Wyzwania dla PKI

Finiszuje – bazujący na blockchainie – projekt zdecentralizowanego PKI (DPKI) – ITU-T X.509 | ISO/IEC 9594-8 (X.509). Ogólna struktura węzła została ustalona, a większość ustaleń uzgodniona. Wprawdzie do końca prac jeszcze długa droga, ale warto poczekać, ponieważ w przypadku pomyślnej realizacji projektu bardzo wzrośnie wiarygodność certyfikatów, co znacząco powinno poprawić zaufanie do transakcji zawieranych w internecie.

Grzegorz Cenkier

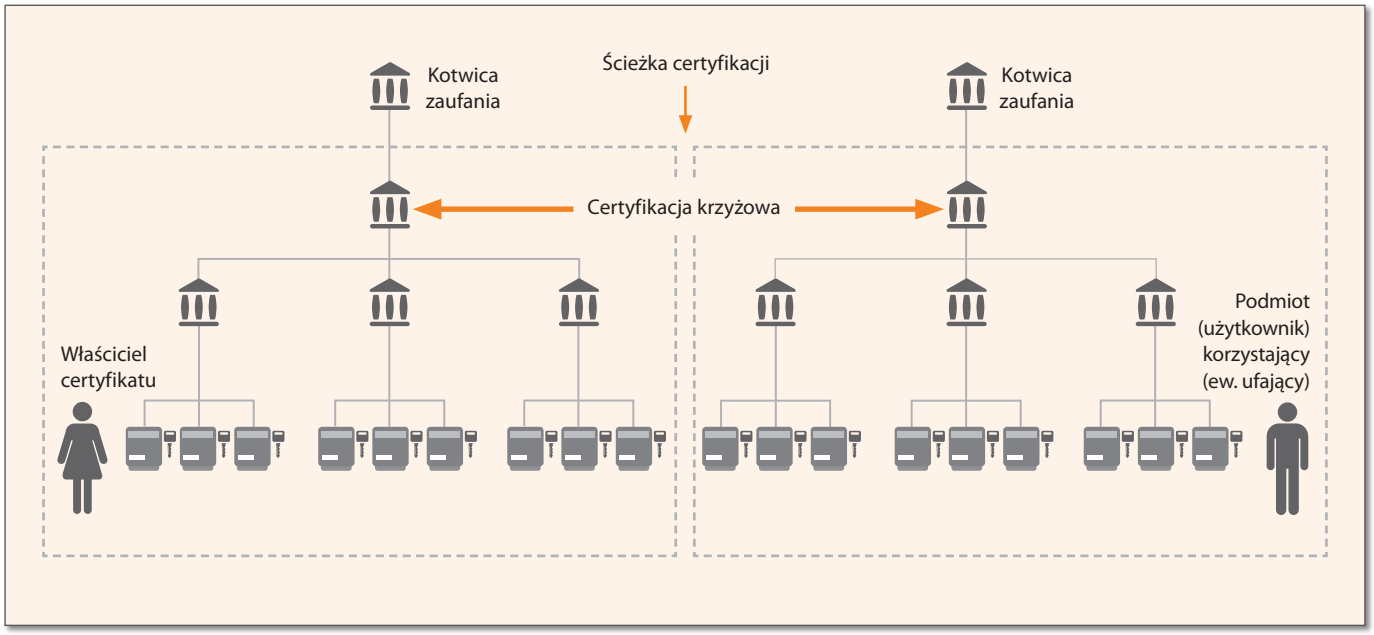
wieloletni pracownik Politechniki Warszawskiej, Instytutu Podstaw Informatyki PAN oraz instytucji finansowych i międzynarodowych systemu ONZ. Członek Zarządu ISSA Polska, Naczelnego Sądu Koleżeńskiego oraz Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego. Ekspert grupy roboczej w zakresie normalizacji: ISO/TC307/WG5 Governance, reprezentant w Komitecie Technicznym PKN 333 Blockchain i Technologii Rozproszonych Rejestrów.

Infrastruktura Klucza Publicznego (PKI – Public Key Infrastructure) to termin dzisiaj powszechnie znany. PKI to swojego rodzaju kryptosystem tworzący hierarchiczną strukturę zaufania, której podstawowym dokumentem jest certyfikat klucza publicznego. Nie wszyscy jednak wiedzą, że pod tym pojęciem kryje się standard X.509 opracowany przez Sektor Normalizacji Międzynarodowego Związku Telekomunikacyjnego – ITU-T w 1988 r. Obecnie obowiązuje trzecia wersja tego certyfikatu. Norma opisuje między innymi standardowe formaty certyfikatów oraz sposoby weryfikacji ścieżki certyfikacji, które pozwalają utworzyć infrastrukturę wiarygodnego potwierdzania tożsamości.

