DOI: 10.34616/151202

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 77–95

Mateusz Jakubik
Uniwersytet Jagielloński w Krakowie
Wydział Prawa i Administracji
ORCID: 0000-0002-8992-7309

Adw. Oskar Grajewski
ORCID: 0009-0009-7968-5543

Implementacja *post-quantum cryptography* w ramach EUDI *Wallet* jako elementu eIDAS 2 w kontekście wyzwań prawnych i technicznych oraz implikacji dla bezpieczeństwa cybernetycznego w świetle regulacji CRA i NIS 2[1]

Streszczenie

Niniejsze opracowanie bada znaczenie kryptografii postkwantowej (ang. *post-quantum cryptography,* PQC) w kontekście postkwantowej rzeczywistości, podkreślając jej rolę jako fundamentu przyszłego bezpieczeństwa cyfrowego. Praca analizuje także wyzwania związane z implementacją PQC w kluczowych projektach europejskich, takich jak Europejski Portfel Tożsamości Cyfrowej (ang. *European Digital Identity Wallet*, EUDI *Wallet*), który ma stać się centralnym elementem ekosystemu cyfrowego Unii Europejskiej (UE). W erze postkwantowej PQC będzie nie tylko narzędziem ochrony przed nowymi zagrożeniami, ale także kluczowym elementem regulacji prawnych, takich jak eIDAS 2 i NIS 2, mających na celu zapewnienie bezpieczeństwa i interoperacyjności systemów cyfrowych w UE. Praca podkreśla znaczenie harmonizacji przepisów międzynarodowych oraz współpracy globalnej, które są niezbędne do skutecznej implementacji PQC, zapewniającej odporność na zagrożenia wynikające z przyszłych osiągnięć technologii kwantowej.

Słowa kluczowe

kryptografia postkwantowa, bezpieczeństwo cyfrowe, algorytmy kryptograficzne, Europejski Portfel Tożsamości Cyfrowej, interoperacyjność, cyberbezpieczeństwo, technologia kwantowa, eIDAS 2, NIS 2

[1] Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autorów i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autorzy byli albo są powiązani.

Wstęp

W obliczu nieustającego postępu technologicznego, gdy każdy kolejny dzień przybliża nas do upowszechnienia osiągnięć w dziedzinie technologii komputeryzacji kwantowej, kwestia zabezpieczenia danych cyfrowych staje się wyzwaniem o bezprecedensowej skali. Jednak powszechnie, z wyjątkiem osób żywo zainteresowanych tą tematyką, zdaje się umykać uwadze, iż wyzwanie to nie ogranicza się jedynie do aspektów technicznych, ale rozciąga się również na szerokie spektrum kwestii prawnych, etycznych oraz społecznych. W kontekście tego dynamicznie zmieniającego się krajobrazu pojęcie kryptografii postkwantowej (ang. *post-quantum cryptography*, PQC)[2] nabiera szczególnego znaczenia, stając się fundamentem przyszłego bezpieczeństwa cyfrowego w erze, którą niektórzy określają już jako postkwantową[3].

W miarę jak świat staje na progu tej nowej epoki technologicznej, której katalizatorem mają być komputery kwantowe, dotychczasowe paradygmaty bezpieczeństwa cyfrowego ulegają istotnym przekształceniom, a infrastruktura kryptograficzna stoi przed bezprecedensowym wyzwaniem, jakim jest zagrożenie złamania przez potężne możliwości obliczeniowe komputerów kwantowych. Rozwój tej technologii, początkowo postrzegany jako odległa i teoretyczna perspektywa, w ostatnich latach nabiera tempa, a implikacje jej wdrożenia zaczynają wpływać na kluczowe obszary regulacji prawnych i polityki bezpieczeństwa. Staje się jasne, że to, co kiedyś było jedynie eksperymentalnym polem badań, dzisiaj wymaga natychmiastowej reakcji, szczególnie w kontekście ochrony danych i systemów cyfrowych na poziomie globalnym. Jednym z najważniejszych narzędzi, które mają zapewnić bezpieczeństwo w tej postkwantowej rzeczywistości, jest właśnie kryptografia postkwantowa. PQC poprzez wprowadzenie algorytmów odpornych na obliczenia kwantowe może stanowić odpowiedź na zagrożenia wynikające z rosnących możliwości technologii kwantowej. Wraz z rozwojem nowych rozwiązań, takich jak Europejski Portfel Tożsamości Cyfrowej (ang. *European Digital Identity Wallet*, EUDI *Wallet*), który ma stać się integralnym elementem ekosystemu cyfrowego Unii Europejskiej (UE), implementacja kryptografii postkwantowej staje się kluczowym, niezwykle naglącym zadaniem.

---

[2] *What Is Post-Quantum Cryptography?*, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography/ [dostęp: 31.08.2024].

[3] *Entering the Quantum Era* , https://www.ox.ac.uk/news/features/entering-quantum-era/ [dostęp: 31.08.2024].

Niniejszy artykuł podejmuje próbę szczegółowej analizy wyzwań związanych z implementacją PQC w EUDI *Wallet* w kontekście obowiązujących i przyszłych regulacji prawnych, takich jak eIDAS 2, NIS 2 oraz CRA. Ponadto badane będą implikacje dla bezpieczeństwa cybernetycznego oraz interoperacyjności systemów cyfrowych. W centrum tych rozważań znajduje się pytanie o to, jak UE może zabezpieczyć swoją infrastrukturę cyfrową na przyszłe dekady oraz jakie kroki legislacyjne i technologiczne są konieczne, aby sprostać tym wyzwaniom.

