Studia Administracyjne 10/2018 | ISSN: 2080-5209 | www.wnus.edu.pl/sa | DOI: 10.18276/sa.2018.10-12 | s. 169–186

Karol Sroka

Uniwersytet Szczeciński
Wydział Prawa i Administracji
e-mail: karol.sroka@usz.edu.pl

Uwarunkowania bezpieczeństwa podpisu elektronicznego

STRESZCZENIE

W Unii Europejskiej wprowadzana jest reforma uwarunkowań prawnych i standaryzacyjnych dotyczących podpisu elektronicznego. Działania te mają na celu wprowadzenie jednolitego traktowania i uznawania usług zaufania na rynku międzynarodowym zwłaszcza przez instytucje sektora publicznego. Jednym z efektów tego procesu może być upowszechnienie i zwiększenie obszarów stosowalności procedur i infrastruktury podpisu elektronicznego. Celem artykułu jest analiza uwarunkowań istotnie wpływających na bezpieczeństwo transakcji cyfrowych realizowanych z wykorzystaniem podpisu elektronicznego w sytuacji ukształtowanej wejściem w życie przepisów rozporządzenia Parlamentu Europejskiego Rady Unii Europejskiej w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym powoływanego dalej jako eIDAS (ang.: *electronic identification and trust services*)[1].

SŁOWA KLUCZOWE

podpis elektroniczny, bezpieczeństwo informacji, administracja publiczna

Wprowadzenie

Od 1 lipca 2016 r. obowiązują przepisy rozporządzenia Parlamentu Europejskiego Rady Unii Europejskiej eIDAS, które określają zasady wzajemnego uznawania środków identyfikacji elektronicznej, warunki notyfikowania systemów identyfikacji elektronicznej, poziomy bezpieczeństwa systemów identyfikacji elektronicznej, zasady odpowiedzialności za szkody oraz zasady współpracy państw członkowskich.

Jednym z podstawowych celów rozporządzenia eIDAS jest „zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami

1 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, (Dz.Urz. UE L 257/73, 28.08.2014).

i organami publicznymi"[2] przez zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania. W drugiej połowie 2018 r. wchodzą w życie regulacje rozporządzenia związane z notyfikowanymi środkami (systemami) identyfikacji elektronicznej przez wszystkie państwa członkowskie. Celem tych prac jest wprowadzenie jednolitego traktowania i uznawania usług zaufania na rynku międzynarodowym zwłaszcza przez instytucje sektora publicznego[3].

W artykule 3 eIDAS zdefiniowano identyfikację elektroniczną jako proces używania danych w postaci elektronicznej, identyfikujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną. Natomiast uwierzytelnianie określono jako proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych. Zatem uwierzytelnianie to w istocie weryfikacja deklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych.

W rozporządzeniu eIDAS ustanowiono także ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług potwierdzonych doręczeń elektronicznych, usług certyfikacyjnych do celu uwierzytelniania witryn internetowych. Wprowadzono uznawalność kwalifikowanych pieczęci wydawanych w państwach członkowskich.

Wejście w życie rozporządzenia eIDAS spowodowało uchylenie polskiej ustawy o podpisie elektronicznym z 2001 r.[4] oraz ustanowienie ustawy o usługach zaufania[5], która wprowadziła wiele uprawnień dla ministra właściwego ds. informatyzacji (obecnie ministra cyfryzacji), związanych m.in. z certyfikowaniem dostawców usług zaufania oraz prowadzeniem stosownych rejestrów.

Jednym z efektów tego procesu może być upowszechnienie i zwiększenie obszarów stosowalności procedur i infrastruktury podpisu elektronicznego. Zasadne jest zatem ponowne przeanalizowanie uwarunkowań wpływających istotnie na bezpieczeństwo korzystania z elektronicznych metod identyfikacji i uwierzytelniania.

Rodzaje podpisu elektronicznego według projektu rozporządzenia eIDAS

W rozporządzeniu eIDAS podpis elektroniczny oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu. Ustanowiony w uchylonej ustawie o podpisie elektronicznym bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu[6] został redefiniowany jako kwalifikowany podpis elektroniczny – „zaawansowany

2 *Ibidem*.

3 P. Chaber, *Rozporządzenie eIDAS wprowadza nowy rozdział w budowaniu e-usług*, Portal Innowacji, online: http://www.pi.gov.pl/PARP/chapter_86197.asp?soid=D1547EEB6C0A40B8804E897CFDED2A7E (dostęp 30.08.2018).

4 Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (uchylona) (Dz.U. z 2001 nr 130 poz. 1450).

5 Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz. 1579).

6 Zob. art. 3 pkt. 2 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (uchylona) (Dz.U. z 2001 r., nr 130, poz. 1450).

podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego". Zaawansowany podpis elektroniczny oznacza podpis elektroniczny, który spełnia następujące wymogi:

a) w sposób unikatowy przyporządkowany podpisującemu;
b) umożliwia ustalenie tożsamości podpisującego;
c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą;
d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna[7].

Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu, a wydany w jednym państwie członkowskim jest uznawany za takowy również w pozostałych państwach członkowskich[8]. W związku z powyższym, organy administracji publicznej w Polsce od lipca 2016 r. zobowiązane są uznawać kwalifikowane podpisy elektroniczne wydane przez inne kraje członkowskie.