Zastosowania PKI są bardzo szerokie – od podpisywania poczty elektronicznej, poprzez zabezpieczania bankowości czy e-administracji, aż po bezpieczne metody uwierzytelniania. PKI jest przydatna także w innych obszarach, takich jak energetyka i Internet rzeczy (IoT). PKI dobrze sprawdziła się w krajach, w których zaufanie może zostać ustanowione przez tak zwaną kotwicę zaufania (urząd certyfikacji), której ufa każdy w domenie PKI. Jednak w dzisiejszym krajobrazie PKI wykracza poza granice pojedynczego urzędu certyfikacji w centrum danych. Jest to sieć zaufania, która obejmuje środowiska lokalne i chmurowe. Większość firm korzysta z wielu usług w chmurze (np. AWS, Azure, Google Cloud Platform), z których każda ma własne wbudowane możliwości wydawania certyfikatów. Infrastruktura PKI jest wdrażana w architekturach klastrowych, geograficznie redundantnych lub o wysokiej dostępności, aby zapewnić nieprzerwany czas odwoływania i wydawania certyfikatów, a środowiska kontenerowe wymagają krótkotrwałych certyfikatów SSL/TLS w porównaniu z tradycyjnymi serwerami internetowymi i urządzeniami, które mogą wykorzystywać certyfikaty długoterminowe.

Niektóre podejścia wykorzystują blockchain jako zdecentralizowany magazyn klucz-wartość dla PKI, ponieważ blockchain zapewnia bezpieczeństwo danych, minimalizuje wpływ stron trzecich i zapobiega atakom typu man-in-the-middle. I takie rozwiązanie bazujące na blockchainie – dla ustanowienia globalnego zaufania – zostało przyjęte w propozycji projektu zdecentralizowanego PKI – DPKI (Distributed PKI) – ITU-T X.509 | ISO/IEC 9594-8 (X.509). Rezultatem prac ma być międzynarodowy standard. Dlatego ze względów między innymi bezpieczeństwa nie może on bazować na istniejącej platformie blockchain – musi zostać szczegółowo określony bez bezpośredniego odniesienia do istniejących rozwiązań, ale może zawierać odniesienia do przyjętych koncepcji, takich jak bezpieczne protokoły konsensusu. Analiza istniejących technologii blockchain wykazała, że potrzebna jest inna platforma niż wykorzystująca konsensus Proof of Work (PoW), który znalazł zastosowanie w bitcoinie. Rozważana jest wersja platformy Hyperledger-Fabric, bo platforma ta bazuje na koncepcji globalnej bazy danych, w której DPKI dysponuje katalogiem przechowującym zaktualizowane informacje o statusie certyfikatu, dostępne globalnie dla użytkowników takich informacji (stron ufających).

Koncepcja urzędów certyfikacji (CA – Certifikate Authority) nie ulega zmianie, ponieważ CA są postrzegane jako znajdujące się poza zdecentralizowaną księgą, ale połą-



Połączona (Interconnected) domena PKI - Infrastruktury Klucza Publicznego

czone z nią za pomocą sieci blockchain. CA jest dołączony do węzła w księdze i reprezentowany przez ten węzeł. Informacje PKI, przede wszystkim wydane certyfikaty (certyfikaty klucza publicznego), są przekazywane do łańcucha bloków w celu ich walidacji przez węzły reprezentujące urzędy certyfikacji. Po pomyślnej weryfikacji certyfikaty są udostępniane we wszystkich węzłach sieci dla wszystkich stron ufających.

PKI a kryptografia postkwantowa

IBM czy HP od kilku lat obiecują, że w 2025 r. pojawią się komercyjne wersje komputerów kwantowych. Europa nie chce pozostać w tyle i dlatego Komisja Europejska podpisała umowy z sześcioma ośrodkami naukowymi z krajów europejskich: Polski, Włoch, Hiszpanii, Francji, Niemiec i Republiki Czeskiej na uruchomienie komputerów kwantowych w Europie, które mają działać od 2025 r. EuroQCS-POLAND będzie zlokalizowany w Poznańskim Centrum Superkomputerowo-Sieciowym (PCSS) i będzie zintegrowany z infrastrukturą Centrum.

