Hibridni certifikati post-kvantne kriptografije

Nastja Cepak,[1,2] Jakob Matek[1]

[1] CREAPLUS d.o.o., Ljubljana, Slovenija
nastja.cepak@creplaus.com, jakob.matek@creaplus.com

[2] Univerza na Primorskem, Fakulteta za naravoslovje, informacijske tehnologije in informatiko, Koper, Slovenija
nastja.cepak@creplaus.com

Kvantni računalniki obetajo omogočiti izračune, ki jim niso kos niti današnji najmočnejši super računalniki. Razvoj kvantnih računalnikov in algoritmov pa bo tudi dosegel razvojno stopnjo, ko obstoječi varnostni mehanizmi ne bodo več nudili zaščite podatkov in digitalnega zaupanja. Pričakujemo, da se bomo v obdobju tranzicije s tradicionalnih asimetričnih kriptografskih algoritmov (RSA in ECC) na post-kvantne algoritme posluževali tako imenovanih »hibridnih rešitev«, torej rešitev, ki hkrati podpirajo klasično in post-kvantno kriptografijo. V prispevku se bomo osredotočili na hibridne digitalne certifikate in bomo prikazali, kako lahko integriramo post-kvantne algoritme v x509 format digitalnih certifikatov.

Ključne besede:
kvantno računalništvo
post-kvantna kriptografija
crytsals-dilithium
digitalna potrdila
hibridna potrdila

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-772-0
DOI https://doi.org/10.18690/um.feri.8.2023.3

1 Uvod

Kvantna teorija je znanstveno področje, ki ponuja dober matematični model za opis narave na atomski in subatomski ravni. Na podlagi teh teorij in načel rase področje kvantnega računalništva. Kar se je včasih zdelo kot znanstvena fantastika, postaja naša resničnost. Njegovi začetki segajo približno 40 let v preteklost, ko je Paul Benioff leta 1980 opisal Turingov stroj s kvantno mehaniko [6]. Kmalu zatem, leta 1982, je Richard Feynman predlagal prvo praktično uporabo tovrstnih strojev – simulacijo kvantne mehanike [7], kar bi imelo velik vpliv na biologijo in kemijo.

Resnično zanimanje za kvantno računalništvo pa se je sprožilo leta 1994, ko je Peter Shor razvil algoritem, ki bi kvantnim računalnikom omogočil učinkovito faktorizacijo velikih celih števil. To je algoritem s potencialom razbijanja šifriranj RSA in ECC, algoritmov, na katera se zanašajo številni kriptosistemi. Namesto da bi za faktorizacijo 300-mestnega števila potrebovali milijone let, bi ga Shorov algoritem lahko faktoriziral v nekaj dnevih.

Kmalu zatem, leta 1996, je Lov Grover zasnoval Groverjev iskalni algoritem, ki omogoča uporabo kvantnih računalnikov za zagotavljanje kvadratne pospešitve iskanja v primerjavi s tradicionalnimi iskalnimi algoritmi. Prečesavanje celotnega prostora ključev v napadu s surovo silo, kjer iščemo šifrirni ključ, bi nenadoma postalo veliko lažje.

Za lažjo predstavo vpliva napadov s kvantnimi računalniki na danes uporabljene kriptografske algoritme prilagamo spodnjo tabelo 1.

Tabela 1: Število bitov varnosti asimetričnih in simetričnih algoritmov danes in ob uporabi Shorjevega/Groverjevega algoritma na dovolj zmogljivem kvantnem računalniku

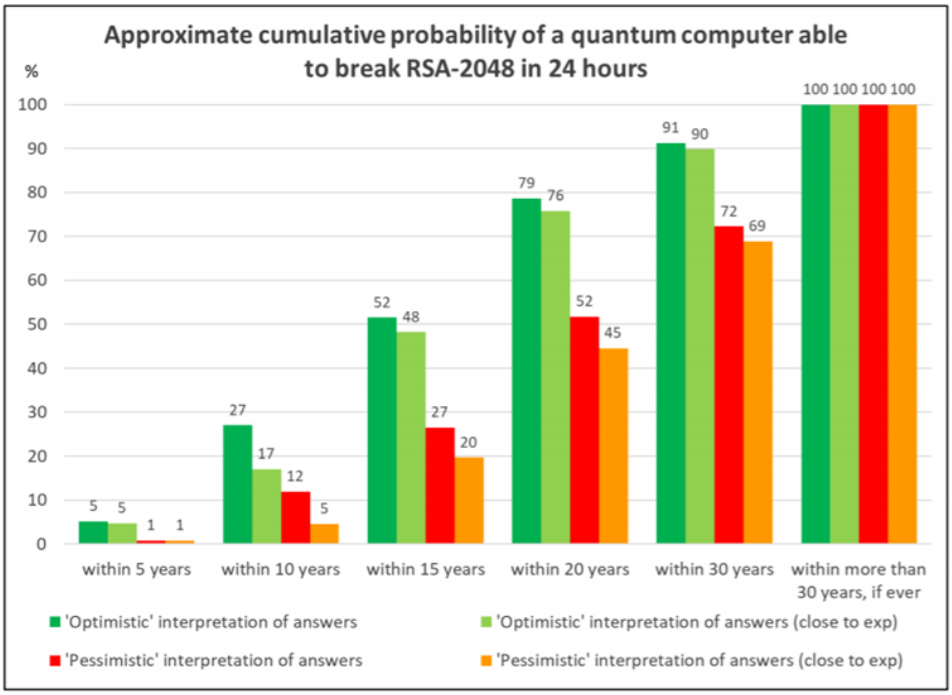
Algoritem	Število bitov varnosti (danes)	Število bitov varnosti z uporabo Shorjevega/Groverjevega algoritma na kvantnem računalniku
RSA-1024	80	0
RSA-2048	112	0
ECC-256	128	0
ECC-384	256	0
AES-128	128	64
AES-256	256	128