1. Znaczenie *post-quantum cryptography* (PQC) w erze postkwantowej

Pojęcie kryptografii postkwantowej zrodziło się z konieczności odpowiedzi na pytanie, jak chronić informacje w świecie, gdzie obliczenia kwantowe stają się rzeczywistością. Od lat 90. XX w., kiedy to P.W. Shor przedstawił swój algorytm do faktoryzacji liczb[4], środowisko kryptograficzne zaczęło dostrzegać nieuchronne zagrożenie ze strony komputerów kwantowych[5]. Wówczas jednak zagadnienie to traktowano jako problem odległy, niemający bezpośredniego wpływu na bieżące praktyki bezpieczeństwa cyfrowego. Z upływem lat badania nad komputerami kwantowymi zaczęły nabierać tempa, a to w konsekwencji wywołało rosnącą świadomość potrzeby opracowania nowych metod szyfrowania. W 2016 r. Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards and Technology*, NIST) w Stanach Zjednoczonych ogłosił konkurs na standardy kryptograficzne odporne na ataki kwantowe, który stał się impulsem dla globalnych wysiłków badawczych w tej dziedzinie[6]. W ramach konkursu złożono setki propozycji algorytmów, które mają potencjał zabezpieczenia przyszłościowych systemów informatycznych przed zagrożeniami wynikającymi z rozwoju komputerów kwantowych[7]. Mimo więc, że kryptografia postkwantowa wciąż stanowi stosunkowo nowy obszar

[4] W matematyce faktoryzacja polega na zapisaniu liczby lub innego obiektu matematycznego jako iloczynu kilku czynników, zwykle mniejszych lub prostszych obiektów tego samego rodzaju. Na przykład 3×5 to rozkład liczby całkowitej 15, a(x – 2)(x + 2) to rozkład wielomianowy x2–4.

[5] P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf/ [dostęp: 31.08.2024].

[6] *NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat*, https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat/ [dostęp: 31.08.2024].

[7] *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, https://csrc.nist.gov/pubs/ir/8309/final [dostęp: 31.08.2024].

badań, to już teraz jawi się jako jeden z kluczowych elementów strategii obronnych przeciwko zagrożeniom wynikającym z rozwoju komputerów kwantowych.

Komputery kwantowe obiecują rewolucję w obliczeniach zdolnych rozwiązywać problemy, które są obecnie niemożliwe do rozwiązania przez klasyczne komputery[8]. Choć potencjał ten niesie ze sobą ogromne możliwości, to stanowi on jednocześnie zagrożenie dla istniejących obecnie systemów kryptograficznych, a co za tym idzie – także dla całej infrastruktury bezpieczeństwa cyfrowego. Obecnie stosowane metody kryptograficzne bazują na założeniu, że pewne operacje matematyczne są zbyt skomplikowane, aby mogły być efektywnie przeprowadzone na klasycznych komputerach w rozsądnym czasie. Na przykład problem rozkładu liczby na czynniki pierwsze, będący podstawą bezpieczeństwa algorytmu RSA, dla odpowiednio dużych liczb uważany jest za nierozwiązywalny przez klasyczne komputery w czasie, który w praktyce uzasadniałby podejmowanie takich działań[9]. Jednakże w przypadku komputerów kwantowych operacje te mogą być wykonane w czasie logarytmicznym względem rozmiaru wejścia, co oznacza, że każde 2048-bitowe klucze RSA mogłyby *de facto* zostać złamane w czasie kilku sekund lub minut przez odpowiednio rozwinięty komputer kwantowy[10].

W tym kontekście systemy kryptograficzne, które dziś są uważane za bezpieczne, mogą stać się podatne na ataki w przeciągu kilku najbliższych dekad, co wymaga pilnego opracowania i wdrożenia nowych, odpornych na kwantowe obliczenia metod szyfrowania[11]. Istnieje kilka przodujących wariantów PQC, które mogą być stosowane w przyszłości do ochrony danych. Najbardziej obiecujące z nich to algorytmy oparte na kratach (ang. *lattice-based cryptography*)[12], kodach (ang. *code-based cryptography*)[13], wielomianach (ang. *multivariate polynomial cryptography*)[14] oraz podpisy oparte na funkcjach skrótu (ang. *hash-based signatures*)[15]. Kryptografia oparta na kratach, będąca jednym z najbardziej rozwiniętych podejść, odnosi się

[8] *Toward a code-breaking quantum computer*, https://www.sciencedaily.com/releases/2024/08/240823120024.htm/ [dostęp: 30.08.2024].

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson 2014, s. 283–308, https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf/ [dostęp: 31.08.2024].

[10] M. Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, „IEEE Security & Privacy" 2018, vol. 16(5), s. 38–41.

[11] *Post-Quantum Cryptography: Current Status and Next Steps*, https://csrc.nist.gov/publications/detail/nistir/8105/final [dostęp: 30.08.2024].

[12] D.J. Bernstein, J. Buchmann, E. Dahmen, *Post-Quantum Cryptography* , Springer 2009, s. 147–187.

[13] *Ibidem*, s. 95–141.

[14] *Ibidem*, s. 193–234.

[15] *Ibidem*, s. 35–91.

do problemów związanych z trudnością znajdowania najkrótszych wektorów w kratach[16]. Problemy te są uważane za niezwykle trudne do rozwiązania nawet przez komputery kwantowe, co czyni je idealnym rozwiązaniem dla przyszłych standardów kryptograficznych. *Code-based cryptography*, choć mniej popularna niż metody oparte na kratach, także wykazuje duży potencjał. Metoda ta została po raz pierwszy zaproponowana przez R. McEliece w 1978 r. i bazuje na trudności dekodowania losowych kodów liniowych. Pomimo że algorytm McEliece'a jest bardzo wydajny i bezpieczny, to wymaga dużych rozmiarów kluczy kryptograficznych[17], co jest jego główną wadą w kontekście jego ewentualnej szerokiej implementacji. Podpisy oparte na *hashach*, jak np. algorytm Merkle'a[18], są również rozważane jako przyszłościowe rozwiązanie[19], albowiem charakteryzują się one prostotą i wysoką odpornością na ataki kwantowe, co czyni je dobrym wyborem dla systemów wymagających bezpiecznych podpisów cyfrowych. Wielomianowe „kryptosystemy", choć jawią się jako mniej rozwinięte niż inne podejścia, również oferują potencjalnie atrakcyjne rozwiązania i zastosowania, zwłaszcza w kontekście tworzenia złożonych algorytmów kryptograficznych opartych na trudnych problemach algebraicznych[20].

Ważąc dotychczasowe dywagacje, można zaryzykować stwierdzenie, iż u postronnego czytelnika dotychczasowa lektura mogłaby wywołać konsternację, jak również mogłoby towarzyszyć mu swoiste niedowierzanie, w jaki sposób tematyka ta łączy się z zagadnieniami natury prawnej. W replice na tego rodzaju wątpliwość dopuszczalny zdaje się truizm, iż znakiem „naszych czasów" pozostaje zjawisko, gdy różne nauki ścisłe oraz techniczne, a szczególnie informatyka, coraz śmielej wkraczają we wszelkie dziedziny współczesnego życia. Skoro więc życie to tak prędko i powszechnie ulega cyfryzacji, to społeczeństwo zmuszone jest zjawisku temu sprostać na różnych płaszczyznach i poprzez różne inicjatywy. Jedną z nich jest projekt UE dotyczący wdrożenia Europejskiego Portfela Tożsamości Cyfrowej

---

[16] W geometrii i teorii grup „krata" w rzeczywistej przestrzeni współrzędnych R^n jest nieskończonym zbiorem punktów tej przestrzeni o następujących właściwościach: dodanie lub odjęcie dwóch punktów należących do kratki daje inny punkt kratki, wszystkie punkty kratki są od siebie oddalone o co najmniej pewną minimalną odległość, a każdy punkt w przestrzeni znajduje się w skończonej maksymalnej odległości od najbliższego punktu kratki.

