganja.

Pomembno je poudariti, da Načrt EU za PQC izrecno priporoča, naj bodo nadgradnje programske in vgrajene programske opreme, varne pred kvantnimi napadi, do konca leta 2030 privzeto omogočene.

2.6 Kako se predlagane časovnice usklajujejo z evropskimi in svetovnimi smernicami?

O: Načrt EU za PQC priporoča, da se prehod vseh primerov uporabe zaključi do konca leta 2035, razen pri nekaterih primerih uporabe z nizkim tveganjem. Ta časovnica se dobro ujema z drugimi smernicami v Evropi in na svetovni ravni, z izjemo Avstralije, kjer je rok ambicioznejši. Avstralski direktorat za signale (ASD) v dokumentu o načrtovanju postkvantne kriptografije priporoča, da organizacije prehod zaključijo do konca leta 2030.

V Združenih državah Amerike prvotni javni osnutek poročila IR 8547 Nacionalnega inštituta za standarde in tehnologijo (NIST) zahteva popoln prehod do leta 2035; ta datum je bil prvič določen v Memorandumu o nacionalni varnosti ZDA št. 10 leta 2022.

Podobno tudi Nacionalni center za kibernetsko varnost Združenega kraljestva (NCSC) v dokumentu o časovnici prehoda na postkvantno kriptografijo priporoča, da organizacije do konca leta 2035 zaključijo prehod vseh svojih sistemov na PQC. Enaka je tudi časovnica v načrtu prehoda na postkvantno kriptografijo za vlado Kanade, ki ga je pripravil Kanadski center za kibernetsko varnost; od zveznih ministrstev in agencij se pričakuje, da bodo do konca leta 2035 svoje sisteme prenesli na PQC.

3 Hibridne sheme

3.1 Kaj so hibridne sheme v kontekstu prehoda na postkvantno kriptografijo?

O: V Načrtu EU za PQC je hibridna shema opredeljena kot kombinacija postkvantnega algoritma in kvantno ranljivega algoritma za isti mehanizem, pri čemer je raven varnosti najmanj enaka varnosti varnejše od obeh sestavin. Načrt EU za PQC ne obravnava hibridnih mehanizmov, ki uporabljajo kvantno distribucijo ključev (QKD), ali mehanizmov, ki združujejo več kot en mehanizem PQC.

3.2 Ali se uporaba hibridnih kriptografskih shem, ki združujejo več shem kriptografije z javnim ključem, šteje za dolgoročno ali kratkoročno strategijo?

O: Trenutno ni jasnih smernic o tem, ali se hibridne kriptografske sheme štejejo za dolgoročno ali kratkoročno strategijo. Čeprav ni priporočila o tem, kdaj naj se hibridne sheme začnejo ali prenehajo uporabljati, so lahko koristne za omogočanje kriptografske prilagodljivosti.

3.3 Ali obstajajo različne smernice za hibridne mehanizme za enkapsulacijo ključev in hibridne podpisne sheme?

O: Da, smernice za hibridne mehanizme za enkapsulacijo ključev (KEM) in hibridne podpisne sheme se razlikujejo. Hibridni KEM so za uporabo preprostejši kot hibridne podpisne sheme. Pri KEM je standardna praksa, da se s funkcijo za izpeljavo ključa (KDF) združijo skrivnosti iz tradicionalnega, kvantno ranljivega asimetričnega algoritma in postkvantnega asimetričnega algoritma, da se izpelje skupna simetrična skrivnost. Če je to izvedeno pravilno, lahko zagotavlja visoko raven varnosti. Hibridne podpisne sheme pa vključujejo bolj zapletene interakcije in številne dejavnike, ki lahko vplivajo na njihovo varnost, zato je zanje težje določiti konkretne smernice. Ta tema sicer presega obseg Načrta EU za PQC. Za podrobnejše smernice o hibridnih KEM glejte npr. NIST SP 800-227.