Kvantni računalniki nenadoma niso bili samo predmet akademske radovednosti, temveč dobro financirane vladne in zasebne raziskave. Napredek, ki je sledil v naslednjih desetletjih, je odraz na novo ustvarjenega zanimanja. Trenutno eno vodilnih podjetij na kvantnem področju, IBM, napoveduje za leto 2023 otvoritev 1121-qbitnega procesorja Condor, pripravljen pa imajo tudi načrt za hitro višanje števila qbitov v naslednjih letih, do leta 2026 [8].

Takoj se postavi sledeče očitno in pomembno vprašanja: Kdaj bodo obstajali kvantni računalniki, ki bodo lahko, na primer, dovolj zmogljivi, da bi zaganjali Shorjev algoritem, ki bo lahko razbil algoritem RSA-2048? Leta 2019 sta Michele Mosca in Marco Piani napisala poročilo o časovnem načrtu kvantne grožnje za Global Risk Institute [10]. Poročilo vključuje anketo, izvedeno med 22 vodilnimi mednarodnimi strokovnjaki za raziskave kvantnega računalništva. Eno od vprašanj v anketi je bilo navesti verjetnost, da bo kvantnemu računalniku uspelo razbiti RSA-2048 v 24 urah v 5/10/15/20/30/30+ letih. Na sliki 1 so prikazane približne vrednosti prejetih odgovorov.

Vidimo, da čeprav obstaja le malo prepričanja, da nas bo grožnja kvantnega napada v naslednjih nekaj letih ujela nepripravljene, se ideja, da bo v naslednjih 20 letih obstajal kvantni računalnik, ki bo lahko zlomil naše varnostne algoritme, zdi precej verjetna. Za ohranitev naše digitalne varnosti v prihodnosti so raziskovalne ustanove že pred več kot desetletjem začele razvijati kvantno odporne kriptografske algoritme. Trenutno najboljši od tako

imenovanih algoritmov za postkvantno kriptografijo (Post Quantum Cryptography - PQC) tekmujejo za kvalifikacijo za NIST (National Institute for Standards and Technology, ZDA) standardizacijo v okviru projekta "Post-Quantum Cryptography Standardization" [11].



Slika 1: Kumulativna verjetnost za obstoj kvantnega računalnika, ki bi lahko zlomil RSA-2048 v 24 urah
Vir: [10].

2 Post-kvantna kriptografija

Ko govorimo o algoritmih post-kvantne kriptografije, govorimo o asimetirčnih algoritmih, ki jih zaganjamo na standardnih digitalnih računalnikih, kot jih poznamo danes, hkrati pa so odporni tako na tradicionalne napade, kot na napade, ki bi se jih zaganjalo na kvantnih računalnikih. Njihov namen je, da v prihodnosti zamenjajo algoritma RSA in ECC.

Proces standardizacije post-kvantne kriptografije NIST se je začel konec leta 2016 z javnim pozivom NIST za oddajo predlogov. Novembra 2017 je bil rok za oddajo predlogov algoritmov. Od 82 predloženih kandidatov je bilo 13 skoraj takoj zlomljenih ali pa so vsebovali drugačne pomanjkljivosti. Tako je bilo decembra 2017 v prvi izbirni krog sprejetih skupno 69 kandidatov. Nekaj mesecev za tem, aprila 2018, je potekala 1. standardizacijska konferenca NIST PQC, kjer so o algoritmih in potencialnih napadih nanje razpravljali raziskovalci iz NIST in širše akademske skupnosti. V začetku leta 2019 je bilo izbranih 26 kandidatov za nadaljevanje v 2. krog, čemur je sledila 2. konferenca o standardizaciji NIST PQC, ki je potekala še isto poletje. 22. julija 2020 je bilo razglašenih 7 finalistov 3. kroga. NIST je tudi javno objavil poročilo o izbirnem postopku. Končno, 5. julija 2022, so bili objavljeni štirje algoritme, ki bodo standardizirani, in kandidati za četrti krog. Končnih standardov še nimamo, pričakujemo pa jih začetek leta 2024.

Ena od omejitev, ki jih še nismo uspeli preseči pri algoritmih post-kvantne kriptografije, je, da algoritmi (še) niso dovolj prilagodljivih, da bi hrkati lahko učinkovito izvajali operacije šifriranja z javnim ključem in digitalnega podpisovanja. Zato je tekmovanje ločeno na 2 kategoriji, kot je prikazano v tabeli 2.

Tabela 2: Finalisti in kandidati za 4. krog NIST PQC tekmovanja.