W odniesieniu do osób prawnych rozporządzenie eIDAS wprowadza kwalifikowaną pieczęć elektroniczną, której definicja jest zawarta w art. 3 pkt 25 rozporządzenia eIDAS i oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych. Oprócz dokumentów pieczęcie elektroniczne mogą być również używane do uwierzytelniania wszelkich zasobów cyfrowych, takich jak kod oprogramowania lub serwery[9].

Rozporządzenie eIDAS wprowadza trzy rodzaje pieczęci elektronicznych: pieczęć elektroniczną, zaawansowaną pieczęć elektroniczną oraz kwalifikowaną pieczęć elektroniczną, będące odpowiednikami podpisu elektronicznego, zaawansowanego podpisu elektronicznego oraz kwalifikowanego podpisu elektronicznego.

Zarówno kwalifikowany podpis elektroniczny, jak i kwalifikowana pieczęć elektroniczna, należą do kategorii tzw. kwalifikowanych usług zaufania. Przymiot „kwalifikowany" oznacza, że po wydaniu certyfikatu przez uprawnione organy administracji publicznej, mogą one wywoływać określone skutki prawne. Skutki prawne pieczęci elektronicznej normuje art. 35 rozporządzenia eIDAS. Pieczęci elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że pieczęć ta ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych pieczęci elektronicznych. Kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich oraz korzysta

7 Art. 26 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…

8 *Ibidem*, art. 25, ust. 2 i 3.

9 A. Zwolińska, D. Szostek, *E-pieczęć uwierzytelni firmowe i urzędowe dokumenty*, „Rzeczpospolita" 23.03.2016, online: https://www.rp.pl/Opinie/303239980-E-pieczec-uwierzytelni-firmowe-i-urzedowe-dokumenty.html (dostęp 21.08.2018).

z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana[10].

W ujęciu technicznym proces tworzenia pieczęci i podpisu elektronicznego jest identyczny – odbywa się przez wykonanie analogicznych przekształceń matematycznych. Różnica dotyczy aspektu formalno-proceduralnego – w przypadku bowiem podpisów elektronicznych w stosownym certyfikacie w polu „subject" zapisuje się imię, nazwisko i PESEL świadczeniobiorcy, natomiast w przypadku pieczęci elektronicznej są to atrybuty osoby prawnej, np. nazwa, REGON.

Wspomniany certyfikat jest to dokument elektroniczny stanowiący zaświadczenie elektroniczne o określonym terminie ważności, które zawiera dane identyfikujące podpisującego oraz klucz publiczny, czyli dane służące do sprawdzenia autentyczności podpisu elektronicznego złożonego za pomocą klucza prywatnego, czyli danych, nad którymi wyłącznie podpisujący ma kontrolę. „Kwalifikowany certyfikat podpisu elektronicznego" oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I rozporządzenia eIDAS. Prawdziwość danych potwierdzona jest przez wystawcę jego elektroniczną pieczęcią.

Uwierzytelnianie przy użyciu podpisu elektronicznego

Uwierzytelnienie użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty publiczne określone w art. 2 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r., nr 64, poz. 565, z 2017 r., poz. 570, z 2018 r., poz. 1000) wymaga:

a) użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub (Nowe brzmienie pkt 1 ust. 1 w art. 20a wejdzie w życie z dn. 29.09.2018 r. (Dz.U. z 2016 r., poz. 1579),
b) profilu zaufanego ePUAP, lub
c) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego[11].

W art. 3 pkt 10 w rozporządzeniu eIDAS zdefiniowano dokument elektroniczny jako każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne. Dokument elektroniczny, który powstaje jako udokumentowanie czynności prawnej, jest podpisywany podpisem elektronicznym. Jak już wspomniano, skutek prawny równoważny podpisowi własnoręcznemu ma kwalifikowany podpis elektroniczny[12].

Zgodnie z art. 63 § 3a. Kodeksu postępowania administracyjnego podanie wniesione w formie dokumentu elektronicznego powinno być opatrzone kwalifikowanym podpisem

10 Zob. art. 35, pkt 1–3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…

11 Art. 20a. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r., nr 64, poz. 565; z 2017 r., poz. 570; z 2018 r. poz. 1000).

12 Art. 25 ust. 2 i 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…

elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, lub uwierzytelniane w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej[13].

Kwalifikowany podpis elektroniczny nadaje się zatem do ostatecznego podpisywania podań, decyzji administracyjnych, postanowień i wszelkich dokumentów, które w wersji nieelektronicznej (papierowej) opatrzono by podpisem własnoręcznym.

Procedura składania podpisu elektronicznego

W procesie składania podpisu elektronicznego stosuje się asymetryczne algorytmy kryptograficzne z parą wzajemnie uzupełniających się kluczy: kluczem prywatnym i kluczem publicznym. Dane zaszyfrowane za pomocą jednego z kluczy mogą zostać odszyfrowane wyłącznie z wykorzystaniem klucza komplementarnego. Umożliwia to realizację działań zapewniających poufność, weryfikację autentyczności oraz potwierdzanie tożsamości nadawcy elektronicznych wiadomości przetwarzanych w systemach teleinformatycznych[14].

Popularnym asymetrycznym algorytmem kryptograficznym stosowanym w procedurze tworzenia podpisu elektronicznego jest algorytm RSA. Został on zaprojektowany w 1977 r. przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana i został po raz pierwszy opublikowany w 1978 r. Jeden z kluczy, który nazwano publicznym, jest jawny. Klucz prywatny – tajny jest przechowywany na zabezpieczonej przed kopiowaniem karcie kryptograficznej i dostępny tylko jego właścicielowi.

