REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Varna digitalna prihodnost v dobi kvantnih računalnikov

Prehod v post-kvantno kriptografijo (PQC)

April 2026

Uvod

V ozadju naših vsakodnevnih digitalnih dejavnosti delujejo številni kriptografski (šifrirni) algoritmi, ki zagotavljajo varnost naših podatkov, dokazujejo resnično identiteto spletnih strani, omogočajo varne bančne transakcije, digitalno podpisovanje in še in še. Kljub temu, da je bila večina teh algoritmov zasnovanih že pred desetletji, so še vedno zanesljivi, saj njihova varnost temelji na reševanju težkih matematičnih problemov.

Stvari pa se počasi spreminjajo zaradi naraščajoče moči kvantnih računalnikov. Ocenjujemo, da tveganje za obstoj dovolj močnega kvantnega računalnika, ki bi bil zmožen zlomiti današnjo kriptografijo (tako imenovan kriptografsko relevanten kvantni računalnik), narašča dovolj hitro, da bomo določene kriptografske algoritme morali zamenjati z novimi.

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.

Implementacija post-kvantne kriptografije (PQC) tudi neposredno naslavlja obveznosti, ki jih subjektom - zavezancem nalaga ZInfV-1. Posebno relevantna je povezava z 8. točko drugega odstavka 22. člena v povezavi s tretjim odstavkom istega člena, ki določa uporabo kriptografije kot enega izmed temeljenjih varnostnih ukrepov, kar pa v kontekstu kvantnih groženj pomeni:

- Zavezanci z visokim tveganjem (izvajalci bistvenih storitev, zlasti kritična infrastruktura) morajo PQC vključiti v svojo varnostno dokumentacijo oziroma politike in izvesti potrebne ukrepe.

- Popis kriptografskih rešitev, ki je splošno priporočilo, postane zakonsko nujen pripomoček za dokazovanje skladnosti z ZInfV-1.

Pravočasen začetek prehoda na PQC za zavezance iz ZInfV-1 tako ne pomeni le tehnološke posodobitve, temveč izpolnjevanje zakonske dolžnosti po zagotavljanju varnosti informacijskih sistemov v skladu z najnovejšimi evropskimi in mednarodnimi standardi ter obstoječimi ali prepoznanimi tveganji.

Slika 1: Shematski prikaz kvantnega računalnika.

Kaj je kvantni računalnik?

Kvantni računalnik je vrsta računalnika, ki za izvajanje izračunov uporablja nenavadna načela kvantne mehanike. Torej mehanike, ki opisuje obnašanje atomskih in subatomskih delcev. Za razliko od klasičnih računalnikov, ki so bili razviti sredi 20. stoletja, je kvantne računalnike prvič teoretično opredelil fizik Richard Feynman v začetku 80. let prejšnjega stoletja. Feynman je predlagal, da bi lahko kvantni računalniki rešili težave, s katerimi se spopadajo običajni računalniki, tako da bi z uporabo kvantnih lastnosti obdelali informacije na povsem nove načine.

Prvi delujoči kvantni računalnik je bil zgrajen leta 1998 in je bil v primerjavi s sodobnimi modeli zelo omejen. Od takrat si znanstveniki prizadevajo izboljšati te stroje, da bi bili hitrejši in zmogljivejši.

Slika 2: Fotografija kvantnega računalnika.

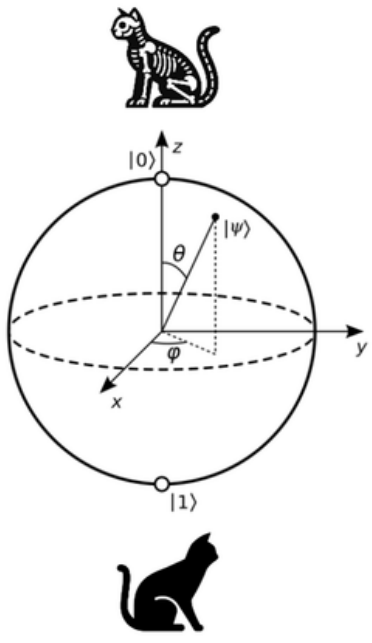
O kubitu

Kubit je okrajšava za kvantni bit, ki je temeljna enota kvantne informacije. Gre za analogijo klasičnemu bitu, ki je osnovna enota informacije v današnjih računalnikih. Poglejmo, kako se obnaša kubit. Vemo, da naši običajni računalniki računajo s pomočjo bitov. Glede na električno napetost, ima lahko bit vrednost ali 1, ali 0. Če tako pogledamo skupek 2 bitov, lahko v njih shranimo eno od štirih vrednosti: 00, 01, 10, ali 11.