	Šifriranje z javnim ključem	Digitalni podpisi
Finalisti, ki bodo standardizirani	CRYSTALS-KYBER	CRYSTALS-DILITHIUM FALCON SPHINCS+
Kandidati za 4. krog	BIKE Classic McEliece HQC	/

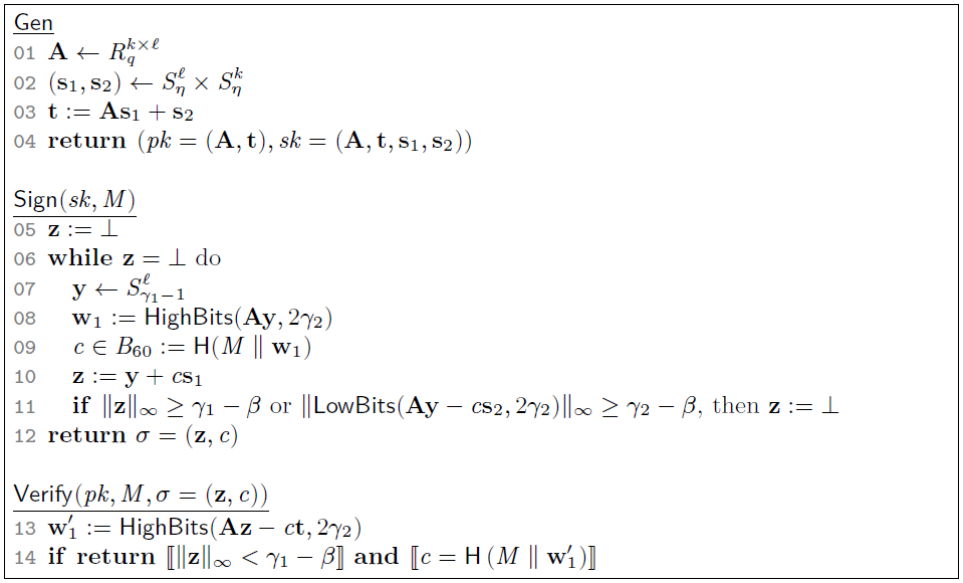
Kot pripombo bi dodali, da je tehnično gledano še vedno kandidat za 4. krog tudi algoritem SIKE (šifriranje z javnim ključem), vendar je bil avgusta 2022 zlomljen na način, da manjši popravki niso dovolj za varno delovanje. Zaradi tega ga nismo dodali v tabelo.

Zanimanje našega projekta leži v digitalnih certifikatih in njihovi hibridiziraciji, torej postopku, ki tradicionalnemu certifikatu doda post-kvantno komponento. Zaradi tega smo se osredotočili na algoritem CRYSTALS-DILITHIUM, ali na kratko, Dilithium. Je najbolj priporočen algoritem za implementacijo PQ digitalnih certifikatov [12].

2.1 CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM je asimetrični kriptografski algoritem za digitalno podpisovanje, ki je odporen tako na tradicionalne napade, kot na napade, ki bi jih lahko zaganjali na kvantnem računalniku. Prvič je bil uradno definiran leta 2017 [13, 14] kot prijava v prvi krog NIST PQC tekmovanja. CRYSTALS ekipa je v tistem času definirala dva algoritma: CRYSTALS-DILITHIUM, ki je namenjen digitalnemu podpisovanju in čigar ime je referenca na material dilithium iz Star Treka. Drugi algoritem, ki je bil prav tako izbran za standardizacijo, je CRYSTALS-KYBER, namenjen šifriranju in z imenom, ki je referenca na kyber kristal iz Star Wars.

Kot opisano v [13], Dilithium temelji na težavnosti problema iskanja kratkih vektorjev v mrežah. Zasnova sheme temelji na pristopu "Fiat-Shamir with Aborts" [15], ki z zavračanjem vzorcev (rejection sampling) poskrbi, da je Fiat-Shamir shema bolj kompaktna in varnejša. Za lažje ne-matematično razumevanje algoritma prilagamo sliko 2 s pseudokodo funkcionalnosti. Pri implementaciji hibridnih certifikatov uporabljamo vse tri funkcionalnosti (generacijo ključa, podpisovanje, verificiranje).



Slika 2: Preudokoda funkcionalnosti Dilithium algoritma
Vir: [13].

3 Digitalni certifikati

Digitalno certifikat je oblika elektronske poverilnice, ki lahko dokaže pristnost uporabnika, naprave, strežnika, spletne strani ali katerekoli druge entitete. Uporablja tako imenovano infrastrukturo javnih ključev (Public Key Infrastructure), ki jo bomo za voljo koherentnosti članka tu le na kratko opisali, za varno izmenjavo komunikacij in podatkov prek interneta in drugih omrežij.

Ta oblika avtentikacije je vrsta kriptografije, ki zahteva uporabo javnih in zasebnih ključev, ki enolično pripadata eden drugemu, za preverjanje identitete uporabnikov. Digitalne certifikate izdajo zaupanja vredne tretje osebe (Certificate Authority, v nadaljevanju tudi CA), ki podpiše potrdilo in tako preveri identiteto naprave ali uporabnika, ki zahteva dostop. Za zagotovitev veljavnosti bo javni ključ usklajen z ustreznim zasebnim ključem, ki ga pozna samo prejemnik. Digitalna potrdila imajo določen par ključev, s katerim so povezana: enega javnega in enega zasebnega.