Powiązanie klucza publicznego z daną osobą potwierdza certyfikat wydawany przez instytucję certyfikacyjną[15]. Klucze prywatne związane z kwalifikowanymi certyfikatami, mogą być przetwarzane wyłącznie w urządzeniach spełniających wymogi, o których mowa w Decyzji wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiającej normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia eIDAS. Wymagania, którym powinny odpowiadać kwalifikowane urządzenia do składania podpisów elektronicznych oraz kwalifikowane urządzenia do weryfikacji podpisów elektronicznych, unormowano w załączniku II rozporządzenia eIDAS[16]. Są to m.in. warunki techniczne, określona struktura podpisu, użyte algorytmy kryptograficzne (szyfrowania oraz skrótu dokumentu). Kwalifikowane urządzenie, którym najczęściej jest procesorowa karta kryptograficzna,

13 Art. 63 § 3a Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r., nr 30, poz. 168; Dz.U. z 2017 r., poz. 1257; z 2018 r., poz. 149, 650).

14 G. Kozieł, *Podpis elektroniczny – rozwiązania techniczne i uwarunkowania prawne*, „Kolegium Analiz Ekonomicznych" 2014, nr 33, s. 265–280.

15 M. Marucha-Jaworska, *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Wolters Kluwer, Warszawa 2015, s. 61.

16 Rozporządzenie Wykonawcze Komisji (UE) 2015/1502 dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L. 235 z 9.09.2015, s. 112).

zapewnia ochronę klucza prywatnego w taki sposób, że nie jest możliwe jego przejęcie i wykorzystanie w nieuprawniony sposób. Standardowo dostęp do klucza jest zabezpieczony kodem PIN. Zamiast kodu PIN możliwe jest stosowanie innych zabezpieczeń, np. podpisów biometrycznych.

Certyfikat kwalifikowany można uzyskać w jednym z kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Aktualnie w Polsce pięć firm oferuje wydawanie certyfikatów kwalifikowanych i zestawów do składania kwalifikowanego podpisu elektronicznego. Są to: Centrum Obsługi Podpisu Elektronicznego, Krajowa Izba Rozliczeniowa S.A., CERTUM – Powszechne Centrum Certyfikacji, Polska Wytwórnia Papierów Wartościowych SA (Sigillum), Centrum Certyfikacji EuroCert Sp. z o.o. oraz Centrum Certyfikacji Kluczy CenCert Enigma Systemy Ochrony Informacji Sp. z o.o.[17]

Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne prowadzi Narodowe Centrum Certyfikacji, które pełni funkcję głównego urzędu certyfikacji dla infrastruktury podpisu elektronicznego w Polsce. Narodowe Centrum Certyfikacji to system informatyczny Narodowego Banku Polskiego zbudowany w celu realizacji zadań powierzonych NBP przez ministra właściwego do spraw informatyzacji zgodnie z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz. 1579)[18].

Wymienione instytucje (urzędy certyfikacyjne [CA], urzędy rejestracyjne [RA]), subskrybenci certyfikatów (użytkownicy), oprogramowanie i sprzęt tworzą infrastrukturę kluczy publicznych PKI (Public Key Infrastructure)[19], której podstawowym zadaniem jest zapewnienie bezpiecznego i skutecznego zarządzania kluczami oraz certyfikatami. Podstawowym dokumentem PKI jest certyfikat klucza publicznego. Aktualny główny certyfikat Narodowego Centrum Certyfikacji jest udostępniony na stronie internetowej centrum. Klucz publiczny algorytmu RSA ma długość 4096 bitów, algorytm wyznaczania wartości skrótu to SHA512, okres ważności certyfikatu to 9.12.2016–10.12.2039[20].

Klucz publiczny służy zatem do weryfikacji e-podpisu i może zostać rozpowszechniony, np. poprzez stronę internetową, bazę urzędu certyfikacji lub z wykorzystaniem certyfikatu.

Zasady wydawania certyfikatów kwalifikowanych są szczegółowo sformułowane w polityce certyfikacji dla kwalifikowanych certyfikatów kwalifikowanych dostawców usług zaufania[21]. Do wydania certyfikatu kwalifikowanego niezbędne jest potwierdzenie tożsa-

17 Narodowe Centrum Certyfikacji, *Rejestr podmiotów kwalifikowanych świadczących usługi certyfikacyjne*, online: http://www.nccert.pl (dostęp 19.08.2018).

18 Narodowe Centrum Certyfikacji, online: https://www.nccert.pl/index.htm (dostęp 24.08.2018).

19 *The public-key infrastructure (PKI) is the infrastructure established to support the issuing, revocation and validation of public-key certificates*; zob. International Telecommunication Union, telecommunication standardization sector of ITU, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks Recommendation ITU-T X.509,* 10/2016, s. 9, online: https://www.itu.int/rec/T-REC-X.509-201610-I/en (dostęp 9.09.2018).