3.4 Katere konkretne hibridne mehanizme priporoča delovna skupina za PQC v okviru Skupine za sodelovanje NIS in kako so ta priporočila usklajena v Evropi in na svetovni ravni?

O: Delovna skupina za PQC v okviru Skupine za sodelovanje NIS ne vodi seznama priporočenih hibridnih ali drugih algoritmov PQC. Priporoča pa, da se standardizirane hibridne rešitve uporabljajo povsod, kjer je to izvedljivo in primerno. To je skladno s priporočili drugih evropskih agencij za kibernetsko varnost, kot sta francoska Agencija za kibernetsko varnost (ANSSI) in nemški Zvezni urad za informacijsko varnost (BSI). Tehnična smernica BSI o kriptografskih algoritmih in dolžinah ključev na primer priporoča uporabo kombinacije tradicionalnih, kvantno ranljivih kriptografskih algoritmov in postkvantne kriptografije v hibridnih rešitvah. Poleg tega priporočilo Evropske komisije iz aprila 2024 o PQC priporoča hibridne sheme. Švedski nacionalni center za kibernetsko varnost (NCSC) je glede uporabe čistih shem PQC ali hibridov nevtralen; glavni cilj je zagotoviti najboljšo varnost v konkretnem primeru uporabe.

Z globalnega vidika Agencija za nacionalno varnost ZDA (NSA) v zbirki algoritmov za komercialno nacionalno varnost 2.0 (CNSA 2.0) priznava, da so hibridne rešitve morda potrebne za protokolarne standarde in interoperabilnost. Vendar hibridne rešitve niso vključene med obvezne algoritme CNSA 2.0 za sisteme nacionalne varnosti ZDA.

Poleg tega prvotni javni osnutek poročila NIST IR 8547 nakazuje, da bodo hibridne tehnike vključene v kriptografske standarde, da bi olajšale prehod na PQC. Hkrati pa dokument nakazuje, da bodo te hibridne metode verjetno prehodni ukrepi, ki bodo vodili k prihodnjemu prehodu na izključno uporabo algoritmov PQC.

V Združenem kraljestvu NCSC sprejema hibridne rešitve PQC kot prehodni ukrep, ki naj se uporablja v prilagodljivem okviru, vendar na splošno priporoča čiste sheme PQC.

Ker naj bi vsaka država članica pripravila nacionalni načrt, usklajen z Načrtom EU za PQC, bi morala upoštevati tudi obstoječa priporočila drugih držav članic.

4 Mejniki, “prvi koraki” in “naslednji koraki”

4.1 Ali mejniki in z njimi povezani roki veljajo za uvedbo in razpoložljivost izdelkov ali izključno za razpoložljivost v standardih?

O: Mejniki in roki, določeni v Načrtu EU za PQC, veljajo za uvedbo PQC. To pomeni, da morajo biti organizacije za razvoj standardov (SDO) in ponudniki pred časovnicami, določenimi v Načrtu EU za PQC.

Leta 2024 je Nacionalni inštitut za standarde in tehnologijo (NIST) objavil prvi sklop standardov PQC. Zaradi tekočega ocenjevanja dodatnih algoritmov bo kriptografska prilagodljivost pomembna ne le za prehod na PQC, temveč tudi za ohranjanje trdnega varnostnega položaja.

Pri presoji mejnikov in z njimi povezanih uvedb priporočila iz prvega koraka v točki 6.2 Načrta EU za PQC poudarjajo, da je treba začeti dialog z dobavitelji izdelkov in storitev, da se razumejo njihovi načrti za vključitev PQC in kriptografske prilagodljivosti v razvoj izdelkov ali storitev. To bo ključno za organizacije pri doseganju rokov iz točke 4.2 Načrta EU za PQC, saj bo izpolnitev teh rokov odvisna od razpoložljivosti skladnih izdelkov in storitev.