Danes so tako rekoč vse postavljene PKI infrastrukture uporabljajo ali RSA algoritem, ali ECC algoritem, ki pa bosta zlomljena s prihodom dovolj zmogljivega kvantnega računalnika. Naj hitro opišemo nekaj primerov uporabe, s katerimi se srečujemo vsak dan in pri katerih stojijo v ozadju digitalni certifikati, da bolje razumemo, zakaj iščemo načine, da ostanejo varni tudi po prihodu kvantnih računalnikov.

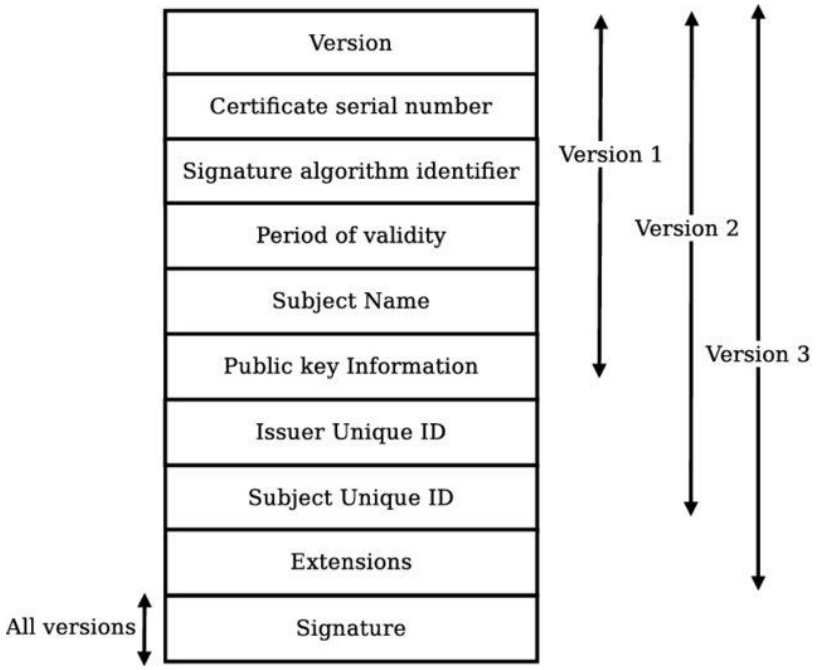
Na naši novi elektronski osebni izkaznici so nameščeni trije digitalni certifikati za različne namene uporabe. Ko se prijavljate v online banko, je velika možnost, da za vašo prijavo stoji digitalni certifikat. Ko se povezujete na spletno stran, se velik del spletnih strani v ozadju najprej identificira vašemu brskalniku, da pokažejo, da so varne. Ko nameščate novo programsko opremo, je ta običajno podpisana z zasebnim ključem proizvajalca. Če vaš operacijski sistem prepozna odgovarjajoči digitalni certifikat, bo samodejno zaupal tudi podpisani kodi.

Glavno vprašanje, ki ga želimo nasloviti, je sledeče. Do časa, ko bodo aplikacije namesto RSA in ECC uporabljale izključno PQC standardizirane algoritme, bo minilo še kar nekaj časa. Po priporočilih ZDA [12], Nemčije [16] in Francije [17] bi se sicer ta preskok moral zgoditi v prvi polovici 30. let (2030-2035). V vmesnem obdobju bomo potrebovali digitalne certifikate, s katerimi bomo lahko hkrati upravljali tradicionalne/legacy kriptografske aplikacije, hkrati pa se bomo lahko identificirali novim aplikacijam, ki podpirajo prioritetno ali izključno PQC algoritme. Kako takšne hibridne certifikate učinkovito zasnovati?

3.1 Hibridni certifikati

V magistrski nalogi leta 2020 Univerze v Barceloni [9] so bili zelo jasno predstavljeni 4 različni pristopi k hibridizaciji digitalnih potrdil. Vse štiri bomo površinsko predstavili, za našo implementacijo pa smo uporabili mešanico pristopa z ugnezdenimi certifikati in pristopa razširitev po meri. Cilj je modificirati standardiziran x509 certifikat na takšen način, da sta v praksi v njemu vključena 2 certifikata: prvi, ki vsebuje podpis s tradicionalnimi kriptografskimi algoritmi, in drugi, ki vsebuje post-kvantni podpis. Hkrati želimo, da certifikat ohranja dovolj uniformno obliko, da je kompatibilen s trenutno uveljavljenimi CA strukturami.

Osnovna struktura x509 certifikata je opisana na sliki 2.



Slika 2: Struktura x509 certifikata
Vir: [18].

3.1.1 Dualni certifikati

Najpreprostejša metoda hibridizacije je izdaja dveh potrdil, ki sta nato vedno predstavljeni v paru. Prvo potrdilo je izdano z uporabo tradicionalnega algoritma, drugo pa z uporabo post-kvantnega [19]. Obe sta podpisani z istim CA sistemom, vendar z uporabo drugačne sheme podpisovanja (konvencionalne oziroma PQ). Pomanjkljivost te metode je, da imata lahko potrdili drugačne datume veljavnosti ter da je potrebno njuno ločeno upravljanje. Vsi sistemi morajo vzdrževati obe različici potrdila in velikost datoteke skupnega certifikata je večja zaradi podvojenih informacij in parametrov.