20 Zob. https://www.nccert.pl/ (dostęp 9.09.2018).

21 Przykładowo: EuroCert Sp. z o.o. Centrum EUROCERT, *Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług zaufania EuroCert Wersja 1*, online: https://eurocert.pl/repozytorium/1.%20Polityka%20Certyfikacji/aktualne/0-PT-025-01-Polit_certyf_i_kodeks_post_certyf_kwalif_usl_EuroCert.pdf (dostęp 04.02.2019) lub ENIGMA Systemy Ochrony Informacji Sp. z o.o. CenCert *Polityka certyfikacji dla kwalifikowanych usług zaufania* (dostęp 4.02.2019).

mości osoby ubiegającej się o podpis elektroniczny i wymaga to osobistego stawienia się w punkcie rejestracji lub notarialnego potwierdzenia tożsamości. W przypadku, gdy osoba ubiegająca się o wydanie lub przedłużenie czasu ważności certyfikatu kwalifikowanego ma już ważny podpis kwalifikowany, może się nim posłużyć w zgłoszeniu certyfikacyjnym.

W skład typowego zestawu do składania kwalifikowanego podpisu elektronicznego wchodzą: czytnik kart kryptograficznych, karta kryptograficzna oraz zapisany na karcie certyfikat, który zawiera parę kluczy asymetrycznego algorytmu kryptograficznego, a także informacje o osobie, na którą jest wystawiony. Przy wystawianiu i wydawaniu certyfikatu weryfikowana jest tożsamość osoby. Dostarczane jest także oprogramowanie służące do obsługi czytnika kart kryptograficznych oraz do składania i weryfikacji podpisów elektronicznych[22].

W pewnym uproszczeniu procedurę tworzenia podpisu elektronicznego można podzielić na etap obliczania funkcji skrótu wiadomości (dokumentu w formie elektronicznej), szyfrowanie wyznaczonej wartości funkcji skrótu asymetrycznym algorytmem kryptograficznym z użyciem klucza prywatnego, znakowanie czasem, dołączenie certyfikatu, weryfikację podpisu elektronicznego[23].

Obliczenie wartości funkcji skrótu

Pierwszy etap to obliczenie skrótu podpisywanego dokumentu elektronicznego. Wygenerowanie z podpisywanego pliku tzw. skrótu to jednokierunkowe przekształcenie matematyczne zamieniające ciąg bitów dowolnej długości w inny ciąg bitów o ustalonej długości. Funkcja skrótu (funkcja haszująca) generuje unikalną wartość (skrót) dla konkretnych danych. Aktualnie w tym celu stosuje się funkcję skrótu z rodziny SHA-2[24].

Argumentem jednokierunkowej funkcji skrótu H(M) jest wiadomość M w formie cyfrowej o dowolnej długości wyrażonej w bitach. Wartością tej funkcji jest liczba *h* o ustalonej długości *h=H(M)*, której wartość zależy od wiadomości *M*. Zastosowanie funkcji skrótu zapewnia możliwość weryfikacji integralności podpisanego dokumentu. Jakakolwiek zmiana dokumentu powoduje bowiem istotną zmianę wartości funkcji skrótu[25].

Szyfrowanie wartości funkcji skrótu – algorytm RSA

W kolejnym etapie obliczony skrót jest szyfrowany z wykorzystaniem asymetrycznego algorytmu kryptograficznego. Popularnym asymetrycznym algorytmem kryptograficznym

22 J. Janowski, *Podpis elektroniczny w obrocie prawnym*, Wolters Kluwer, Warszawa 2007, s. 129, 149.

23 Obszerniej: R. Kossowski, *Podpis cyfrowy klasyfikacja i standardy*, „Prawo Europejskie" 2003, nr 10, s. 103–107.

24 SHA-2 (Secure Hash Algorithm) – zestaw kryptograficznych funkcji skrótu (SHA-224, SHA-256, SHA-384, SHA-512) zaprojektowany przez National Security Agency (NSA) i opublikowany w 2001 r. przez National Institute of Standards and Technology (NIST) jako federalny standard przetwarzania informacji rządu Stanów Zjednoczonych. SHA-2 składa się z zestawu czterech funkcji dających skróty wielkości 224, 256, 384 lub 512 bitów.

25 R. Poznański, D. Wachnik, *Podpis elektroniczny – prawo i rzeczywistość*, „Czas Informacji" 2011, nr 2, s. 25.

jest algorytm RSA, opublikowany w 1978 r. przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jest to powszechnie znany i szeroko opisywany w literaturze algorytm, który można stosować zarówno do szyfrowania, jak i do podpisów cyfrowych[26].

Warunkiem wykonania operacji szyfrowania jest uwierzytelnienie karty kryptograficznej z zapisanym kluczem prywatnym. W tym celu można zastosować kod PIN lub podpis biometryczny.

Zaszyfrowana funkcja skrótu jest dołączana do oryginalnego dokumentu. Dodatkowo do dokumentu oraz zaszyfrowanego skrótu dodany zostaje certyfikat zawierający m.in. dane osoby składającej podpis oraz jej klucz publiczny.

Znakowanie czasem

Czas złożenia podpisu elektronicznego w wielu zastosowaniach ma decydujące znaczenie. Rozporządzenie eIDAS definiuje elektroniczny znacznik czasu jako dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie. Czasem urzędowym na obszarze Rzeczypospolitej Polskiej jest czas środkowoeuropejski zwiększony o jedną godzinę w stosunku do uniwersalnego czasu koordynowanego UTC[27](PL)[28].

Kwalifikowany elektroniczny znacznik czasu wiąże datę i czas z danymi, tak aby wykluczyć możliwość niewykrywalnej zmiany danych; oparty jest na źródle czasu powiązanym z uniwersalnym czasem koordynowanym oraz jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania, lub w inny równoważny sposób[29].