4.2 Ali mora organizacija dokončati pripravo svojega kriptografskega inventarja, preden začne načrtovati in prednostno razvrščati prehod na postkvantno kriptografijo?

O: Ne, organizacijam ni potrebno dokončati popisa, preden začnejo načrtovati in določati prednostne naloge. Kot je navedeno v točki 6.2 Načrta EU za PQC, sta vzpostavitev in vzdrževanje kriptografskega inventarja bistven prvi korak in ukrep “brez obžalovanja” za prepoznavanje, ocenjevanje in dokumentiranje kriptografskih sredstev. Kljub temu sta priprava celovitega inventarja in zmožnost razlage vse njegove vsebine zahtevni nalogi, saj lahko vključujeta tisoče kriptografskih funkcij, ključev, potrdil itd. Zato je pomembno, da subjekti hkrati z vzpostavljanjem inventarja pripravijo tudi okviren pregled svojih aplikacij: kaj podpirajo, katere so bistvene in od katerih strežnikov so odvisne.

Začetni inventar bo omogočil začetek načrtovanja na visoki ravni in določanja prednostnih nalog za prehod primerov z visokim tveganjem. Uporaba faznega pristopa, kot je opisan v časovnem načrtu EU za postkvantno kriptografijo, pomeni, da lahko organizacije nadaljujejo postopek priprave inventarja, hkrati pa že izvajajo prehod pri primerih uporabe z najvišjim tveganjem. Ker je priprava inventarja iterativen proces, bosta pri vsaki iteraciji nujna sočasna pregledovanje in izpopolnjevanje prednostnega razvrščanja ter načrtovanja. Vzdrževanje kriptografskega inventarja zahteva stalen pregled in posodabljanje, da se dobra varnostna drža ohrani tudi po prehodu na postkvantno kriptografijo.

4.3 Ali je treba "prve korake" dokončati, preden se začnejo izvajati "naslednji koraki"?

O: Ne, "prvih korakov" ni treba dokončati pred začetkom izvajanja "naslednjih korakov". Točka 6.3 Načrta EU za PQC poudarja pomen izvajanja drugih dejavnosti, ki lahko pripomorejo k nemotenemu prehodu, potem ko so "prvi koraki" že začeti. Izvajanje dejavnosti iz "naslednjih korakov" vzporedno s potekajočimi "prvimi koraki" bo zagotovilo, da bo prehod potekal brez nepotrebnih zamud.

5 Nacionalni načrti

5.1 Katere vidike Načrta EU za PQC bi bilo treba vključiti v nacionalni načrt?

O: Načrt EU za PQC za države članice določa konkretne ukrepe v okviru "prvih korakov" in "naslednjih korakov". Pri pripravi nacionalnega načrta bi morala vsaka država članica upoštevati te korake in jih nadgraditi, tako da jasno opredeli načrtovane dejavnosti in ustrezne časovne okvire.

V okviru "prvih korakov" bi morale države članice razmisliti o vključitvi naslednjih elementov:

- Pregled relevantnih nacionalnih in mednarodnih deležnikov z opisom njihove načrtovane vključenosti v nacionalni prehod.
- Načrt za spodbujanje in podporo:

1. pripravi in vzdrževanju popisov kriptografskih sredstev in zemljevidov odvisnosti;
2. izvedbi analiz kvantnega tveganja;
3. vključevanju dobavne verige.

- Sklic na nacionalni program ozaveščanja in komuniciranja, vključno s prilagojenimi strategijami ozaveščanja in komuniciranja.
- Predlog za izmenjavo znanja in sodelovanje v delovni skupini za PQC v okviru Skupine za sodelovanje NIS.