3.1.2 Konkatenacija

Ideja konkatenacije certifikatov prihaja iz projekta Open Quantum Safe [20]. Uvedemo lahko nov identifikator objekta OID (Object Identifier), ki predstavlja, na primer, kombinacijo algoritmov RSA in Dilithium. Nato konkateniramo bajtna zapisa obeh javnih ključev v en velik javni ključ, ki ga nato lahko zapišemo v x509 certifikat. Če takšen certifikat nato obdeluje programska oprema, ki prepozna naš novi OID, natanko ve, kaj mora narediti z velikim javnim ključem - kako ga razbiti na dva ločena javna ključa in nato po potrebi uporabljati ali RSA, ali Dilithium. Čeprav je ta pristop združljiv z x509 standardom, ni združljiv s starejšimi aplikacijami, ker te ne prepoznavajo nove OID oznake.

3.1.3 Ugnezdeni certifikati

Drugačna različica dualnih potrdil je gnezdenje enega potrdila znotraj drugega potrdila ko razširitev po meri [21]. Najprej ustvarimo potrdilo z javnim post-kvantnim ključem in generiramo post-kvantni podpis, ki ga obravnavamo kot notranji certifikat. Nato ustvarimo potrdilo s tradicionalnim javnim ključem, ki predstavlja zunanje potrdilo, bajtni zapis notranjega potrdila pa je shranjen v razširitvi po meri zunanjega potrdila.

Pri tem pristopu se podatki o predmetu še vedno podvajajo, vendar je celotno potrdilo združljivo s starejšimi aplikacijami, če je razširitev označena kot nekritična. Starejša programska oprema ignorira razširitev po meri z notranjim post-kvantnim potrdilom in preveri le zunanje tradicionalno potrdilo.

Za realizacijo tega pristopa v širšem kontekstu programske opreme, ki jo zahteva uporaba infrastrukture javnih ključev, sta potrebni dve certifikacijski avtoriteti. Ena za izdajo in verifikacijo post-kvantnih certifikatov in druga za tradicionalne algoritme. S certifikatoma morata podvojeno upravljati obe avtoriteti.

3.1.4 Razširitve po meri

Pristop razširitve po meri je zelo podoben gnezdenju certifikatov. Da bi se izognili dodatnim stroškom podvojenih predmetnih polj, je bilo predlagano samo hranjenje dodatnega javnega ključa in dodatnega podpisa v dveh po meri razširitvah [21]. To prinaša sicer tudi nekaj pomanjkljivosti.

Za realizacijo tega pristopa v infrastrukturi javnih ključev je potrebna ena certifikacijska avtoriteta, ki zna upravljati tako s podpisi post-kvantnih algoritmov, kot s konvencionalnimi RSA podpisi. Upravljanje s certifikati je v tem primeru lažje.

4 Implementacija

Cilj projekta je implementirati sistem, ki ga je mogoče dodati k že obstoječi infrastrukturi javnih ključev z minimalnimi spremembami. Za ta namen sta primerna le dva od omenjenih pristopov hibridizacije certifikatov v poglavju 3.

Pristop dualni certifikati (3.1.1) bi zaradi popolne ločitve konvencionalnih in PQ certifikatov omogočal postavitev vzporedne infrastrukture javnih ključev, ki bi temeljila na PQ algoritmih. Enako bi omogočal tudi pristop ugnezdenih certifikatov (3.1.3). Da pa bi se izognili lastnosti velikih datotek, ki jih prinese slednji in lastnosti razdružljivosti PQ in konvencionalnih certifikatov v pristopu dualnih certifikatov (3.1.1), smo združili pristop ugnezdenih s pristopom razširitev po meri (3.1.4).

Velikost certifikatov smo nekoliko zmanjšali z idejo deljenih x509 atributov med PQ in konvencionalnim podpisom. Med tem, ko so v pristopu ugnezdenih certifikatov vsi atributi podvojeni, smo podvojili le x509 atribute, ki jih na certifikat doda certifikacijska avtoriteta. Ne-razdružljivost pa je zagotovljena z uporabo x509 razširitev po meri (custom extensions).

Z našim mešanim pristopom lahko PQ del samostojno predstavlja svoj podpis, iz hibridnega certifikata pa je nemogoče izvleči posamezne dele podatke/ključe/podpis na ta način, da bi lahko dobili samostojen tradicionalni certifikat. To je želena lastnost, ker je na tak način hibridnemu certifikatu nemogoče odvzeti PQ del, kar bi znižalo pričakovano varnost hibridnega certifikata.

4.1 Orodja

Za postavitev testne infrastrukture javnih ključev smo postavili enostavno certifikacijsko avtoriteto z uporabo OpenSSL 3.0.7, v nadaljevanju CA. Orodje OpenSSL je uporabljeno za generacijo CA ključa in certifikata ter za nadaljnjo izdajanje uporabniških certifikatov. V konfiguraciji CA je potrebno omogoči razširitve po meri, ki jih uporabljamo za gnezdenje PQC vsebine v x509 certifikat.

Za postavitev alternativne PQC certifikacijske avtoritete, v nadaljevanju PQCA, smo razvili orodje HCTool (4.2), ki je med drugim sposobno generirati PQC del certifikata in ga vgraditi v konvencionalno CSR zahtevo, ki je nato poslana na CA.

4.2 Orodje za upravljanje s hibridnimi certifikati HCTool

HCTool je orodje, ki smo ga razvili za upravljanje s hibridnimi certifikati. Orodje ja napisano v Python jeziku, ki smo ga za izbrali zaradi že obstoječih knjižnic in kompatibilnostjo z različnimi operacijskimi sistemi. Uporabili smo različico Python 3.10.5.