Kubit se obnaša precej drugače. Spomnimo se miselnega eksperimenta Schrödingerjeve mačke. Običajna razlaga pravi, da je mačka, ki jo spravimo v škatlo in škatlo zapremo, hkrati živa in mrtva. Če smo bolj natančni, je opis sledeč. Ko je škatla zaprta, obstaja določena možnost, da je mačka živa, in določena možnost, da je mačka mrtva. Da ugotovimo njeno stanje, moramo škatlo odpreti in pogledati vanjo.

To je dober opis kubita. Vendar ko računamo s kubitom, ne moremo vmes brati njegove vrednosti (škatla je zaprta). Vemo pa, da bo na koncu zavzel ali vrednost 0 (mrtva mačka), ali vrednost 1 (živa mačka). Med samim računanjem obstaja določena verjetnost, da bo kubit končal v 1 in določena verjetnost, da bo končal v 0. Mačka torej ni hkrati živa in mrtva, ampak v vsakem trenutku obstaja določena možnost, da je živa, in določena možnost, da je mrtva. Ob koncu računanja kubit zavzame vrednost (ko škatlo odpremo) in preberemo rezultat.

Vizualno kubit običajno predstavimo z Blochovo sfero. Zgornji pol sfere, vrh predstavlja vrednost 0 (mrtva mačka), spodnji pol oziroma dno predstavlja vrednost 1 (živa mačka). Vse ostalo območje vrednosti predstavlja kombinacijo obeh dveh možnosti.



Slika 3: Blochova sfera s Schrödingerjevo mačko.

Kaj lahko kvantni računalniki naredijo?

To nenavadno in nam neintuitivno obnašanje je eden od razlogov, zakaj težko razumemo delovanje kvantnih računalnikov. A prav to nenavadno obnašanje pri specifičnih izračunih omogoča učinkovitejše in hitrejše iskanje rešitve. Trenutni kvantni računalniki sicer še niso pretirano zmogljivi, vendar njihova računska moč, stabilnosti kubitov, kakovost kod za popravljanje napak in druge pomembne komponente bistveno napredujejo iz leta v leto.

Pričakuje se, da bodo kvantni računalniki reševali zapletene matematične probleme veliko hitreje kot tradicionalni računalniki, na primer simuliranje molekul za odkrivanje zdravil, optimizacijo dobavnih verig ali razbijanje številnih danes uveljavljenih metod šifriranja.

Prav razbijanje metod šifriranja je še posebej zaskrbljujoče. V 90. letih prejšnjega stoletja sta bila definirana dva kvantna algoritma – Shorjev in Groverjev algoritem. Ta algoritma bosta z uporabo dovolj zmogljivega kvantnega računalnika lahko oslabila skoraj vso danes uporabljeno kriptografijo ter popolnoma zlomila določene algoritme (RSA in ECC). Zaradi te moči so kvantni računalniki prelomno orodje in hkrati tehnologija, ki zahteva nove oblike digitalne varnosti. Z zaščito šifriranja pred grožnjami kvantnega računalništva se ukvarja post-kvantna kriptografija, katere cilj je varnost naših podatkov in identitet v prihodnosti, ko bo kvantno računalništvo sposobno izničiti danes učinkovite varnostne mehanizme.

Kaj so post-kvantni algoritmi?

Algoritme, ki bodo odporni na grožnje kvantnega računalništva imenujemo algoritmi post-kvantne kriptografije ali post-kvantni algoritmi. Prednost teh algoritmov je, da za njihovo uporabo ne potrebujemo kvantnih naprav in jih zato lahko uporabimo že danes. Delujejo v običajnih računalnikih, mobilnih napravah in strežnikih in so odporni na prihodnje napade s kvantnimi računalniki.