V okviru “naslednjih korakov” bi morale države članice razmisliti o vključitvi naslednjih elementov:

- Predlog za spodbujanje in, kjer je to primerno, uveljavljanje podpore za kriptografsko prilagodljivost ter kvantno varno pot nadgradnje izdelkov.
- Načrte za:

1. oceno in zagotovitev dodelitve ustreznih proračunskih in kadrovskih virov na vseh ravneh, vključno z rezervacijami proračunskih sredstev v okviru upravljanja življenjskega cikla;
2. prilagoditev nacionalnih in evropskih shem certificiranja kibernetske varnosti za obravnavo nastajajočih groženj, ki jih prinaša napredek kvantnega računalništva;
3. prepoznavanje in po potrebi pripravo predpisov in politik na področju kriptografije ter njihovo posodabljanje v skladu z najnovejšimi priporočili za PQC;
4. izvedbo pilotnih primerov uporabe in prispevanje k testnim centrom.

- Celovit pregled priložnosti v ekosistemu za nemoten globalni prehod, vključno z zasebnim sektorjem, programi usposabljanja in programi financiranja.
- Opis načrtovanih horizontalnih dejavnosti za podporo standardizaciji PQC, vključno z vključevanjem v standardizacijske odbore, sodelovanjem z drugimi subjekti in spodbujanjem nadaljnjih raziskav.

Države članice bi morale zgoraj navedene ukrepe obravnavati kot minimalni okvir, hkrati pa imajo možnost, da glede na nacionalne potrebe vključijo tudi dodatne ukrepe.

5.2 Ali bo delovna skupina za PQC v okviru Skupine za sodelovanje NIS objavila dodatne sektorske smernice?

O: Ne, delovna skupina za PQC v okviru Skupine za sodelovanje NIS ne bo objavila dodatnih sektorskih smernic. Vendar močno spodbuja sodelovanje na nacionalni in mednarodni ravni za krepitev partnerstev v industriji in pripravo sektorskih načrtov. Objava sektorskih načrtov bo organizacijam koristila pri izmenjavi znanja in izkušenj, ne le znotraj posameznih sektorjev, temveč tudi med sektorji.

5.3 Ali bo delovna skupina za PQC v okviru Skupine za sodelovanje NIS priporočila določene algoritme?

O: Ne, delovna skupina za PQC v okviru Skupine za sodelovanje NIS ne bo predlagala ali priporočala posebnih algoritmov ali mehanizmov, razen s sklicevanjem na obstoječe standarde in priporočila. Nacionalne agencije spodbuja, naj svoje predpise in priporočila, kadar je to mogoče, uskladijo s predpisi in priporočili drugih držav članic. Tak pristop bo optimiziral združljivost in sprejemljivost kriptografskih izdelkov po vsej Evropski uniji.

5.4 Kaj pomeni "zrelo upravljanje kriptografskih sredstev"?

O: Izraz "zrelo upravljanje kriptografskih sredstev" v Načrtu EU za PQC ali povezanih dokumentih ni izrecno opredeljen. Za namene Načrta EU za PQC se nanaša na dobro razvit, strukturiran in varen pristop k upravljanju vseh kriptografskih sredstev, kot so ključi in certifikati, skozi njihov celotni življenjski cikel. To vključuje vzdrževanje popolnega in posodobljenega popisa kriptografskih sredstev, razumevanje z njimi povezanih tveganj ter upravljanje z jasnimi politikami in postopki, ki omogočajo kriptografsko prilagodljivost in pravočasen prehod na nove standarde.

V praksi bi moral sistem za upravljanje sredstev informacijske tehnologije (ITAM) vključevati tudi popis in upravljanje življenjskega cikla kriptografskih sredstev. Za več podrobnosti glejte poglavje 2.4 Priročnika za prehod na PQC.

5.5 Katere kriptografske algoritme in protokole je treba zamenjati, da se zagotovi odpornost proti prihodnjim napadom dovolj zmogljivih kvantnih računalnikov?