W październiku 2023 r. Fińskie Centrum Badań Technicznych VTT oraz europejski producent komputerów kwantowych, IQM Quantum Computers, ukończyły budowę drugiego fińskiego komputera kwantowego. Nowy 20-kubitowy komputer kwantowy wzmacnia pozycję Finlandii wśród krajów inwestujących w obliczenia kwantowe i pokazuje, że Europa zacznie się liczyć na rynku tej technologii. Warto dodać, że Finlandia ukończyła swój pierwszy komputer kwantowy, 5-kubitowy, w 2021 r.

> *Te zaawansowane prace nad budową komputerów kwantowych powodują, że należy przyspieszyć prace nad systemami bezpieczeństwa, które będą w stanie oprzeć się mocy obliczeniowej komputerów kwantowych.*

Celem kryptografii postkwantowej jest opracowanie systemów kryptograficznych, które sprawdzają się zarówno w przypadku korzystania z komputerów kwantowych, jak i klasycznych oraz mogą współdziałać z istniejącymi protokołami i sieciami komunikacyjnymi. Problem polega na tym, że zarówno kryptosystemy klucza publicznego, jak i funkcje skrótu są zagrożone przez ewolucję komputerów kwantowych. Postęp obliczeń kwantowych otworzył możliwość przeprowadzania ataków wykorzystujących algorytmy Grovera i Shora. Takie algorytmy zagrażają zarówno kryptografii klucza publicznego, jak i funkcjom skrótu, zmuszając do przeprojektowania struktur informatycznych.

Potencjalne ataki przeprowadzane z wykorzystaniem komputerów kwantowych mają wpływ na najpopularniejsze algorytmy klucza publicznego, w tym RSA (Rivest–Shamir–Adleman), ECDSA (Elliptic Curve Digital Signature Algorithm), ECDH (Elliptic Curve Diffie-Hellman) czy DSA (Digital Signature Algorithm), które można złamać algorytmem Shora. Algorytm ten stanowi potencjalne zagrożenie dla powszechnie używanego w internecie kryptosystemu RSA. Klucz publiczny w RSA jest iloczynem dwóch dużych liczb pierwszych. Możliwość efektywnego odtworzenia tych liczb na podstawie klucza publicznego pozwalałaby poznać klucz prywatny i tym samym złamać cały szyfr. Podobnie jest w przypadku szyfru DES (Data Encryption Standard) oraz AES (Advanced Encryption Standard), które są szyframi blokowymi, uznanymi za standardy kryptograficzne przez rząd USA. Nie są już oficjalnie zalecane, ale nadal używane w aplikacjach oprogramowania bankomatów, zapewniania poufności poczty elektronicznej czy zdalnego dostępu do zasobów. Badacze pracują więc nad rozwojem kryptografii postkwantowej, która obejmuje algorytmy, takie jak kraty bazujące na trudnych problemach matematycznych, które są odporne na ataki komputerów kwantowych.

Wychodząc naprzeciw tym zagrożeniom, Amerykański Instytut Normalizacyjny NIST zainicjował publiczny proces wyboru kwantowych algorytmów kryptograficznych klucza publicznego do standaryzacji. W grudniu 2016 r. NIST ogłosił publiczne zaproszenie do składania wniosków do procesu standaryzacji algorytmów postkwantowych i po trzech rundach oceny i analizy ogłosił wybór pierwszych algorytmów, które zostaną znormalizowane. Wybrano mechanizm enkapsulacji klucza publicznego (KEM) CRYSTALS-Kyber. Podpisy cyfrowe, które zostaną ustandaryzowane, to CRYSTALS-Dilithium, FALCON i SPHINCS. Z wyjątkiem SPHINCS wszystkie schematy bazują na twardości obliczeniowej problemów związanych z sieciami strukturalnymi.

Niedawno NIST opublikował te trzy nowe standardy FIPS (Federal Information Processing Standard): FIPS 203, FIPS 204 i FIPS 205.