[17] Klucz kryptograficzny to liczba lub ciąg danych, które są wykorzystywane w procesie szyfrowania i deszyfrowania informacji.

[18] Nazywany także „Puzzlami Merkle'a". Jest jedną z pierwszych wersji algorytmu kryptografii z kluczem publicznym zaproponowaną przez R. Merkle'a w 1974 r., a opublikowaną w 1978 r.

[19] B. Schneier, *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, wyd. 2, Warszawa 2002, s. 51–81.

[20] P. Kapcia, *Kryptosystemy oparte na problemach trudnych obliczeniowo z wyszczególnieniem problemu faktoryzacji liczb całkowitych*, „Elektrotechnika i Elektronika" 2005, t. 24, nr 2, s. 148–57.

(ang. *European Digital Identity Wallet*, EUDI *Wallet*), mającego stanowić bezpieczne i zaufane środowisko dla cyfrowej identyfikacji obywateli UE, a który to projekt będzie częścią większego ekosystemu, mającego na celu ułatwienie cyfrowej transformacji i wzmocnienie jednolitego rynku cyfrowego UE[21]. Zaznaczyć należy, iż koncepcja EUDI *Wallet* nie stanowi osobnego bytu w ramach europejskiej legislacji, lecz jest elementem szerszej propozycji legislacyjnej Komisji Europejskiej, znanej jako rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[22] (ang. *European Identity Digital and Authentication Services 2.0.*, eIDAS 2).

Jednym z głównych wyzwań w implementacji EUDI *Wallet* jest zapewnienie, że system ten będzie mógł sprostać przyszłym zagrożeniom, w tym związanym z rozwojem omawianych już komputerów kwantowych. Implementacja PQC w ramach EUDI *Wallet* jest zatem kluczowa dla osiągnięcia tego zamierzenia i zapewnienia, że system ten pozostanie bezpieczny i zaufany również w erze postkwantowej. Projekt ten zakłada, iż EUDI *Wallet* będzie narzędziem, które umożliwi obywatelom UE przechowywanie i zarządzanie różnymi rodzajami cyfrowej tożsamości, w tym danymi osobowymi, certyfikatami oraz innymi informacjami wrażliwymi tak, aby były one całkowicie bezpieczne[23], do czego niezbędne jest, zważywszy na sygnalizowane już zagrożenia ery postkwantowej, zastosowanie najnowocześniejszych technologii kryptograficznych, w tym PQC, które będą w stanie skutecznie chronić dane przed nowymi rodzajami ataków. Odnośnie do rozporządzenia eIDAS 2 EUDI *Wallet* pełnić ma więc nie tylko funkcję narzędzia do zarządzania tożsamością cyfrową, ale ma być również platformą umożliwiającą realizację różnorodnych usług zaufania, a usługi te, jak np. elektroniczne podpisy, muszą być również chronione przed potencjalnymi zagrożeniami związanymi z kryptografią kwantową. Implementacja PQC w EUDI *Wallet* pozwala zatem na wprowadzenie dodatkowej warstwy zabezpieczeń, która jest niezbędna do spełnienia wymogów bezpieczeństwa określonych w rozporządzeniu eIDAS 2.

Warto także zwrócić uwagę na aspekt interoperacyjności EUDI *Wallet* w kontekście PQC, polegający na tym, że musi być on kompatybilny z różnymi systema-

[21] *What is the EU Digital Identity Wallet*, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet/ [dostęp: 30.08.2024].

[22] Dz. Urz. UE L 257/73 z 2014 r. (dalej: „eIDAS 2").

[23] Art. 3 ust. 42 eIDAS2.

mi cyfrowymi zarówno w ramach UE, jak i poza nią. Wprowadzenie PQC stawia wyzwanie w zakresie zapewnienia, że nowe algorytmy będą mogły współpracować z istniejącymi systemami kryptograficznymi, a także że będą one spełniać wymogi regulacyjne w różnych innych jurysdykcjach, miejscami wciąż zasadniczo odmiennych od unijnej[24]. To z kolei wymaga ścisłej współpracy między regulatorami, dostawcami technologii oraz organizacjami standaryzacyjnymi. Z tej perspektywy nie będzie przesadą stwierdzenie, że wprowadzenie PQC do EUDI *Wallet* ma nie tylko znaczenie technologiczne i regulacyjne, ale także strategiczne i polityczne.

2. Techniczno-prawna analiza implementacji PQC w EUDI *Wallet*

Implementacja PQC w ramach EUDI *Wallet* napotyka na szereg trudności technicznych, które muszą zostać pokonane, aby zapewnić skuteczność i bezpieczeństwo tego systemu. Owe kłopotliwe zagadnienia związane są z różnymi aspektami technologii PQC, w tym przede wszystkim z efektywnością algorytmów, kompatybilnością z istniejącą już infrastrukturą cyfrową, a także z wymogami dotyczącymi mocy obliczeniowej i zasobów. Sytuacja ta nie powinna jednak dziwić, albowiem praktyczne wykorzystanie PQC wymaga znacznie większej mocy obliczeniowej niż tradycyjne metody kryptograficzne, co w tej konkretnej sytuacji może stanowić problem w kontekście implementacji tej technologii w systemach takich jak EUDI *Wallet*. Portfele cyfrowe, które w założeniu powinny działać sprawnie na różnych urządzeniach, w tym także na tych o ograniczonej mocy obliczeniowej (jak chociażby smartfony, czy inne urządzenia mobilne), muszą być odpowiednio zoptymalizowane pod kątem efektywności. Przykładowo algorytmy oparte na kratach, takie jak np. Kyber[25], wymagają znacznej liczby operacji matematycznych, które mogą spowalniać działanie systemów, w związku z czym przy ich hipotetycznym zastosowaniu konieczne jest znalezienie kompromisu między bezpieczeństwem a wydajnością, by zapewnić, że EUDI *Wallet* będzie działał sprawnie i bezpiecznie, niezależnie od mocy obliczeniowej urządzenia, na którym jest uruchamiany (co w przeciwnym razie, prócz zagrożenia, mogłoby wiązać się także z ryzykiem narażania części obywa-

[24] L. Chen *et al.*, *Report on Post-Quantum Cryptography*, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf [dostęp: 31.08.2024].