Znakowanie czasem zapewnia, że dokument elektroniczny istniał w danym momencie w danej formie. Sposób generowania znacznika czasu polega na utworzeniu skrótu z dokumentu (np. za pomocą funkcji SHA-2) i wysłaniu go do zaufanego centrum wydającego certyfikowane znaczniki. Tam do tego skrótu zostaje dołączony znacznik czasu (czyli bieżący czas) i z całości ponownie liczony jest skrót, który jest podpisywany za pomocą klucza prywatnego tego centrum. W ten sposób razem z dokumentem będzie przetwarzany i przechowywany odebrany od centrum znacznik czasu wraz z podpisem.

26 Zob. W. Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*, tł. A. Grażyński, Helion, Gliwice 2011, s. 346.

27 Obszerniej pojęcie uniwersalnego czasu koordynowanego definiuje Instytut Geodezji i Kartografii, online: http://www.igik.edu.pl/pl/a/Czas-uniwersalny (dostęp 26.08.2018).

28 Art. 2 Ustawy z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz.U. z 2004 r., nr 16, poz. 144).

29 Zob. artykuł 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…

Weryfikacja podpisu elektronicznego

Procedura weryfikacji podpisu elektronicznego polega m.in. na określeniu, czy podpis elektroniczny złożony został na podstawie ważnego certyfikatu i czy został zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez urząd certyfikacji certyfikacie, oraz czy podpisany dokument nie został zmodyfikowany po złożeniu e-podpisu[30].

W celu weryfikacji integralności porównuje się wartości funkcji skrótu obliczonej przez autora dokumentu (nadawcę wiadomości) z wartością funkcji skrótu wyznaczoną przez adresata dokumentu. Jeśli rozszyfrowany za pomocą klucza publicznego skrót dołączony do dokumentu jest równy skrótowi obliczonemu przez adresata, wtedy weryfikacja jest pozytywna. Gwarancję, że osoba, która użyła klucza prywatnego, jest tą, za którą się podaje, daje system certyfikacji kluczy. Certyfikacji dokonuje odpowiednie centrum certyfikacji – tzw. zaufana trzecia strona (Trusted Third Party), której zadaniem jest wydawanie i zarządzanie certyfikatami, poświadczający autentyczność danego klucza publicznego. Certyfikat cyfrowy zawiera unikatowy numer seryjny, tożsamość urzędu certyfikacji wydającego certyfikat, okres ważności certyfikatu, identyfikator właściciela certyfikatu (imię, nazwisko, pseudonim, e-mail itp.), klucz publiczny właściciela certyfikatu i podpis cyfrowy urzędu certyfikacji potwierdzający autentyczność certyfikatu.

Artykuł 18 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej stanowi, że podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu[31]. Po tym czasie certyfikat staje się nieważny i podpisy złożone po upłynięciu terminu ważności są automatycznie weryfikowane negatywnie. Możliwe jest także unieważnienie lub zawieszenie certyfikatu. Jeżeli kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty postanowi unieważnić certyfikat, rejestruje on takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku[32]. Unieważnienie certyfikatu weryfikuje się na podstawie list unieważnionych certyfikatów CRL (ang. Certificate Revocation List). Przyjmuje się że listy CRL są aktualne, jeśli nie nastąpiła jeszcze data planowego wystawienia następnej listy[33]. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu. Cyfrowy podpis pod dokumentem wraz z dołączonym certyfikatem oznacza, że właściciel certyfikatu złożył podpis i tym samym zna treść dokumentu.

30 J. Janowski, *op. cit.*, s. 159.

31 Zob. art. 18 Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz. 1579).

32 Zob. artykuł 3 pkt 33 i 34 oraz art. 42 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…

33 Polityka Certyfikacji Narodowego Centrum Certyfikacji OID: 1.3.6.1.4.1.31995.3.3.3, wersja 3.3, Departament Bezpieczeństwa NBP, online: https://www.nccert.pl/dokumenty.htm#dPolityka (dostęp 15.08.2018).

Alternatywne technologie podpisu elektronicznego – elektroniczny podpis biometryczny

Postęp w obszarze technologii teleinformatycznych i praktyka posługiwania się dokumentami w formie elektronicznej spowodowały opracowanie nowych sposobów na ich podpisywanie. W uwarunkowaniach prawnych ukształtowanych przez rozporządzenie eIDAS interesującymi technologiami realizacji podpisu elektronicznego są metody biometryczne wykorzystujące biometryczny podpis odręczny, rejestrujące układ naczyń krwionośnych palca (*finger vein*), biometrię głosową czy biometrię twarzy[34].

Podpis biometryczny pozwala na identyfikację sygnatariusza, lecz nie zapewnia integralności danych nim opatrzonych, dlatego też podpis biometryczny można wykorzystać w procesie składania podpisu cyfrowego opartego na PKI zamiast numeru PIN zabezpieczającego dostęp do klucza prywatnego przechowywanego na karcie kryptograficznej[35].

Istotne czynniki wpływające na bezpieczeństwo podpisu elektronicznego

Bezpieczeństwo informacji przetwarzanej w systemach teleinformatycznych zależy od możliwości zapewnienia jej integralności, dostępności, poufności i autentyczności. Ważne jest także zachowanie takich cech jak: rozliczalność, autentyczność, niezaprzeczalność i niezawodność[36]. Dostępność to właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym. Integralność to właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony. Poufność to właściwość określająca, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym[37]. Przy czym zapewnienie poufności jest opcjonalne i może wynikać z przesłanek prawnych.