Za zaščito naših digitalnih podatkov pred prihodnjo grožnjo kvantnih računalnikov je ameriški Nacionalni inštitut za standarde in tehnologijo (NIST) leta 2016 začel pomemben natečaj. Njegov cilj je bil najti nove kriptografske algoritme, ki so dovolj močni, da se lahko uprejo napadom kvantnih računalnikov. S tem svetovnim natečajem so pozvali znanstvenike, kriptografe in matematike z vsega sveta, da predložijo in preizkusijo potencialne algoritme. Avgusta 2024 so bili tako definirani prvi trije standardi post-kvantne kriptografije, v prihodnjih letih pa pričakujemo še druge.

Na področju kibernetske varnosti standardizacija pomeni izbiro enotnega, zaupanja vrednega nabora varnostnih algoritmov, na katerega se lahko zanesejo vsi, od vladnih agencij do zasebnih podjetij. Poleg tega je vzpostavljanje varnih sistemov, ki delujejo skupaj po vsem svetu precej lažje, če vsi uporabljajo iste metode. NIST pomaga z vzpostavitvijo standardiziranih algoritmov za post-kvantno kriptografijo zagotoviti, da bodo še pred napadi s kvantnimi računalniki vsi lahko prešli na varne in zanesljive metode šifriranja.

Kje bodo uporabljeni post-kvantni algoritmi?

Ko bodo kvantni računalniki postali zmogljivejši, bo post-kvantna kriptografija (PQC) postopoma vgrajena v čisto vsakdanja digitalna orodja, saj bodo le na tak način naši podatki varni. PQC bomo v prihodnosti prej ali slej uporabljali v medmrežju – pri komunikacijskih protokolih – ter v različnih primerih uporabe digitalnih potrdil.

Ko brskamo po internetu, uporabljamo elektronsko pošto ali dostopamo do varnih spletnih mest, se naše naprave zanašajo na omrežne protokole za zaščito podatkov, ki jih pošiljamo in prejemamo. Vsi se na primer vsakodnevno srečujemo s protokolom HTTPS za varno dostopanje do spletnih strani. Ta pomaga ohranjati naše osebne podatke zasebne in varne. V prihodnosti bo tem protokolom dodana PQC, ki jih bo zaščitila pred grožnjo kibernetskih napadov s kvantnimi računalniki. Tako bomo lahko še naprej brez skrbi uporabljali spletne storitve, saj bomo vedeli, da so naši podatki varni pred tradicionalnimi in kvantnimi grožnjami.

Slika 4: Shematski prikaz računalniške mreže.

Digitalna potrdila so nekakšne osebne izkaznice, s katerimi spletna mesta, računalniški programi in storitve dokazujejo, da so legitimne in da jim lahko zaupamo. Vsakič, ko na primer obiščete varno spletno mesto (pogosto označeno z ikono ključavnice v naslovni vrstici), se preko digitalnega potrdila tega spletnega mesta izvede preverjanje, ali ste res na pravem spletnem mestu. Kvantno odporna digitalna potrdila, zavarovana s PQC, bodo v prihodnosti uporabnike in ponudnike zaščitila pred tveganjem goljufije in kraje identitete s kvantnimi računalniki. To pomeni, da bomo lahko zaupali, da so spletna mesta in storitve pristne in varne.

Digitalna potrdila se uporabljajo tudi kot digitalne identitete za ljudi, zato je njihova varnost še posebej pomembna. V Sloveniji lahko vsak zaprosi za pridobitev digitalnega potrdila SIGEN-CA, ki ga državljanom zagotavlja Republika Slovenija, ali drugih, kot sta REKONO in HALCOM.

SI-TRUST
SIGEN-CA

Slika 5: SIGEN-CA logotip.