[25] *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, https://csrc.nist.gov/pubs/fips/203/final/ [dostęp: 31.08.2024].

teli UE na wykluczenie społeczne)[26]. Taka optymalizacja algorytmów PQC, aby były one wydajne nawet na urządzeniach o ograniczonej mocy obliczeniowej, wymaga zaawansowanego podejścia inżynierskiego, które pozwoli na dostosowanie właściwych metod kompresji danych, redukcji liczby operacji matematycznych oraz wykorzystania nowoczesnych technologii, takich jak przetwarzanie rozproszone, aby zminimalizować obciążenie obliczeniowe. W przeciwnym razie korzystanie z EUDI *Wallet* na urządzeniach mobilnych mogłoby stać się niepraktyczne z powodu długiego czasu przetwarzania lub nadmiernego zużycia baterii[27].

Kolejnym kluczowym wyzwaniem jest zapewnienie kompatybilności algorytmów PQC z istniejącą już infrastrukturą cyfrową. Obecne systemy bezpieczeństwa, które bazują na tradycyjnych algorytmach kryptograficznych, muszą być zintegrowane z nowymi metodami PQC w sposób, który nie zakłóca ich funkcjonowania, co jest zadaniem wymagającym zaawansowanej inżynierii i testowania. W kontekście EUDI *Wallet*, który będzie musiał działać w ramach szeroko zintegrowanego ekosystemu cyfrowego, zapewnienie takiej kompatybilności jest szczególnie istotne, tym bardziej w warunkach europejskich, gdzie EUDI *Wallet* będzie musiał być w stanie współpracować z wieloma różnymi systemami identyfikacji elektronicznej, usługami zaufania oraz infrastrukturą sieciową, która już funkcjonuje w ramach Unii Europejskiej i w obrębia każdego jej państwa członkowskiego[28].

Jednakże implementacja PQC w ramach EUDI *Wallet* wiąże się nie tylko z wyzwaniami technicznymi, ale również z licznymi kwestiami natury prawnej oraz regulacyjnej. Rozporządzenie eIDAS 2 stanowi fundament prawny dla funkcjonowania EUDI *Wallet*, a główne cele eIDAS 2 obejmują zapewnienie wysokiego poziomu bezpieczeństwa usług identyfikacji elektronicznej oraz zwiększenie zaufania do tych usług w całej Unii Europejskiej. Wprowadzenie PQC do EUDI *Wallet* jest więc bezpośrednio związane z wymogami eIDAS 2 dotyczącymi bezpieczeństwa, albowiem rozporządzenie to wymaga, aby wszystkie systemy identyfikacji elektronicznej były odpowiednio zabezpieczone przed zagrożeniami cybernetycznymi[29], jak również szczegółowo opisuje obowiązki państw członkowskich oraz dostawców usług zaufania w zakresie zapewnienia bezpieczeństwa danych i identyfikacji elektronicznej, a to podkreślając konieczność stosowania odpowiednich środków tech-

[26] L. Chen *et al*., *op. cit*., s. 6–7.

[27] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe, *Post-Quantum Key Exchange – A New Hope*, 25th USENIX Security Symposium (USENIX Security 16), 2016, s. 327–343.

[28] *Ibidem*.

[29] Art. 8 eIDAS 2.

nicznych i organizacyjnych, które uwzględniają aktualny stan wiedzy technicznej[30]. Oznacza to więc, że w erze postkwantowej systemy muszą być odporne właśnie na ataki kwantowe. Wprowadzenie PQC jest zatem niezbędne do spełnienia tych postawionych sobie nominalnie (*de facto* minimalnych) wymogów, lecz implementacja PQC w EUDI *Wallet* oferuje jednocześnie nowoczesne rozwiązania kryptograficzne, które będą mogły sprostać wyzwaniom także w przyszłości.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148[31] (ang. *Network and Information Systems Directive 2*, NIS 2) rozszerza zakres dotychczasowych regulacji dotyczących bezpieczeństwa sieci i systemów informatycznych w UE (tj. wynikających z NIS), albowiem wprowadza ona nowe wymogi dotyczące zarządzania ryzykiem, zgłaszania incydentów bezpieczeństwa oraz wymiany informacji między państwami członkowskimi[32]. Dyrektywa NIS 2 kładzie szczególny nacisk na zabezpieczenia techniczne, które mają na celu ochronę przed zagrożeniami cybernetycznymi, w tym także przed potencjalnymi atakami przeprowadzanymi za pomocą komputerów kwantowych. Odnosząc się ponownie do implementacji PQC w EUDI *Wallet*, dyrektywa NIS 2 stanowi istotny punkt odniesienia, ponieważ nakłada obowiązek stosowania najnowszych technologii zabezpieczających na operatorów usług krytycznych, w tym na dostawców usług identyfikacji elektronicznej[33]. Wymogi dyrektywy NIS 2 dotyczące zarządzania ryzykiem i odporności na zagrożenia kwantowe są zbieżne z celami eIDAS 2, co czyni te dwa akty prawnymi filarami regulacyjnymi, na których opiera się implementacja PQC w EUDI *Wallet,* przy czym dyrektywa NIS 2 dodatkowo zobowiązuje państwa członkowskie do współpracy przy wdrażaniu i monitorowaniu środków ochrony, co może przyczynić się do szybszego i bardziej jednolitego wdrożenia PQC w całej UE[34]. Istotne jest również, że dyrektywa NIS 2 nakłada obowiązki w zakresie raportowania incydentów, co może obejmować incydenty związane z nowymi zagrożeniami kwantowymi i prowadzić do ich nagłaśniania. Wprowadzenie PQC może zatem stanowić kluczowy element strategii zapobiegania takim incydentom i zapewnienia zgodności z dyrektywą NIS 2[35].

---

[30] Art. 19 eIDAS 2.
[31] Dz. Urz. UE L 333/80 z 2022 r. (dalej: „NIS 2").
[32] Art. 21 NIS 2.
[33] *Ibidem*.
[34] Art. 8 NIS 2.
[35] Art. 18 NIS 2.