Zakładając, że ryzyko ujawnienia poufności klucza prywatnego przez jego właściciela jest stosunkowo łatwo kontrolować i zmniejszyć do akceptowalnego poziomu, bezpieczeństwo wiadomości i dokumentów podpisanych elektronicznie w największym stopniu zależy od stosowanej funkcji skrótu i algorytmu kryptograficznego[38].

34 Obszerniej: M. Marucha-Jaworska, *op. cit.*, s. 168–170.

35 M. Maciejewska-Szałas, *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, C.H. Beck, Warszawa 2014, s. 7.

36 J. Czekaj, *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012, s. 126–129.

37 Zob. § 2 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r., w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. nr 159, poz. 948).

38 „RSA – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Algorytm, który może być stosowany zarówno do szyfrowania jak i do podpisów cyfrowych. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców", zob. B. Schneier, *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, tł. R. Rykaczewski, R. Sobczak, P. Szpryngier, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, s. 572–581.

Bezpieczeństwo funkcji skrótu

Zastosowanie funkcji skrótu zapewnia możliwość weryfikacji integralności podpisanego dokumentu. Jakakolwiek zmiana dokumentu powoduje bowiem istotną zmianę wartości funkcji skrótu[39]. Bezpieczna kryptograficznie funkcja skrótu powinna zapewniać brak możliwości odtworzenia danych wejściowych na podstawie skrótu. Dla funkcji skrótu znalezienie wiadomości, która odpowiada podanemu skrótowi, nazywa się atakiem *preimage*. Drugi rodzaj ataku, czyli znalezienie dwóch różnych wiadomości o tym samym skrócie znany jest jako kolizja. Uznanie funkcji skrótu za bezpieczną do zastosowań kryptograficznych opiera się wyłącznie na domniemaniu odporności na znane ataki kryptoanalityczne, nie zaś na formalnych dowodach gwarantujących niemożność złamania. Istnienie jednokierunkowych funkcji nie zostało dotychczas dowiedzione[40]. W 2017 r. opracowano praktyczną metodę generowania kolizji SHA-1[41], w efekcie tego algorytm SHA-1 utracił rekomendację ETSI (zob. ETSI TS 119 312)[42]. W tej sytuacji konieczne jest odejście od stosowania algorytmu SHA-1 przy składaniu zaawansowanego, w tym kwalifikowanego, podpisu elektronicznego i pieczęci elektronicznej.

Zalecane algorytmy funkcji służących do generowania skrótu wiadomości są określone w federalnych standardach przetwarzania informacji: *FIPS 180-4, Secure Hash Standard*[43] i FIPS 180-4 określają rodzinę algorytmów funkcji skrótu SHA-2: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 i SHA-512/256. Cechą wyróżniającą te funkcje jest relatywnie duża długość skrótu wynosząca 512 bitów dla funkcji SHA-512.

W 2012 r. w ramach trwającego pięć lat konkursu ogłoszonego przez amerykański NIST uzyskano funkcję skrótu SHA-3 (Secure Hash Algorithm 3), która w przyszłości może zastąpić funkcję SHA-2[44]. W 2015 r. opracowano normę dla tej funkcji – zatem jest już możliwe jej stosowanie[45]. Standard FIPS 202, SHA-3 Standard charakteryzuje rodzinę funkcji SHA-3 i opisuje cztery algorytmy skrótu o stałej długości: SHA3-224, SHA3-256, SHA3-384 i SHA3-512 i dwie funkcje SHAKE128 i SHAKE256. Obecnie tylko cztery algorytmy SHA-3 o stałej długości są zatwierdzonymi algorytmami zapewniającymi perspektywiczną alternatywę dla rodziny funkcji skrótu SHA-2[46].

Fakty te uwzględniono w art. 137 ustawy z 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016, poz. 1579), który stanowi: „Do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci

39 R. Poznański, D. Wachnik, *op. cit.*, s. 25.

40 W. Nowakowski, R. Poznański, *Podpis elektroniczny – zasady działania*, „Elektronika" 2010 nr 7, s. 266.

41 M. Stevens *et al.*, *The first collision for full SHA-1*, CWI Amsterdam, Google Research, online: https://shattered.io/static/shattered.pdf (dostęp 30.08.2018).

42 *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*, ETSI TS 119 312 V1.2.1 (2017-05), online: https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf (dostęp 2.01.2019), s. 17.

43 *Secure Hash Standard (SHS)*, FIPS PUB 180-4, online: http://dx.doi.org/10.6028/NIST.FIPS.180-4 (dostęp 2.02.2019).

44 *NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition*, online: https://www.nist.gov/news-events/news/2012/10/nist-selects-winner-secure-hash-algorithm-sha-3-competition (dostęp 1.09.2018).

45 *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, FIPS PUB 202, online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (dostęp 1.09.2018).

46 *Ibidem*.

elektronicznych można stosować funkcję skrótu SHA-1, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu".

Konieczne jest zatem dostosowanie aplikacji służących do składania lub weryfikacji podpisu elektronicznego do algorytmów funkcji skrótu z rodziny SHA-2[47], które w najbliższych kilku latach można uznać za wystarczająco bezpieczne.