O: Za odpornost proti prihodnjim napadom dovolj zmogljivega kvantnega računalnika je nujno tradicionalne asimetrične kriptografske mehanizme nadomestiti s kvantno varnimi alternativami. Mnogi kriptografski protokoli temeljijo na asimetričnih mehanizmih in so zato ranljivi za prihodnje kvantne napade. Posebej izpostavljeni so asimetrični algoritmi, kot so RSA, algoritem digitalnega podpisa (DSA) in kriptografija eliptičnih krivulj (ECC). Več informacij o pogostih protokolih je na voljo v poglavju 4.3 Priročnika za prehod na kvantno varno kriptografijo.

Pri simetričnih mehanizmih in zgoščevalnih funkcijah se razprava o vplivu kvantnih napadov nadaljuje. Trenutne raziskave preučujejo, ali bi bili taki napadi v praksi izvedljivi. Glede na uporabljene kriptografske standarde je lahko za večjo varnost priporočljiva uporaba daljših ključev ali večjih izhodnih dolžin. Podrobne informacije so na voljo v Priročniku za prehod na PQC, zlasti v poglavju 4.2, ki obravnava priporočene kriptografske primitive, in v poglavju 6, ki podaja ozadje teh primitivov. Dodatne podrobnosti in pojasnila vsebuje tudi tehnična smernica BSI o kriptografskih algoritmih in dolžinah ključev.

Ocena kvantnega tveganja vključuje tudi določitev kvantnih ranljivosti uporabljenih algoritmov. Poglavje 2.4 Priročnika za prehod na PQC obravnava oceno kvantnega tveganja, vključno s seznamom kriptografskih algoritmov in njihovimi ocenami kvantne ranljivosti.

5.6 Kaj pa kvantna distribucija ključev (QKD)? Ali se šteje za kvantno varno alternativo ali dodatno rešitev?

O: Delovna skupina za PQC v okviru Skupine za sodelovanje NIS močno priporoča, da se organizacije osredotočijo na zamenjavo kvantno ranljive kriptografije s postkvantno kriptografijo (PQC). To priporočilo temelji na trenutni uporabnosti in zrelosti PQC ter je skladno z dokumentom s stališčem o kvantni distribuciji ključev (QKD), ki so ga pripravili francoska Agencija za kibernetsko varnost (ANSSI), nemški Zvezni urad za informacijsko varnost (BSI), nizozemska Nacionalna agencija za varnost komunikacij (NLNCSA) in švedski Nacionalni organ za varnost komunikacij pri švedskih oboroženih silah.

Algoritmi PQC so zasnovani za delovanje na obstoječih sistemih in infrastrukturi informacijske tehnologije. Vse bolj so pripravljeni kot neposredna zamenjava za kvantno ranljive sisteme kriptografije z javnim ključem, kot sta RSA in ECC.

Nasprotno pa je QKD eksperimentalna, strojno zasnovana tehnologija. Uporablja načela kvantne fizike za zagotavljanje dodatne varnostne plasti, vendar je omejena na zelo specializirane primere uporabe, ki zahtevajo namensko infrastrukturo. Zaradi omejene praktične uporabnosti in nezadostne zrelosti se QKD trenutno ne šteje za izvedljivo kvantno varno alternativo.

6 Evropska unija

6.1 Kakšna je vloga institucij Evropske Unije (EU) in katere ukrepe lahko sprejmejo za podporo prehodu?

O: Institucije EU lahko za podporo prehodu na PQC sprejmejo različne pobude.