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020[36] (ang. *Cyber Resilience Act*, CRA) to kolejny kluczowy akt prawny, który ma znaczenie przy implementacji PQC w EUDI *Wallet*. Rozporządzenie CRA ma na celu wzmocnienie odporności cybernetycznej produktów i usług cyfrowych w UE i wprowadza nowe przepisy dotyczące projektowania, produkcji i zarządzania cyklem życia produktów cyfrowych z naciskiem na bezpieczeństwo i odporność na zagrożenia cybernetyczne[37]. Rozporządzenie CRA wymaga, aby wszystkie produkty cyfrowe, w tym systemy identyfikacji elektronicznej, były projektowane z myślą o najwyższym poziomie bezpieczeństwa, co oznacza, że już na etapie projektowania muszą być uwzględnione potencjalne zagrożenia wynikające z rozwoju technologii kwantowej. Dlatego też wprowadzenie PQC do EUDI *Wallet* wpisuje się w tę filozofię, oferując zaawansowane zabezpieczenia kryptograficzne, które mogą sprostać wyzwaniom przyszłości. Ważkie w tym przypadku pozostaje także zapewnienie, że produkty cyfrowe będą regularnie aktualizowane tak, aby mogły odpowiadać na nowe zagrożenia, co w przypadku PQC oznacza konieczność ciągłego monitorowania rozwoju technologii kwantowej oraz dostosowywania algorytmów kryptograficznych do nowych wyzwań.

W świetle opisanych okoliczności oczywiste pozostaje zasadnicze wyzwanie związane z implementacją PQC, jakim będzie zapewnienie harmonizacji przepisów i to nie tylko na poziomie unijnym, lecz także międzynarodowym, ponieważ w obliczu globalnych zagrożeń kwantowych skuteczna implementacja PQC wymaga ścisłej współpracy między państwami członkowskimi UE oraz z innymi partnerami międzynarodowymi. Istotnym elementem tej współpracy jest też harmonizacja standardów kryptograficznych, co pozwoli na stworzenie jednolitego podejścia do bezpieczeństwa cyfrowego na całym świecie. Poprzez swoje inicjatywy regulacyjne, takie jak eIDAS 2, NIS 2 oraz CRA, UE dąży do stworzenia spójnego i kompleksowego systemu ochrony przed zagrożeniami kwantowymi, lecz aby osiągnąć pełną skuteczność, regulacje te muszą być zharmonizowane nie tylko między sobą, lecz także z międzynarodowymi standardami, takimi jak te opracowywane przez NIST.

[36] Dalej: „CRA".
[37] Motyw 25, 60, 91 i art. 13 CRA.

W kontekście UE zaznaczyć należy, iż harmonizacja prawa obejmuje również kwestie związane z ochroną danych osobowych i prywatności. Wprowadzenie PQC w EUDI *Wallet* musi być zgodne z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO, *General Data Protection Regulation, GDPR*)[38], co oznacza, że algorytmy kryptograficzne muszą zapewniać nie tylko bezpieczeństwo danych, ale również ich integralność i poufność.

Niezależnie od powyższego zastrzec należy, że w ramach implementacji PQC w EUDI *Wallet* odnieść należy się także do kwestii merkantylnych, albowiem działanie to wymaga niewątpliwie poczynienia znacznych inwestycji. Przede wszystkim mowa tu o wydatkach na dalsze badania i rozwój (ang. *Research and Development*, R&D), testowanie i wdrożenie algorytmów PQC, a dodatkowo konieczne będzie również poniesienie kosztów związanych z przeszkoleniem personelu technicznego oraz dostosowaniem istniejącej infrastruktury cyfrowej do nowych wymogów kryptograficznych. Kwestie te mogą być szczególnie problematyczne dla mniejszych państw członkowskich UE, które mogą nie dysponować wystarczającymi zasobami finansowymi, aby sprostać takim wymogom. W związku z tym UE może być zmuszona do wprowadzenia programów wsparcia finansowego dla państw członkowskich oraz dla podmiotów gospodarczych, które będą musiały zainwestować w tę technologię. Z drugiej strony pomimo wysokich kosztów związanych z implementacją PQC istnieją również potencjalne znaczące korzyści ekonomiczne. Wprowadzenie PQC może przyczynić się do zwiększenia bezpieczeństwa cyfrowego na całym kontynencie, co z kolei może zwiększyć zaufanie do cyfrowych usług zaufania i identyfikacji elektronicznej. Taka sytuacja może natomiast zaowocować przyciąganiem nowych użytkowników i inwestorów do ekosystemu EUDI *Wallet*, co przyniesie korzyści gospodarcze w dłuższej perspektywie. Dodatkowo UE dzięki swojej wiodącej roli w implementacji PQC może stać się liderem w dziedzinie bezpieczeństwa cyfrowego na świecie. To z kolei może przyczynić się do zwiększenia konkurencyjności europejskich firm technologicznych na rynku globalnym, co potencjalnie przełoży się na wzrost gospodarczy i innowacyjność w sektorze cyfrowym. W tych okolicznościach z jednej strony zapewnienie bezpieczeństwa w erze postkwantowej może zapobiec potencjalnym stratom gospodarczym

[38] Dz. Urz. UE L 119 z 2016 r.

wynikającym z ataków kwantowych, które mogłyby sparaliżować systemy finansowe i inne kluczowe sektory gospodarki. Z drugiej strony wprowadzenie PQC może wymusić na firmach inwestycje w nowe technologie, co przyspieszy innowacyjność i rozwój nowych produktów oraz usług cyfrowych.

Dodatkowo w ramach problematyki implementacji zaznaczyć należy również nie mniej ważny aspekt społeczny. Jedną z najważniejszych kwestii społecznych związanych z implementacją PQC jest zaufanie publiczne. Wprowadzenie nowej, zaawansowanej technologii kryptograficznej może budzić obawy wśród obywateli, zwłaszcza gdy chodzi o ochronę danych osobowych i prywatności. Aby zbudować zaufanie do EUDI *Wallet* i zapewnić społeczną akceptację dla PQC, niezbędne jest przeprowadzenie szeroko zakrojonych działań edukacyjnych i informacyjnych. Społeczeństwo musi być świadome korzyści wynikających z wprowadzenia PQC, a także zrozumieć, w jaki sposób technologia ta przyczyni się do poprawy bezpieczeństwa ich danych osobowych. Transparentność w zakresie działania algorytmów PQC oraz ich wpływu na prywatność stanowi tym samym doskonały punkt wyjścia do wzmocnienia zaufania publicznego.