Bezpieczeństwo algorytmu RSA

Z istoty asymetrycznej procedury szyfrowania wynika potencjalna możliwość jej złamania. Znany od 1978 r. i powszechnie stosowany algorytm RSA od wielu lat jest przedmiotem bardzo licznych badań kryptoanalitycznych. Można zatem stwierdzić, że zarówno podatności, ryzyko zagrożeń, realne i potencjalne metody ataku, jak i działania, które podnoszą bezpieczeństwo korzystania z tego algorytmu są znane i opisane w wielu publikacjach. Jednym z podstawowych zagrożeń jest problem poufności klucza prywatnego. Jego nieuprawnione pozyskanie ma katastrofalne skutki – podpisy składane z wykorzystaniem skompromitowanego klucza prywatnego są nierozróżnialne od podpisów elektronicznych legalnego właściciela. Z tego powodu klucze prywatne generowane są na kartach elektronicznych posiadających odpowiedni certyfikat instytucji standaryzujących[48] i nie mogą zostać z nich wyeksportowane. Dostęp do operacji związanych z użyciem tych kluczy jest zabezpieczony kodem PIN lub podpisem biometrycznym[49].

Bezpieczeństwo algorytmu RSA zależy od długości i jakości zastosowanych kluczy[50]. Jest to związane ze znanymi trudnościami faktoryzacji dużych liczb[51]. Istnieją metody, które pozwalają na szybką faktoryzację w przypadku zastosowania liczb pierwszych konkretnego typu. Z tego właśnie powodu wprowadza się dodatkowe warunki na procedury generowania i parametry klucza RSA, których przestrzeganie zapewnia akceptowalny poziom ryzyka związany z bezpieczeństwem podpisu elektronicznego[52].

47 Komunikat Ministra Cyfryzacji z dnia 1 marca 2018 r. w sprawie wycofania algorytmu SHA-1 w zastosowaniach związanych z zaawansowanym podpisem i pieczęcią elektroniczną, NBP, online: https://www.nccert.pl/komunikaty2018.htm#k2018 (dostęp 19.08.2018).

48 *Security requirements for cryptographic modules*, FIPS PUB 140-2, online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf (dostęp 2.02.2019).

49 *PKI NBP – Polityka Certyfikacji dla certyfikatów „ESCB Podpis" OID: 1.3.6.1.4.1.31995.1.2.2.1 wersja 1.8*, NBP Departament Bezpieczeństwa, online: https://www.nbp.pl/pki/PC_podpis.pdf (dostęp 2.02.2019), s. 14–15.

50 P. Kotlarz, *Jak wzrost mocy obliczeniowej i postęp w badaniach matematycznych zagraża współczesnym rozwiązaniom bezpieczeństwa informatycznego*, XII Konferencja PLOUG Zakopane 2006, online: http://www.ploug.org.pl/wp-content/uploads/ploug-konferencja-12-09_Kotlarz.pdf (dostęp 20.09.2018).

51 K. Bartyzel, *Kryptografia asymetryczna i jej zastosowanie w algorytmach komunikacji*, docplayer.pl, online: https://docplayer.pl/7557429-Kryptografia-asymetryczna-i-jej-zastosowanie.html (dostęp 2.02.2019), s. 12, 13; R. Anderson, *Inżynieria zabezpieczeń*, tł. P. Carlson, Wydawnictwo Naukowo-Techniczne, Warszawa 2005, s. 122–123.

52 A. Chmielowiec, *Ataki na algorytm RSA*, CMM SIGMA, online: andrzej.chmielowiec.cmmsigma.eu/data/ataki_na_rsa.pdf (dostęp 6.09.2018).

Odkrycie szybkiej metody faktoryzacji bądź radykalne przyspieszenie obliczeń może spowodować, że algorytm RSA stanie się nieprzydatny[53]. Prawdopodobieństwo takiego zdarzenia jest istotne, ponieważ tempo zmian w zakresie stosowanych technologii jest bardzo duże.

Mirosław Kutyłowski ilustruje ten problem przykładem postępu w zakresie łamania RSA: „Początkowo wydawało się, że możliwe jest oszacowanie bezpiecznych parametrów kluczy służących do składania i do weryfikacji podpisu RSA. Okazało się jednak, że prognozy dotyczące bezpiecznej wielkości klucza bywały niedoszacowane – postęp algorytmów faktoryzacji był dużo szybszy od oczekiwań"[54].

Zabezpieczeniem przed atakami opartymi na znanych metodach faktoryzacji jest wyznaczanie kluczy opartych na dostatecznie dużych liczbach pierwszych generowanych zgodnie z zalecanymi w standardach procedurami.

Standard FIPS (Federal Information Processing Standard) 186-4, Digital Signature Standard (DSS)[55] określa trzy algorytmy podpisu cyfrowego zatwierdzone przez NIST: DSA, RSA i ECDSA. Wszystkie trzy są używane do generowania i weryfikowania podpisów cyfrowych w połączeniu z zatwierdzoną funkcją skrótu określoną w FIPS 180-4[56], Secure Hash Standard lub FIPS 202[57], SHA-3 Standard: Hash oparty na permutacji i Extendable-Output Functions. W chwili obecnej przewiduje się, że 2048-bitowe moduły RSA jeszcze przez co najmniej kilka lat będą znajdować się poza granicą możliwości rozłożenia ich na czynniki pierwsze przy zastosowaniu znanych metod i racjonalnych nakładów obliczeniowych[58, 59]. Odporność algorytmu na ataki inne niż faktoryzacja można zapewnić, stosując odpowiednie zalecenia dotyczące doboru kluczy, np. te znajdujące się w dokumentach NIST.