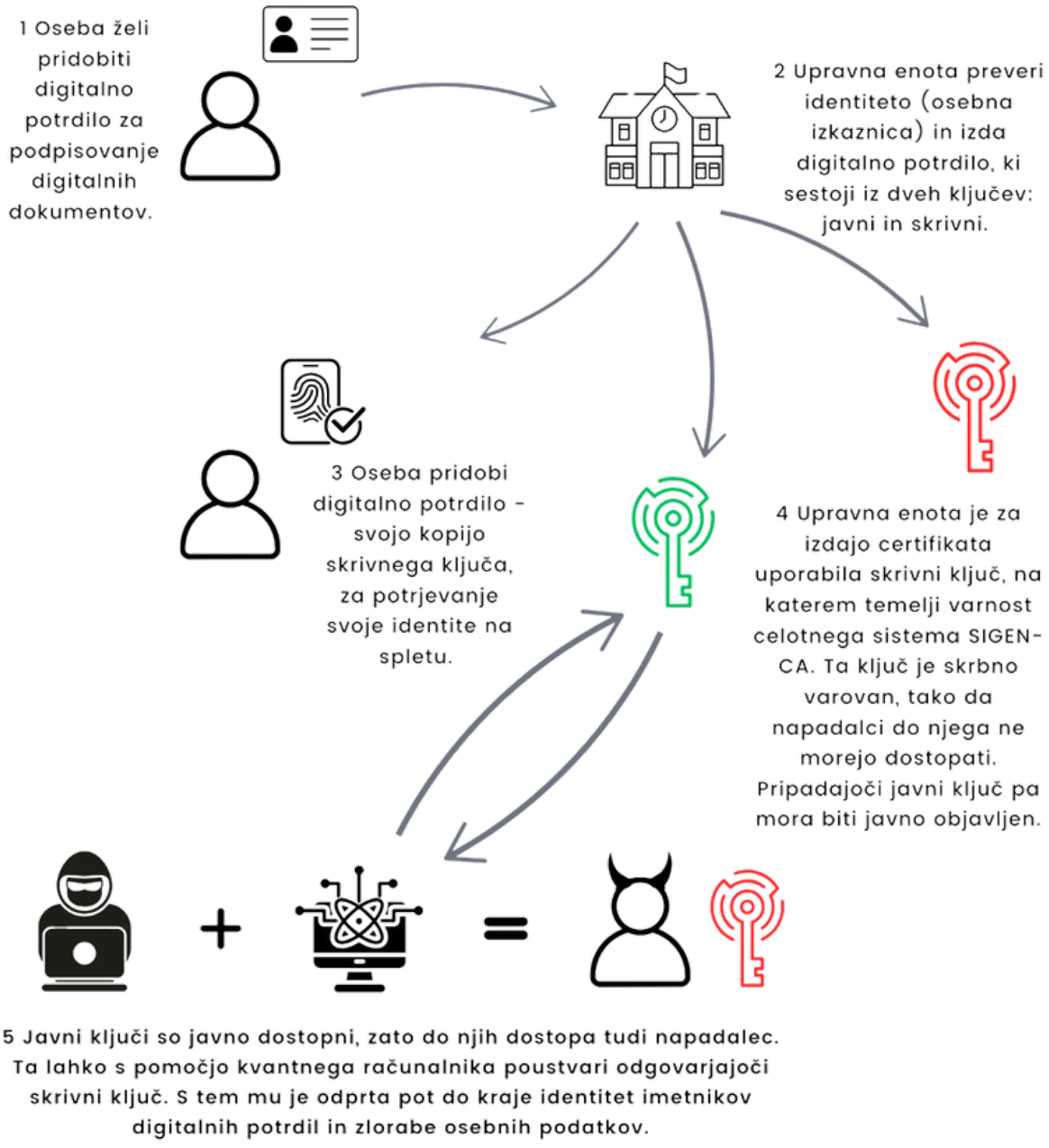
Kako poteka kvantni napad

Poglejmo si, kako bi lahko napadalec z enim samim izračunom na kvantnem računalniku ogrozil digitalna potrdila. Takšen napad je izvedljiv na poljubnih digitalnih potrdilih, za primer pa si bomo izbrali digitalna potrdila SIGEN-CA, ker so najširše poznana in kot brezplačna tudi pogosto uporabljena.