3. Implikacje oraz dalsze wyzwania i perspektywy związane z implementacją PQC w EUDI *Wallet*

Wprowadzenie EUDI *Wallet* opartego na technologii PQC otwiera zupełnie nowy rozdział w dziedzinie cyberbezpieczeństwa. Rozważając implikacje omawianego rozwiązania w tejże dziedzinie, konieczne jest szczegółowe zbadanie, jak może ono wpłynąć na różne aspekty bezpieczeństwa cybernetycznego, w tym ochronę danych, odporność na zagrożenia oraz interoperacyjność z istniejącymi systemami, które to kwestie również komplikują się istotnie w sytuacji szybko rozwijającej się technologii kwantowej.

Jednym z najważniejszych skutków wprowadzenia PQC w ramach EUDI *Wallet* jest zatem znaczące podniesienie poziomu ochrony danych. Jak wskazano już na wstępie, tradycyjne metody kryptograficzne, takie jak omówiony już RSA czy ECC (ang. *Elliptic Curve Cryptography*)[39], które od lat stanowią fundament bezpieczeństwa w systemach cyfrowych, stają się podatne na zagrożenia ze strony komputerów

[39] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography* 2004. s. 7–14, http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Guide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf/ [dostęp: 31.08.2024].

kwantowych. Implementacja PQC w EUDI *Wallet* ma więc kluczowe znaczenie dla ochrony wrażliwych danych osobowych przechowywanych w portfelu, ponieważ oferuje narzędzia, które mają na celu przeciwdziałanie tym zagrożeniom poprzez zastosowanie algorytmów odpornych na ataki kwantowe. Zastosowanie PQC w EUDI *Wallet* nie tylko zwiększa poziom ochrony danych, ale również zapewnia ich integralność oraz autentyczność. W erze cyfrowej, w której „cyberprzestępczość" przybiera na sile, możliwość zagwarantowania, że dane nie zostały zmienione ani przechwycone przez nieuprawnione osoby, jest istotnym elementem bezpieczeństwa cybernetycznego. Co więcej, PQC może również przeciwdziałać atakom opartym na manipulacji danymi, co stanowi dodatkowy jeszcze aspekt ochrony. Zastosowanie PQC w EUDI *Wallet* ma ponadto także długoterminowe implikacje w zakresie odporności na przyszłe zagrożenia, co oznacza, że systemy cyfrowe są projektowane z myślą o ewolucji technologii i zmieniających się metodach ataków. PQC, dzięki swojej złożoności matematycznej i specyfice algorytmów, oferuje poziom ochrony, który będzie trudny do pokonania nawet przez przyszłe technologie kwantowe, ale mimo to, aby zapewnić długoterminową odporność, konieczne jest ciągłe monitorowanie rozwoju technologii kwantowych oraz dostosowywanie stosowanych algorytmów do nowych odkryć.

Interoperacyjność, czyli zdolność różnych systemów i organizacji do współpracy i wymiany danych, jest kluczowym elementem współczesnej infrastruktury cyfrowej. Wprowadzenie PQC w EUDI *Wallet* ma zatem istotne znaczenie dla interoperacyjności na wielu poziomach, zarówno w kontekście technologicznym, jak i regulacyjnym. Na poziomie technologicznym zastosowanie nowych algorytmów kryptograficznych może wpłynąć na zdolność systemu EUDI *Wallet* do współpracy z innymi systemami cyfrowymi, które wciąż opierają się na tradycyjnych metodach kryptograficznych. Jednak aby zapewnić płynną integrację i współpracę pomiędzy różnymi systemami, konieczne będzie opracowanie standardów, które umożliwią bezproblemową wymianę danych pomiędzy systemami korzystającymi z PQC a tymi, które jeszcze nie przeszły na nowe technologie. To wyzwanie wymaga skoordynowanego podejścia, tak aby uniknąć fragmentacji rynku. Na poziomie regulacyjnym wprowadzenie PQC w EUDI *Wallet* może wymagać dostosowania istniejących przepisów dotyczących ochrony danych, cyberbezpieczeństwa oraz interoperacyjności systemów cyfrowych. W związku z tym organy regulacyjne będą musiały opracować nowe wytyczne i standardy, które uwzględnią specyfikę PQC oraz jego wpływ na współpracę pomiędzy systemami cyfrowymi.

Wprowadzenie PQC w EUDI *Wallet* nie tylko stawia UE przed nowymi wyzwaniami, ale również otwiera perspektywy rozwoju, które mogą zdefiniować przy-

szłość bezpieczeństwa cyfrowego na całym świecie. Jednym z głównych wyzwań z tym związanych jest jednak złożoność implementacji nowych algorytmów kryptograficznych, które wymagają zaawansowanej wiedzy technicznej oraz ustawicznej iteracji, polegającej na testowaniu nowych algorytmów w różnych scenariuszach w ten sposób, aby upewnić się, że są one wystarczająco bezpieczne i skuteczne w praktyce. Kolejnym wyzwaniem jest zarządzanie kluczami kryptograficznymi związanymi z PQC, albowiem w przeciwieństwie do tradycyjnych metod kryptograficznych zarządzanie kluczami w PQC może być bardziej skomplikowane, co wymaga opracowania nowych narzędzi i procedur do tego potrzebnych, a to chociażby po to, aby umożliwić skuteczne zarządzanie kluczami oraz ich bezpieczną wymianę pomiędzy różnymi systemami[40].

Implementacja PQC wiąże się również z pewnymi wyzwaniami etycznymi, ponieważ rozwój technologii kryptograficznej, która jest odporna na ataki kwantowe, może prowadzić do zintensyfikowania wyścigu zbrojeń w dziedzinie cyberbezpieczeństwa. Tego rodzaju konkurencja może nieść ze sobą ryzyko eskalacji już dość wysokich napięć międzynarodowych oraz pogłębienia nierówności technologicznych między krajami rozwiniętymi a rozwijającymi się. Dodatkowo kwestia dostępu do technologii PQC może stać się przedmiotem debat, zwłaszcza w aspekcie równości i sprawiedliwości społecznej, tym bardziej, że istnieje duże ryzyko, że tylko najbogatsze kraje i korporacje będą w stanie wdrażać na bieżąco najnowsze technologie zabezpieczające, co może prowadzić do marginalizacji innych podmiotów na rynku globalnym. W związku z tym implementacja PQC w EUDI *Wallet* musi być przeprowadzona w sposób odpowiedzialny z uwzględnieniem zarówno aspektów technicznych, społecznych, jak i etycznych, zaś wprowadzenie tej technologii powinno być poprzedzone szeroką dyskusją na temat jej potencjalnych konsekwencji nie tylko w kręgach specjalistycznych, lecz także na forum publicznym, co obecnie nie jest niestety praktykowane.