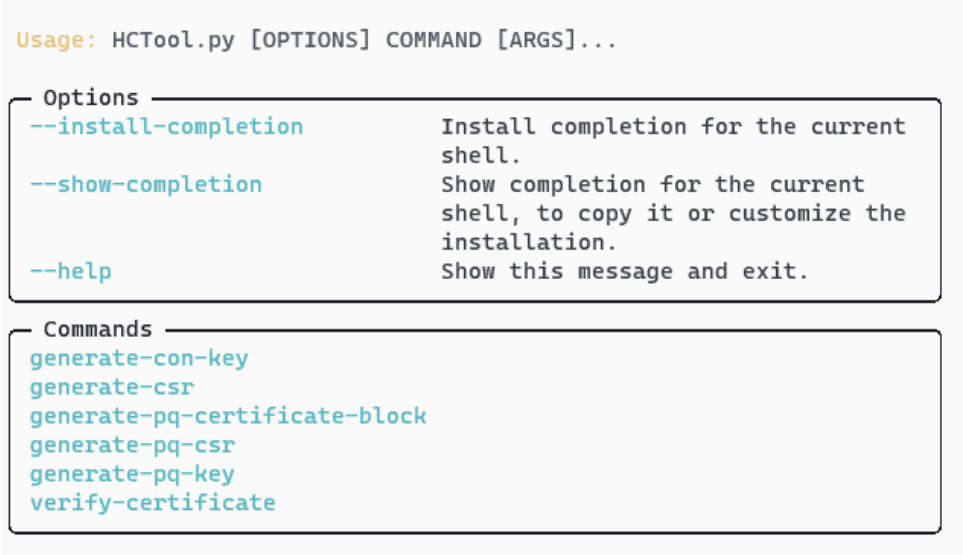
Za delo s konvencionalnimi šifrirnimi algoritmi, certifikacijskimi zahtevami in x509 certifikati smo uporabili knjižnico cryptography [23].

Za delo s PQC algoritmi smo uporabili knjižnico liboqs-python [24] različico 0.8.0, ki je del Open Quantum Safe Projekta [25].

Za uporabo ustvarjenih Python funkcij preko CLI vmesnika, smo uporabili knjižnico Typer [26] različico 0.9.0.

Implementirali smo sledeče funkcije:

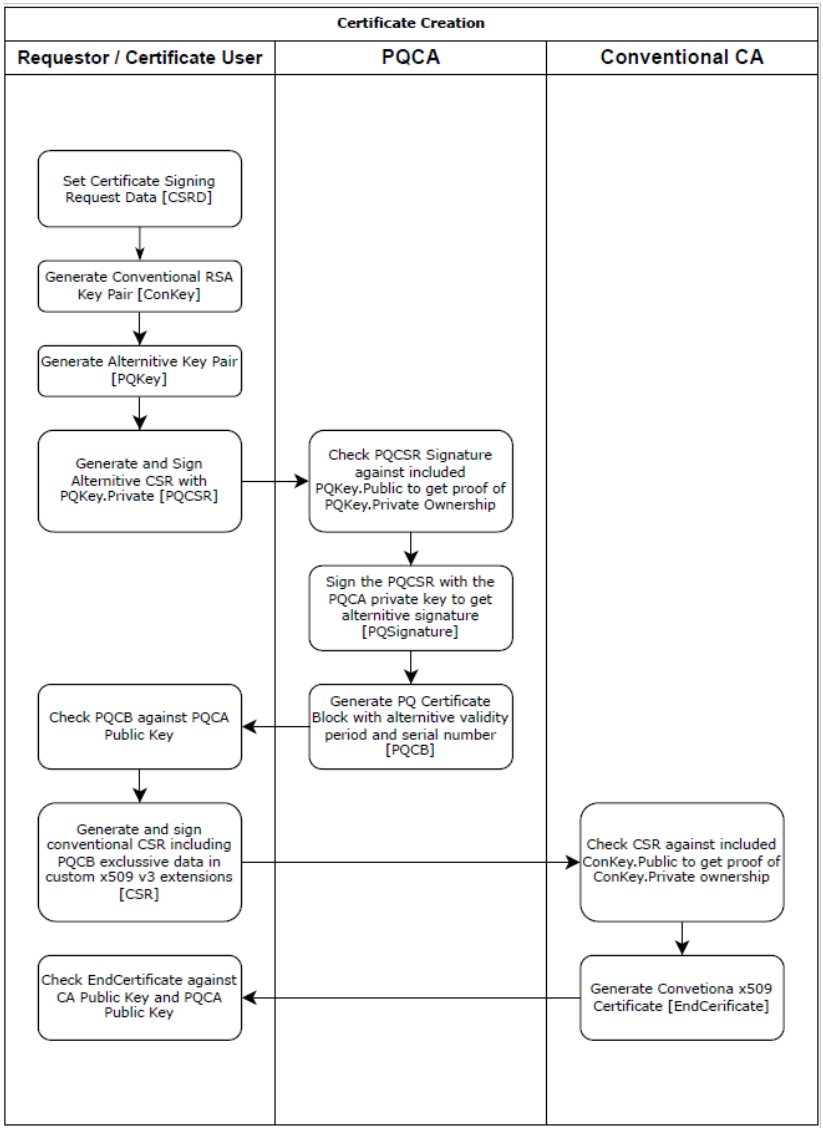
- Generate_PQ_Key(algorithm, passphrase, outDir) --> Par PQC ključev
  Ustvari par ključev z izbranim PQ algoritmom.
- Generate_Con_Key(algorithm, passphrase, outDir) --> Par RSA ali EC ključev
  Ustvari par ključev z izbranim konvencionalnim algoritmom.
- Generate_PQ_CSR(PQKey, ConKey.Public, SubjectData) --> PQCSR zahteva
  Sestavi PQCSRzahtevo, opisano v poglavju 4.3.
- Generate_PQ_Cerificate_Block(PQCSR, PQKey.Public, IssuerData) --> PQCB
  Podpiše PQCSR in sestavi PQCB certifikat, opisan v 4.3.
- Verify_PQ_Certificate_Link(PQCB, PQKey.Pub) --> bool
  Preveri, ali je bil certifikat PQCB podpisan s privatnim ključem, ki pripada ključu PQKey.Public.
- Generate_CSR(PQCB, ConKey.Private) --> x509 CSR
  Ustvari konvencionalno x509 CSR zahtevo.
- Verify_Certificate(Certificate, IssuerCertificate, PQIssuerCertificate) -> bool
  Preveri, ali je hibridni certifikat podpisan s podanim PQ cerifikatom in/ali je podpisan s podanim konvencionalnim certifikatom.