Za pridobitev digitalnega potrdila SIGEN-CA mora slovenski državljan, ki je starejši od 15 let in opravilno sposoben, z veljavnim osebnim dokumentom obiskati registrski organ, na primer upravno enoto, kjer izpolni vlogo in uredi potrebno identifikacijo za preverjanje pristnosti njegove identitete. Ko je potrdilo odobreno, državljan prejme potrdilo bodisi na varnem USB ključku, ali kot elektronsko datoteko, ki jo lahko nato namesti na svoj računalnik ali napravo, s čimer omogoči varne spletne storitve in digitalno podpisovanje.

Celotno hierarhijo digitalnih potrdil varuje par kriptografskih ključev: skrivni (zasebni) ključ, ki ga certifikatska agencija SIGEN-CA uporablja za izdajo certifikatov, ter javni ključ za preverjanje identitete, ko se želimo identificirati z našim digitalnim potrdilom. Ker je javni ključ javno objavljen, lahko napadalec pridobi dostop do njega. Z dovolj zmogljivim kvantnim računalnikom lahko izračuna, kateri je njemu pripadajoči skrivni (zasebni) ključ, ki ga SIGEN-CA uporablja za izdajo digitalnih potrdil. Ta ključ lahko zlonamerni akterji uporabijo bodisi za poneverjanje digitalnih certifikatov, bodisi za krajo identitet.

Možen scenarij kvantnega napada na uporabnika digitalnega potrdila



Slika 6: Prikaz potencialnega napada na infrastrukturo javnih ključev.

Evropski načrt prehoda v post-kvantno kriptografijo

Postkvantna kriptografija (PQC) postaja nujni del zagotavljanja kibernetske varnosti. Današnje kriptografske rešitve namreč ne bodo zadostovale ob zmogljivih kvantnih računalnikih v bližnji prihodnosti. Zato obstaja tveganje »shrani danes, dešifriraj kasneje« (store-now-decrypt-later): napadalci lahko že danes prestrežejo šifrirane podatke in jih dešifrirajo šele čez leta, ko bo tehnologija to omogočila.

Evropska komisija je 11. aprila 2024 objavila priporočilo o usklajenem načrtu za implementacijo PQC. V okviru NIS skupine za sodelovanje je bila vzpostavljena delovna skupina za PQC, ki je 20. junija 2025 sprejela t. i. EU roadmap za PQC.

Ta dokument določa ukrepe za usklajen prehod na uporabo PQC na ravni držav članic EU. Predvideva dva tipa ukrepov. Prvi so začetni koraki, potrebni za uspešen začetek prehoda. Ti se lahko začnejo izvajati takoj in so pomembni predvsem zato, ker povečujejo pripravljenost sistemov ter omogočajo večjo kriptografsko prilagodljivost.

Drugi so nadaljnji koraki, ki temeljijo na pristopu, zasnovanem na oceni tveganj. To pomeni, da imajo pri prehodu na PQC prednost sektorji in sistemi z višjo stopnjo tveganja. Stopnja tveganja je odvisna od treh dejavnikov: ranljivosti obstoječe kriptografije, posledic njenega morebitnega zloma ter časa in napora, potrebnih za prehod na PQC. Kot visoko tvegani se obravnavajo entitete in sistemi, kjer bi razkritje podatkov tudi po desetih letih ali več povzročilo veliko škodo.

Na podlagi ocene tveganja načrt uvaja tudi tri mejnike. Do 31. 12. 2026 naj bodo izvedeni začetni koraki – sprejeti nacionalni načrti prehoda na PQC ter zagon pilotnih projektov. Do 31. 12. 2030 naj bo zaključen prehod na PQC za entitete z visokim tveganjem. Do 31. 12. 2035 pa naj bo zaključen prehod na PQC za vse ostale entitete.

Ker napredka pri razvoju kvantnih računalnikov ni mogoče z gotovostjo predvideti, obstaja realno tveganje, da se bodo roki za implementacijo posameznih ukrepov skrajšali. Organizacije se morajo zato pripraviti na t. i. kriptografsko agilnost – sposobnost hitre posodobitve algoritmov brez korenitih posegov v infrastrukturo.

Načrt poudarja tudi, da prehod na PQC ne pomeni nadomestitve obstoječih kriptografskih rešitev, temveč njihovo dopolnitev – t. i. hibridne kriptografske rešitve.