PQC, choć obiecująca, nie jest rozwiązaniem ostatecznym, albowiem tak dynamiczny rozwój technologii kwantowej oraz innych zaawansowanych technik obliczeniowych może prowadzić do pojawienia się już wkrótce nowych zagrożeń, które będą wymagały dalszej adaptacji systemów bezpieczeństwa, dlatego też EUDI *Wallet* musi być przygotowany na ciągłe zmiany i ewolucję zagrożeń. Adaptacja do nowych zagrożeń będzie wymagała stałego monitorowania i analizy ryzyk związanych

[40] D. Chawla, P.S. Mehra, *A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions*, https://www.sciencedirect.com/science/article/abs/pii/S2542660523002731/ [dostęp: 31.08.2024].

z rozwojem technologii kwantowej. Konieczne będzie również wdrożenie mechanizmów pozwalających na szybką aktualizację systemów kryptograficznych, aby mogły one skutecznie odpowiadać na nowe wyzwania. W tym kontekście ważne będzie zbudowanie infrastruktury cyfrowej, która będzie cechowała się elastycznością. W tej kwestii zauważyć należy także, że technologia kryptograficzna jest tylko jednym z elementów zapewniających bezpieczeństwo cyfrowe, ponieważ kluczową rolę odgrywa tu przede wszystkim świadomość „najsłabszego ogniwa", a więc samych użytkowników i ich zdolności do odpowiedzialnego korzystania z narzędzi cyfrowych. Wprowadzenie PQC w EUDI *Wallet* będzie skuteczne tylko wtedy, gdy użytkownicy będą świadomi jego znaczenia i będą umieć z niego korzystać w sposób, który zapewni maksymalne bezpieczeństwo ich danych. Użytkownicy muszą zrozumieć, w jaki sposób nowe algorytmy kryptograficzne chronią ich dane oraz jakie kroki mogą podjąć, aby zwiększyć swoje bezpieczeństwo w cyfrowym świecie. Działania edukacyjne mogą obejmować kampanie informacyjne, szkolenia oraz dostęp do zasobów edukacyjnych, które będą pomagały użytkownikom w zrozumieniu technologii kryptograficznych. Świadomość użytkowników jest więc kluczowa dla zapobiegania atakom socjotechnicznym, które mogą stanowić poważne zagrożenie nawet w najbardziej zaawansowanych systemach kryptograficznych. Nawet najlepsze zabezpieczenia technologiczne mogą być nieskuteczne, jeśli użytkownicy nie będą przestrzegali podstawowych zasad bezpieczeństwa[41].

Ostatecznie wraz z rozwojem PQC i jego implementacją w EUDI *Wallet*, możemy spodziewać się także dalszych inicjatyw legislacyjnych (eIDAS 3.0?), które mogą obejmować zarówno szczegółowe wytyczne dotyczące implementacji PQC, jak i szersze ramy prawne dotyczące zarządzania technologiami kwantowymi.

Wnioski

Implementacja PQC w ramach EUDI *Wallet* stanowi bezprecedensowy krok w kierunku zabezpieczenia cyfrowej infrastruktury Unii Europejskiej na miarę zagrożeń nadchodzącej ery obliczeń kwantowych. W dobie intensywnych przemian technologicznych i coraz bardziej zaawansowanych zagrożeń cybernetycznych PQC jawi się nie tylko jako innowacyjny fundament zabezpieczeń kryptograficznych, lecz także jako nieodzowny element architektury cyberbezpieczeństwa, wspieranej regu-

[41] *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, https://csrc.nist.gov/publications/detail/nistir/8413/final/ [dostęp: 31.08.2024].

lacjami prawnymi takimi jak eIDAS 2, NIS 2 oraz CRA. Algorytmy postkwantowe, choć odporne na przyszłe zagrożenia ze strony komputerów kwantowych, wymagają od systemów takich jak EUDI *Wallet* zupełnie nowego podejścia do optymalizacji, szczególnie w kontekście urządzeń mobilnych, które stanowią ważny element ekosystemu cyfrowego UE, a to chociażby z uwagi na utrzymującą się tendencję wzrostową w aspekcie popularności tego rodzaju urządzeń oraz szerokiego wachlarza ich zastosowań. Jednocześnie konieczne jest wypracowanie rozwiązań pozwalających na płynne przejście od obecnie stosowanych metod kryptograficznych do nowych standardów PQC bez narażania systemów na luki bezpieczeństwa, które mogłyby zostać wykorzystane przez „cyberprzestępców".

Poza wyzwaniami technologicznymi i prawnymi wdrożenie PQC w EUDI *Wallet* niesie ze sobą istotne korzyści gospodarcze i społeczne. Wprowadzenie zabezpieczeń postkwantowych przyczyni się do wzrostu zaufania publicznego do usług cyfrowych, co z kolei może znacząco zwiększyć ich adopcję zarówno w sektorze prywatnym, jak i publicznym. Podniesienie poziomu bezpieczeństwa danych osobowych, integralności cyfrowych podpisów i zaufania do systemów transakcyjnych sprawi, że korzystanie z portfeli cyfrowych takich jak EUDI *Wallet* stanie się powszechne, przyczyniając się do budowy zintegrowanego jednolitego rynku cyfrowego w UE. Z technicznego punktu widzenia wdrożenie PQC będzie motorem napędowym innowacji, szczególnie w sektorach związanych z bezpieczeństwem cyfrowym, a także dla branż technologicznych odpowiedzialnych za rozwój nowych algorytmów i rozwiązań kryptograficznych. Długofalowe efekty tego procesu mogą obejmować ponadto wzrost konkurencyjności europejskich firm na rynku globalnym oraz stymulację nowych innowacyjnych rozwiązań w dziedzinie technologii postkwantowych.