Większość krajów przyjmuje rozwiązania postkwantowe NIST, ale Francja pozwala na stosowanie kryptografii wykorzystującej algorytm FrodoKEM, który przeszedł większość testów w NIST, ale nie uzyskał pełniej akceptacji tej organizacji normalizacyjnej. FrodoKEM to rodzina mechanizmów hermetyzacji kluczy, które zostały zaprojektowane jako konserwatywne, ale praktyczne konstrukcje postkwantowe. Ich bezpieczeństwo wywodzi się z ostrożnych parametryzacji dobrze zbadanego problemu uczenia się z błędami, który z kolei

CRYSTALS-Kyber to zaprojektowany do ogólnych celów szyfrowania, takich jak tworzenie bezpiecznych stron internetowych, mechanizm hermetyzacji kluczy oparty na sieci modułów – Module-Lattice-Based Key-Encapsulation Mechanism Standard. Zalety tego rozwiązania to stosunkowo małe klucze szyfrowania, które dwie strony mogą łatwo wymienić, a także szybkość działania.

CRYSTALS-Dilithium został zaprojektowany w celu ochrony podpisów cyfrowych, których używamy podczas zdalnego podpisywania dokumentów. Ten standard podpisu cyfrowego bazuje na sieci modułów – Module-Lattice-Based Digital Signature Standard.

Protokół SPHINCS+, również przeznaczony do podpisów cyfrowych, jest nieco większy i wolniejszy, ale cenny jako kopia zapasowa, ponieważ wykorzystuje inne podejście matematyczne (bazuje na skrótach (hash) – Stateless Hash-Based Digital Signature Standard)

FALCON, również zaprojektowany z myślą o podpisach cyfrowych, ma otrzymać własny standard FIPS w tym roku.

ma ścisłe powiązania z domniemanymi trudnymi problemami na ogólnych, algebraicznie niestrukturalnych sieciach.

Dużym problemem wdrożeniowym jest to, że większość algorytmów postkwantowych używa większego rozmiaru klucza, na przykład AES z kluczami większymi niż dzisiejsze klucze 128-bitowe, co będzie wymagać adaptacji istniejących protokołów internetowych, takich jak TLS, do obsługi większych kluczy wymaganych przez algorytmy postkwantowe.

Technologia kwantowa wymaga od użytkowników i dostawców PKI tzw. zwinności kryptograficznej. Oznacza to, że muszą być w stanie aktualizować i zmieniać swoje algorytmy kryptograficzne, co wymaga posiadania wykazu kluczy, certyfikatów i używanych algorytmów, automatyzacji i podziału zarządzania zmianami oraz skrócenia ważności certyfikatów. Zaleca się również wypróbowanie nowych algorytmów kryptografii postkwantowej w miarę ich udostępniania i ocenę ich wpływu na wydajność, projekt, protokoły i zasoby. W wielu krajach całego świata prace przygotowujące do kryptografii kwantowej już zostały rozpoczęte, może czas zacząć takie prace w naszym kraju.

Wszystkie informacje zawarte w artykule są podane według stanu na 7 maja 2024 r.

KRAJ	Algorytm zalecany do wdrożenia	Opublikowane zalecenia lub norma	Okres wdrożenia
Australia	NIST	CTPCO (2023)	Start planowania, implementacja 2025–2026
Kanada	NIST	Cyber Centre (2021)	Start planowania, implementacja od roku 2025
Chiny	Własny, specyficzny dla kraju	CACR (2020)	Start planowania
Komisja Europejska	NIST	ENISA (2022)	Start planowania i mitygacja
Francja	NIST (ale nie wyłącznie)	ANSSI (2022, 2023)	Start planowania, początek w roku 2024
Niemcy	NIST (ale nie wyłącznie)	BSI (2022)	Start planowania
Japonia	Monitoruje NIST	CRYPTREC	Start planowania
Holandia	AES, monitoruje NIST, SPHINCS-256 i XMSS		
Nowa Zelandia	NIST		Start planowania
Singapur	Monitoruje NIST	MCI (2022)	Brak informacji
Korea Południowa	KpqC	MSIT (2023)	Konkurs na rozwiązanie (pierwsza runda listopad 2022 – listopad 2023)
Wielka Brytania	NIST	NCSC (2023)	Start planowania, wdrożenie od 2024
Stany Zjednoczone	NIST	CISA (2021, 2022), 2023), NIST (2023), NSA (2022, 2023), White House (2022)	Wdrożenie 2023–2033

Źródło: GSM Association. Post Quantum Cryptography – Guidelines for Telecom Use Cases Version 1.0 22 February 2024