Ključni ukrepi vključujejo:

- Letni delovni program EU za evropsko standardizacijo, ki ga pripravlja Evropska komisija, je mogoče uporabiti za podporo prehodu na PQC. V programu za leto 2025 so bili kot prednostne naloge opredeljeni standardi, ki spodbujajo razvoj kvantne tehnologije in izvajanje protokolov PQC. Evropska komisija ima možnost, da v prihodnjih delovnih programih standardizacijske ukrepe na področju PQC posebej izpostavi kot ločeno politično prednostno nalogo.
- Evropska komisija bi morala ukrepe v zvezi s PQC vključiti v tekoči načrt za standardizacijo informacijsko-komunikacijskih tehnologij (IKT), ki povezuje politike EU in standardizacijske dejavnosti. Načrt dopolnjuje Letni delovni program EU za evropsko standardizacijo ter vključuje prispevke Evropske platforme več deležnikov za standardizacijo IKT (MSP).
- Evropska komisija ali Agencija Evropske unije za kibernetsko varnost (ENISA) bi lahko razvila indeks pripravljenosti EU na PQC, ki bi organizacijam omogočal poročanje o njihovi pripravljenosti na PQC in primerjavo s pripravljenostjo drugih organizacij. Tak indeks bi omogočil celovito oceno splošne pripravljenosti EU na prihodnje grožnje, ki jih predstavljajo dovolj zmogljivi kvantni računalniki.
- Zagotovitev dodatnih sredstev EU za raziskovalne in inovacijske projekte, povezane s prehodom na PQC, bi okrepila konkurenčnost evropskega notranjega trga in povečala kibernetsko odpornost po vsej EU.
- Institucije EU lahko ozaveščajo o kvantni grožnji za kriptografijo in o PQC prek konferenc, okroglih miz, delavnic, spletnih seminarjev, publikacij in sporočil za javnost. Ta seznam ni izčrpen; obstaja še veliko možnih pobud pod vodstvom EU, ki bi lahko podprle prehod na PQC.

6.2 Kako se Načrt Evropske Unije (EU) za PQC usklajuje z zakonodajo EU, kot so Direktiva NIS 2, Akt o kibernetski odpornosti (CRA), Splošna uredba o varstvu podatkov (GDPR), Akt o kibernetski varnosti (CSA) in Akt o digitalni operativni odpornosti (DORA)?

O: Načrt EU za PQC podpira te zakonodajne okvire, saj zagotavlja smernice o naprednih kriptografskih ukrepih za pripravo na morebitne grožnje kvantnega računalništva. Njegovo izvajanje prispeva k varnosti in odpornosti digitalne infrastrukture ter k varstvu podatkov, vključno z zasebnostjo, v EU. S ključno zakonodajo se usklajuje tako:

- Direktiva NIS 2: določa ukrepe za izboljšanje kibernetske varnosti EU. Uvedba PQC je ključna za zaščito bistvenih in pomembnih subjektov pred grožnjami kvantnega računalništva.
- Akt o kibernetski odpornosti (CRA): določa obvezne zahteve glede kibernetske varnosti za izdelke z digitalnimi elementi, vključno z zaupnostjo podatkov, po pristopu, ki temelji na tveganju. PQC je potrebna za zaščito teh izdelkov pred kvantnimi grožnjami.
- Splošna uredba o varstvu podatkov (GDPR): ureja varstvo podatkov, vključno z varnostjo obdelave podatkov. Prehod na PQC pomaga zagotavljati skladnost z GDPR, saj varuje podatke pred kvantnimi tveganji.
- Akt o kibernetski varnosti (CSA): vzpostavlja evropski okvir za certificiranje kibernetske varnosti, ki omogoča razvoj in sprejetje evropskih shem certificiranja kibernetske varnosti. Vključitev zahtev PQC v certifikacijski postopek zagotavlja, da so izdelki zaščiteni pred kvantnimi ranljivostmi.
- Akt o digitalni operativni odpornosti (DORA): krepi digitalno operativno odpornost finančnih subjektov. Uvedba PQC je ključna za zaščito finančnih sistemov pred grožnjami kvantnega računalništva.

6.3 Kaj je mogoče storiti za odpravo vrzeli v znanju in pomanjkanja strokovnjakov v Evropski Uniji (EU), da bi podprli prehod na PQC?