Społeczna akceptacja PQC, a w szczególności jej implementacja w głównych systemach identyfikacji cyfrowej, będzie wymagała szeroko zakrojonych działań edukacyjnych. Konieczne jest uświadomienie obywatelom Unii Europejskiej, jakie korzyści płyną z zastosowania technologii kryptograficznych odpornych na ataki kwantowe oraz jak nowe standardy bezpieczeństwa będą chronić ich dane osobowe i transakcje w cyfrowym świecie. Transparentność w zakresie sposobu działania PQC, w połączeniu z zaawansowanymi mechanizmami ochrony prywatności, stanie się podstawą budowy zaufania społecznego, które będzie niezbędne dla sukcesu takich inicjatyw jak EUDI *Wallet*.

W dalszej perspektywie prawodawcy unijni mogą sięgnąć po nowe inicjatywy legislacyjne, w tym nie jest wykluczone, że powstanie eIDAS 3.0, którego przepisy będą jeszcze bardziej precyzyjne w zakresie wymogów dotyczących PQC oraz tech-

nologii kwantowych. Być może przyszłość przyniesie nie tylko standardy zabezpieczeń przeciwko komputerom kwantowym, ale również zupełnie nowe paradygmaty w obszarze ochrony danych oparte na technologiach, które dziś są jeszcze w fazie badań albo o których nie mamy nawet pojęcia.

Jednocześnie nie można zapominać o potencjalnych zagrożeniach związanych z nierównym dostępem do nowoczesnych technologii kryptograficznych. Istnieje ryzyko, że mniejsze kraje lub mniej rozwinięte sektory gospodarki mogą nie być w stanie szybko wdrożyć PQC z powodu braku zasobów, co może prowadzić do nierówności technologicznych na skalę globalną. W związku z tym wprowadzenie PQC musi iść w parze z międzynarodową współpracą i wsparciem finansowym dla mniej rozwiniętych regionów, tak aby zapewnić globalną koordynację i spójność w obszarze cyberbezpieczeństwa.

Podsumowując, kryptografia postkwantowa w EUDI *Wallet* to kamień milowy na drodze do zapewnienia długoterminowego bezpieczeństwa cyfrowego dla obywateli i instytucji UE. Mimo wyzwań technicznych i prawnych, które wiążą się z jej wdrożeniem, PQC stwarza wyjątkowe możliwości zarówno w kontekście zwiększenia poziomu ochrony danych, jak i wzmocnienia pozycji Europy na globalnej mapie innowacji technologicznych. Kluczem do sukcesu będzie jednak nie tylko zaawansowanie technologiczne, ale także harmonizacja międzynarodowych standardów, edukacja społeczeństwa oraz wielopłaszczyznowa współpraca między państwami członkowskimi i globalnymi partnerami. Tylko takie zintegrowane i kompleksowe podejście pozwoli na pełne wykorzystanie potencjału PQC i zapewnienie, że cyfrowy ekosystem UE będzie odporny na nadchodzące wyzwania ery kwantowej.

Bibliografia

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do trans akcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257/73 z 2014 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, *General Data Protection Regulation, GDPR*) (Dz. Urz. UE L 119 z 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków mających na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji) oraz uchylająca dyrektywę (UE) nr 2016/1148 (Dz. Urz. UE L 333/80 z 2022 r.).

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020.

Źródła internetowe

Chawla D., Mehra P.S., *A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions,* https://www.sciencedirect.com/science/article/abs/pii/S2542660523002731/ [dostęp: 31.08.2024].

Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D., *Report on Post-Quantum Cryptography*, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf [dostęp: 31.08.2024].

Entering the Quantum Era, https://www.ox.ac.uk/news/features/entering-quantum-era/ [dostęp: 31.08.2024].

Module-Lattice-Based Key-Encapsulation Mechanism Standard, https://csrc.nist.gov/pubs/fips/203/final/ [dostęp: 31.08.2024].

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat, https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat/ [dostęp: 31.08.2024].

Post-Quantum Cryptography: Current Status and Next Steps, https://csrc.nist.gov/publications/detail/nistir/8105/final [dostęp: 30.08.2024].

Shor P.W., *Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf/ [dostęp: 31.08.2024].

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/pubs/ir/8309/final [dostęp: 31.08.2024].

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/publications/detail/nistir/8413/final/ [dostęp: 31.08.2024].

Toward a code-breaking quantum computer, https://www.sciencedaily.com/releases/2024/08/240823120024.htm/ [dostęp: 30.08.2024].

What Is Post-Quantum Cryptography?, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography/ [dostęp: 31.08.2024].

What is the EU Digital Identity Wallet, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet/ [dostęp: 30.08.2024].

Literatura

Alkim E., Ducas L., Pöppelmann T., Schwabe P., *Post-Quantum Key Exchange – A New Hope*, 25th USENIX Security Symposium (USENIX Security 16), 2016.

Bernstein D.J., Buchmann J., Dahmen E., *Post-Quantum Cryptography*, Springer 2009.

Hankerson D., Menezes A., Vanstone S., *Guide to Elliptic Curve Cryptography*, 2004, http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Guide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf/ [dostęp: 31.08.2024].

Kapcia P., *Kryptosystemy oparte na problemach trudnych obliczeniowo z wyszczególnieniem problemu faktoryzacji liczb całkowitych*, „Elektrotechnika i Elektronika" 2005, t. 24, nr 2.

Mosca M., *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, „IEEE Security & Privacy" 2018, vol. 16(5).

Schneier B., *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, wyd. 2, Warszawa 2002.

Stallings W., *Cryptography and Network Security: Principles and Practice*, Pearson 2014, https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf/ [dostęp: 31.08.2024].

Implementation of post-quantum cryptography within EUDI Wallet as an element of eIDAS 2 – legal, technical challenges and cybersecurity implications in the context of CRA and NIS 2 regulations

Abstract

This article examines the importance of post-quantum cryptography (PQC) in the context of the post-quantum reality, emphasizing its role as a foundation for future digital security. It also examines the challenges related to the implementation of PQC in key European projects such as the European Digital Identity Wallet (EUDI Wallet), which is set to become a central element of the European Union (EU) digital ecosystem. In the post-quantum era, PQC will not only be a tool for protection against new threats, but also a key element of legal regulations, such as eIDAS 2 and NIS 2, aimed at ensuring the security and interoperability of digital systems in the EU. The paper emphasizes the importance of harmonization of international regulations and global cooperation, which are necessary for the effective implementation of PQC, ensuring resilience to threats resulting from future developments in quantum technology.

Keywords

Post-quantum cryptography, digital security, cryptographic algorithms, EUDI Wallet, interoperability, cybersecurity, quantum technology, eIDAS 2, NIS 2