Slika 3: HCTool orodje

4.3 Izdajanje hibridnega certifikata

Proces izdajanja hibridnega certifikata je ponazorjen na sliki 4.



Slika 4: Proces izdajanja hibridnega certifikata

Za lažje razumevanje oznak v nadaljevanju dodajamo opombo, da so uporabljeni izrazi kot so Issuer, Validity, Serial, CA, CSR, TBS, itd. uporabljeni v kontekstu x509 standarda in konvencionalne infrastrukture javnih ključev (PKI). Ko želimo poudariti, da so Issuer, Validity, CA, itd vezani na post-kvantni del izdaje certifikata, je dodana predpona PQ (npr. PQCSR, PQCA, PQTBS, itd.).

Za izdajanje hibridnega certifikata je uporabljeno orodje HCTool. Uporabnik, ki zahteva certifikat (requestor) najprej ustvari par konvencionalnih ključev, v nadaljevanju ConKey (ConKey.Private in ConKey.Public) in par ključev, ki temelji na PQC algoritmih, v nadaljevanju PQKey (PQKey.Public in PQKey.Private). Istočasno se tudi odloči za algoritme samih ključev. Podprti so konvencionalni algoritmi RSA in EC ter sledeči PQC algoritmi:

- Dilithium 2, 3 in 5,
- Falcon 512 in 1024,
- SPHINCS+ s Haraka, SHA in SHAKE zgoščevalnimi (hash) algoritmi.

Uporabnik nato določi x509 atribute, ki bodo vstavljeni v CSR zahtevo. S pomočjo orodja HCTool nato ustvari PQCSR, torej zahtevo za podpis s PQC algoritmom, ki ga izda PQCA. Zahteva je sestavljena iz podatkov o subjektu, javnim ključem konvencionalnega algoritma, javnim ključem PQC algoritma in dodatnih x509 razširitev, ki so želene v končnem certifikatu. Ti podatki so konkatenirani in podpisani s PQC privatnim ključem PQKey.Private. Podpis, v nadaljevanju PQCSR.Signatue, je dodan v PQCSR.

PQCSR zahteva je nato poslana na PQCA za podpis. PQCA preveri PQCSR.Signature podpis s podatki v PQCSR in javnim ključem PQKey.Public, ki ga zahteva vsebuje. Uspešno preverjen podpis dokazuje, da si subjekt, ki certifikat zahteva, tudi lasti privatni ključ PQKey.Private. V primeru neuspešno preverjenega podpisa PQCSR:Signature, PQCA zavrne zahtevo. V nasprotnem primeru PQCA določi alternativno veljavnost certifikata, v nadaljevanju PQValidity, določi atribut PQIssuer, ki identificira PQCA, in PQSerial, ki je številka uporabljena za upravljanje s certifikati.

Nato PQCA sestavi podatke, ki bodo podpisani, v nadaljevanju PQTBS (to be signed). PQTBS podatki so sestavljeni iz vseh podatkov, ki so vključeni v PQCSR, razen PQCSR.Signature. V PQTBS so dodani atributi PQValidity, PQIssuer, PQSerial. PQTBS podatki so nato podpisani s privatnim ključem PQCA (PQCA.PQKey.Private). Podpis, v nadaljevanju PQSignature, in PQTBS podatki so združeni v "PQ Certifikat", v nadaljevanju PQCB (PQ Certificate Block), in poslani uporabniku, ki je zahteval certifikat.

Uporabnik nato preveri PQSignature podpis s podatki v PQCB in v naprej deljenem PQ certifikatu, ki pripada PQCA avtoriteti. V primeru uspešnega preverjanja uporabnik sestavi konvencionalno x509 CSR zahtevo. Zahteva je sestavljena v skladu z x509 standardom s podatki, ki so bili določeni za PQCSR. PQKey.Public in podatki, ki so bili dodani v PQCB s strani PQCA so dodani v konvencionalno zahtevo kot razširitve po meri (Custom x509 extensions). CSR zahteva je nato poslana na konvencionalno certifikacijsko avtoriteto (CA).