O: Na nacionalni ravni in ravni EU je mogoče sprejeti več ukrepov za vzpostavitev trdne baze strokovnjakov, sposobnih obravnavati izzive in priložnosti, ki se pojavljajo pri prehodu sistemov na PQC, ter zagotoviti tehnološki napredek in kibernetsko odpornost. Nekateri od teh ukrepov so:

- Izobraževalni programi in programi usposabljanja: razvoj specializiranih predmetov in študijskih programov na področju kriptografije, vključno s postkvantno kriptografijo, na univerzah in tehničnih ustanovah ob upoštevanju povratnih informacij držav članic o potrebah industrije in javnega sektorja na področju PQC. To bi lahko vključevalo tudi podiplomske predmete, posebej usmerjene v PQC.
- Spletne učne platforme in množični odprti spletni tečaji (MOOC): razvoj, spodbujanje in ponudba množičnih odprtih spletnih tečajev ter drugih spletnih virov, osredotočenih na postkvantno kriptografijo, za širši dostop do izobraževanja po vsej EU.
- Strokovni razvoj in certificiranje: razvoj certificiranja za strokovnjake na področju kibernetske varnosti na podlagi Evropskega okvira znanj in spretnosti na področju kibernetske varnosti (ECSF) ter spodbujanje razvoja specializiranih dodatnih certifikatov na področju PQC z izkoriščanjem partnerstev s strokovnimi organi in industrijskimi združenji.
- Javno-zasebna partnerstva: spodbujanje sodelovanja med industrijo, akademskim okoljem in javnim sektorjem za lažjo izmenjavo znanja in razvoj praktičnih spretnosti, vključno z možnostmi za pripravništva in programe praktičnega usposabljanja za študente in strokovnjake.
- Financiranje in podpora raziskavam: povečanje financiranja raziskav na področju PQC, da se omogoči večje vključevanje študentov in raziskovalcev v razvoj strokovnega znanja in izobraževalnih virov.
- Sodelovalni raziskovalni projekti: podpora sodelovalnim raziskovalnim projektom po vsej EU za napredek tehnologij PQC, hkrati pa zagotavljanje možnosti usposabljanja za raziskovalce in strokovnjake.
- Delavnice in konference: organizacija dogodkov o PQC za izmenjavo znanja in dobrih praks ter spodbujanje mreženja med strokovnjaki in študenti, s čimer se zagotovi platforma za učenje in sodelovanje na tem področju.
- Kampanje ozaveščanja: začetek kampanj za ozaveščanje o pomenu PQC za kibernetsko varnost, s katerimi se študente in strokovnjake spodbuja k izbiri poklicne poti na tem področju.

6.4 Kateri viri so pri institucijah Evropske Unije (EU) na voljo za podporo izvajanju rešitev PQC?

O: Izvajanje rešitev PQC v EU podpirajo pobude institucij EU, katerih namen je olajšati raziskave, razvoj in sprejemanje tehnologij PQC, da bi kriptografski sistemi ostali varni tudi v prihodnosti. Nekateri ključni razpoložljivi viri so:

- Obzorje Evropa: vodilni program EU za raziskave in inovacije zagotavlja sredstva za projekte, usmerjene v napredek temeljnih raziskav na področju PQC in praktičnih rešitev PQC. Podpira sodelovalne raziskave držav članic EU na področju PQC v številnih razpisih v sklopu "Civilna varnost za družbo" in v več razpisih v sklopu "Digitalno področje, industrija in vesolje". Evropski raziskovalni svet (ERC) z individualnimi in sodelovalnimi nepovratnimi sredstvi ter sheme Evropskega sveta za inovacije (EIC) so prav tako del programa Obzorje Evropa in zagotavljajo sredstva za temeljno znanost, inovacije in pospeševanje razvoja;
- Program Digitalna Evropa (DIGITAL): program se osredotoča na krepitev strateških digitalnih zmogljivosti EU, vključno s kibernetsko varnostjo. Podpira uvajanje in sprejemanje PQC s financiranjem povezanih raziskovalnih in razvojnih projektov ter izboljšav infrastrukture.
- Agencija Evropske unije za kibernetsko varnost (ENISA): ENISA je objavila več študij o PQC, v katerih predstavlja ključne koncepte PQC, stanje standardizacijskih dejavnosti, ocene tveganj ter nujnost oblikovanja novih kriptografskih protokolov in vključevanja postkvantnih sistemov v obstoječe protokole.
- Pobude za sodelovanje in mreženje: EU podpira različne mreže in platforme za sodelovanje, ki olajšujejo izmenjavo znanja in skupna prizadevanja pri razvoju in izvajanju PQC ter združujejo deležnike iz akademskega okolja, industrije in javnega sektorja.