Je post-kvantna kriptografija že del vašega vsakdana?

Vsi načini uporabe kriptografskih algoritmov ne morejo z enako lahkoto preklopiti na post-kvantno kriptografijo. Implementacija PQC v osnovnih omrežnih protokolih, kot je varno sporočanje ali nekatere oblike šifriranega prenosa podatkov je običajno enostavnejša, zato že opažamo zgodnje sprejemanje algoritmov PQC v komunikacijskih protokolih. To omogoča boljšo zaščito varnega sporočanja in prenosa podatkov pred prihodnjimi kvantnimi napadi brez večjih motenj v delujočih sistemih.

Prehod na post-kvantno kriptografijo pri digitalnih potrdilih, ki preverjajo identiteto na spletu, na primer pri dostopu do varnih spletnih mest ali podpisovanju digitalnih dokumentov, je precej bolj zapleten. Pri tem ne gre za popolno zamenjavo obstoječih kriptografskih sistemov, temveč za njihovo dopolnitev in postopno nadgradnjo z rešitvami, odpornimi na prihodnje kvantne napade. Posodabljanje teh sistemov zato zahteva prilagoditve celotne infrastrukture javnih ključev, vključno s programsko in strojno opremo, ki ta potrdila izdaja, preverja in uporablja.

Slika 7: Shematski prikaz vsakdanjega uporabnika.

Poglejmo nekaj primerov komunikacijskih protokolov in internetnih brskalnikov, ki že ponujajo možnost uporabe algoritmov PQC.

Googlova kriptografska knjižnica, BoringSSL, podpira ML-KEM, kar pomeni, da ga lahko zdaj uporabljajo vse aplikacije, ki temeljijo na tej knjižnici. Različica spletnega brskalnika Chrome 131 že podpira ML-KEM, medtem ko so starejše različice podpirale hibridno izmenjavo ključev z algoritmom Kyber.

Apple je februarja 2024 napovedal nadgradnjo protokola iMessage, ki bo uporabljal hibridni protokol PQ3, odporen na napade s kvantnim računalnikom.

Aplikacija za sporočanje Signal je že septembra 2023 implementirala protokol PQDXK, ki prav tako uporablja algoritem Kyber.

PQC algoritmi so prisotni tudi že v mnogih drugih produktih, od oblaka do varne komunikacije:

Priporočeni prvi koraki organizacij za prihodnost s PQC

Splošno priporočilo za prehod na PQC za vse organizacije je čim prejšnji popis vseh kriptografskih rešitev, ki so v uporabi.

Sam postopek popisa kriptografskih rešitev je ključen prvi korak v strategiji prehoda na kvantno varno kriptografijo, saj organizacijam omogoča natančen vpogled v to, kateri podatki, komunikacijski kanali in aplikacije so najbolj izpostavljeni tveganjem »shrani zdaj, dešifriraj pozneje« (ang. Harvest Now, Decrypt Later).

Sam postopek popisa kriptografskih rešitev običajno vključuje naslednje korake:

- Identifikacija algoritmov: iskanje vseh mest, kjer se uporabljajo asimetrični algoritmi (kot sta RSA in ECC), ki so ranljivi na napade s kvantnimi računalniki.
- Analiza podatkovnih tokov: ugotavljanje, kateri občutljivi podatki se prenašajo prek omrežij in kje so shranjeni v šifrirani obliki.
- Ocena življenjske dobe podatkov: določanje prioritet glede na to, kako dolgo morajo podatki ostati zaupni (podatki z dolgo življenjsko dobo potrebujejo hitrejšo migracijo).
- Preverjanje odvisnosti: popis zunanjih knjižnic, ponudnikov v oblaku in strojne opreme, ki podpirajo trenutne kriptografske standarde.

Brez celovitega seznama CBOM (ang. Cryptography Bill of Materials) organizacije ne morejo učinkovito načrtovati kriptografske agilnosti — sposobnosti hitre zamenjave algoritmov brez korenitih posegov v infrastrukturo, ko bodo standardi PQC popolnoma uveljavljeni.