CA nato preveri podpis v CSR zahtevi in v primeru uspešnega preverjanja izda x509 certifikat, ki je poslan uporabniku. Uspešno preverjen podpis dokazuje, da si uporabnik, ki zahteva certifikat, tudi lasti ConKey.Private. Politika na CA je nastavljena tako, da se razširitve po meri, ki so vključene v CSR, kopirajo v certifikat.

OID številke uporabljene za x509 razširitve po meri so nanizane v Tabeli 3.

Tabela 3: Uporabljene OID številke.

OID	Vrednost
0.0.0.1	Alternativni PQC Algoritem
0.0.0.2	Alternativni PQC Javni Ključ
0.0.0.3	Alternativna Veljavnost
0.0.0.4	Alternativni Izdajatelj (Issuer)
0.0.0.5	Alternativna Serijska Številka
0.0.0.6	Alternativni PQC Podpis

5 Zaključek

V članku smo opisali postopek generacije hibridnega certifikata, ki ga je mogoče integrirati z obstoječim tradicionalnim PKI sistemom. Razvito je bilo orodje HCTool, ki s pomočjo PQC in konvencionalnih kriptografskih knjižnic omogoča upravljanje hibridnih certifikatov. V prihodnje načrtujemo integracijo orodja v manjše aplikativne projekte ter benchmark različnih implementacij kot del real-life rešitev.

Literatura

[1] Sodobne tehnologije in storitve OTS 2022: Zbornik petindvajsete konference. Maribor 2022.

[2] PODGORELEC Vili, HERICKO Marjan »Estimating software complexity from UML models », SIGSOFT Software Engineering Notes, letnik 32, številka 2, marec 2007, str. 31-38.

[3] JOSEPH David, MISOCZKI Rafael, MANZANO Marc, et.al. »Transitioning organizations to post-quantum cryptography », Nature 605, 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2

[4] ALAGIC Gorjan, APON Daniel, COOPER David, et.al. »Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process«, NIST, Julij 2022, https://doi.org/10.6028/NIST.IR.8413-upd1

[5] SCHEIBLE Patrik »Quantum Resistant Authenticated Key Exchange for OPC UA using Hybrid X.509 Certificates«, Master thesis, UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONA, april 2022, http://hdl.handle.net/2117/191775

[6] Paul BENIOFF »The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines«. Journal of Statistical Physics, 22 (5), 1980, 563–591.

[7] Richard FEYNMAN »Simulating Physics with Computers«. International Journal of Theoretical Physics «. 21 (6/7), 1982, 467–488.

[8] IBM's Roadmap For Scaling Quantum Technology https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

[9] SCHEIBLE Patrik »Quantum Resistant Authenticated Key Exchange for OPC UA using Hybrid X.509 Certificates», magistrska naloga, UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH, Barcelona, 2020 https://upcommons.upc.edu/bitstream/handle/2117/191775/thesis_patrik_scheible.pdf?sequence=1

[10] MOSCA Michele, PIANI Marco » Quantum Threat Timeline « October 2019 https://globalriskinstitute.org/publications/quantum-threat-timeline/

[11] Post-Quantum Cryptography Standardization https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[12] Announcing the Commercial National Security Algorithm Suite 2.0 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[13] DUCAS Léo, KILTZ Eike, LEPOINT Tancrède et al. »CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme«, IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 238-268

[14] Official "CRYSTALS - Cryptographic Suite for Algebraic Lattices" webpage https://pq-crystals.org/dilithium/resources.shtml

[15] LYUBASHEVSKY Vadim »Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures« ASIACRYPT, pp. 598–616, 2009. 2, 20

[16] https://dserver.bundestag.de/btd/19/252/1925208.pdf

[17] ANSSI views on the Post-Quantum Cryptography transition https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

[18] X.509 Public Key Certificates, Microsoft https://learn.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates

[19] BINDEL Nina, HERATH Udyani, MCKAGUE Matthew, STEBILA Douglas »Transitioning to a Quantum-Resistant Public Key Infrastructure« Post-Quantum Cryptography, Springer International Publishing, 2017, pp. 384–405, isbn: 978-3-319-59879-6

[20] STEBILA Douglas, MOSCA Michele »Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project« Lecture Notes in Computer Science, 2017, DOI: 10.1007/978-3-319-69453-5_2

[21] BINDEL Nina, BRAUN Johannes, GLADIATOR Luca, STOCKERT Tobias, WIRTH Johannes »X.509-Compliant Hybrid Certificates for the Post-Quantum Transition« Journal of Open Source Software, vol. 4, no. 40, p. 1606, 2019, issn: 2475-9066. doi: 10.21105/joss.01606.

[22] GLADIATOR Luca, »Hybrid Certificates in OpenSSL«, GitHub, 2019. [Online]. Available: https://github.com/CROSSINGTUD/openssl-hybrid-certificates/blob/OQS-OpenSSL_1_1_1-stable/HybridCert_technical_documentation.pdf

[23] Python knjižnica "Cryptography": https://cryptography.io/en/

[24] Python knjižnica "liboqs-python": https://github.com/open-quantum-safe/liboqs-python/releases/tag/0.8.0

[25] "Open Quantum Safe" projekt: https://openquantumsafe.org/