7 Razno

7.1 Kako lahko izvedem prehod svoje organizacije na PQC?

O: Načrt EU za PQC vsebuje splošna priporočila, mejnike in časovne okvire za prehod na PQC. "Prvi koraki", opisani v točki 6.2 Načrta EU za PQC, bodo v pomoč organizacijam, ki začenjajo načrtovati in pripravljati prehod na PQC. "Naslednji koraki", opisani v točki 6.3, lahko organizacijam olajšajo nemoten prehod. Poleg tega so v Priročniku za prehod na PQC na voljo posebne smernice v zvezi s koraki opredeljenimi v Načrtu EU za PQC.

V skladu s poglavjem 4.1 Načrta EU za PQC bi morale države članice do konca leta 2026 pripraviti svoje začetne nacionalne načrte. Organizacije bi morale nacionalne načrte upoštevati skupaj s smernicami in nasveti, ki jih izdajo njihove nacionalne agencije za kibernetsko varnost.

Delovna skupina za PQC v okviru Skupine za sodelovanje NIS razmišlja o dodatnih publikacijah, ki bi lahko organizacijam dodatno pomagale pri prehodu na PQC.

7.2 Kaj če se razvoj kvantnih računalnikov hitro pospeši?

O: Vsaka pospešitev razvoja kvantnega računalništva bo povečala nujnost prehoda na PQC. Za obravnavo grožnje za prednostne sisteme je bistveno, da organizacije pripravijo načrte za nepredvidene razmere, v katerih opredelijo hitre ukrepe za ublažitev tveganj.

7.3 Ali morajo biti vsi sistemi kritične infrastrukture do leta 2030 odporni proti morebitnim napadom dovolj zmogljivega kvantnega računalnika?

O: Priporoča se pristop, ki temelji na tveganju, kot je opisan v Načrtu EU za PQC. Načrt EU za PQC določa, da bi morali vsi primeri uporabe z visokim tveganjem preiti na PQC do konca leta 2030. Čeprav ocena tveganja za posamezne sisteme kritične infrastrukture presega obseg tega dokumenta, bi morala vsaka država članica ponudnike kritične nacionalne infrastrukture spodbujati, naj kvantno grožnjo vključijo v svoje strategije obvladovanja tveganj.

7.4 Kateri subjekti bi morali pripraviti popise kriptografskih sredstev in zemljevide odvisnosti, vključiti dobavno verigo ter opraviti analizo kvantnega tveganja, kot je navedeno v "prvih korakih"?

O: V Načrtu EU za PQC se izraz „subjekt" nanaša na katero koli organizacijo. Najmanj subjekti, ki spadajo na področje uporabe Direktive NIS 2, vključno z organi javne uprave in ponudniki kritične infrastrukture, bi morali pripraviti popis kriptografskih sredstev in zemljevide odvisnosti, vključiti dobavno verigo ter opraviti analizo kvantnega tveganja. Vendar se kot proaktivni ukrep za zagotavljanje trdnega varnostnega položaja vse organizacije spodbuja, da sprejmejo te ukrepe.