Podsumowanie

Wejście w życie rozporządzenia eIDAS stworzyło uwarunkowania prawne pozwalające na znaczne zwiększenie obszarów zastosowań podpisu elektronicznego. Ważnym zagadnieniem pozostaje złożona kwestia bezpieczeństwa podpisu elektronicznego. Jeśli z przetwa-

53 W. Nowakowski, *O bezpieczeństwie algorytmu RSA*, „Elektronika" 2012, nr 2, s. 80.

54 M. Kutyłowski, *Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny*, CBKE e-Biuletyn 2004, nr 3, online: http://www.bibliotekacyfrowa.pl/dlibra/docconten-t?id=24750 (dostęp 2.02.2019), s. 2.

55 *Digital Signature Standard (DSS)*, FIPS PUB 186-4, online: http://dx.doi.org/10.6028/NIST.FIPS.186-4 (dostęp 2.02.2019).

56 *Secure Hash Standard (SHS)…*

57 *SHA-3 Standard. Permutation-Based…*

58 W. Nowakowski, *op. cit.*, s. 80.

59 E. Barker, A. Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, (NIST Special Publication 800-131A Computer Security Division Information Technology Laboratory), U.S. Department of Commerce, National Institute of Standards and Technology, January 2011, online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-131a.pdf (dostęp 2.02.2019).

rzaniem[60] dokumentów elektronicznych[61] wiążą się określone skutki prawne lub finansowe, to konieczne jest zapewnienie bezpieczeństwa rozumianego jako zachowanie poufności, integralności i dostępności przetwarzanych informacji. Dodatkowo istotne jest zapewnienie autentyczności, rozliczalności, niezaprzeczalności i niezawodność transakcji w systemach teleinformatycznych. Wymienione atrybuty bezpieczeństwa można uzyskać, korzystając z procedur kwalifikowanego podpisu elektronicznego. Przypomniane w artykule cechy asymetrycznych algorytmów kryptograficznych i funkcji skrótu są niezwykle przydatne w procesach identyfikacji i uwierzytelniania oraz mechanizmach niezaprzeczalności.

Zastosowanie kryptografii asymetrycznej i PKI wraz z zabezpieczonym kodem PIN lub podpisem biometrycznym dostępem do klucza prywatnego pozwalają na osiągnięcie bardzo wysokiego poziomu wiarygodności uwierzytelnienia.

Niewątpliwie należy brać pod uwagę zagrożenia wiążące się z tą technologią. Wydaje się, że ryzyko związane z błędnym funkcjonowaniem urządzeń lub wadami oprogramowania, znane problemy związane z archiwizacją dokumentów w formie elektronicznej nie wpływają istotnie na poziom bezpieczeństwa transakcji elektronicznych. Stosowane w instytucji podpisu elektronicznego algorytmy asymetryczne i funkcje skrótu są starannie zbadane i zweryfikowane w praktyce. Znane są zarówno ryzyko zagrożeń, jak i mechanizmy zabezpieczające. Przygotowywane są rozwiązania umożliwiające bezpieczne korzystanie z podpisu elektronicznego w perspektywie wzrostu mocy obliczeniowych sprzętu komputerowego. Obiecująca wydaje się technika kryptografii asymetrycznej, zwana kryptografią krzywych eliptycznych ECC (ang. Elliptic Curve Cryptography), która może być zastosowana w miejsce algorytmu RSA. Algorytmy ECC oferują porównywalne bezpieczeństwo z RSA przy mniej złożonych kluczach. Klucz ECC o długości 160 bitów jest równie bezpieczny jak 1024-bitowy RSA. Zapewnia to znacznie wydajniejsze szyfrowanie w stosunku do RSA, który jest uważany za wolny i wymagający sporych mocy obliczeniowych[62].

W 2018 r. firma IBM zaprezentowała na targach CES 2018 w Las Vegas prototyp komputera kwantowego. W perspektywie wykorzystanie komputerów kwantowych może znacznie ułatwić złamanie powszechnie stosowanego mechanizmu klucza publicznego RSA. Jednak pomimo postępu w tym obszarze, komputery te wciąż nie mają praktycznego zastosowania, a problemy techniczne związane z koniecznością zapewnienia bardzo specjalistycznego środowiska ich pracy są bardzo dalekie od rozwiązania[63]. W sierpniu 2015 r. NSA[64] opubli-

60 Na podstawie art. 2 punkt 5 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., nr 182, poz. 1228), w artykule przyjęto, że przetwarzanie informacji „to wszelkie operacje wykonywane w odniesieniu do informacji […] i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie".

61 Zob. art. 3 punkt 35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.…: „dokument elektroniczny" oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

62 Zob. I. Blake, G. Seroussi, N. Smart, *Krzywe eliptyczne w kryptografii*, tł. W. Kraśkiewicz, Wydawnictwa Naukowo-Techniczne, Warszawa 2004.

63 Obszerniej: *IBM Building First Universal Quantum Computers for Business and Science*, online: https://www-03.ibm.com/press/us/en/pressrelease/51740.wss (dostęp 31.08.2018).

64 NSA – The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO).

kowało swoje oświadczenie w sprawie kryptografii post-kwantowej, gdzie zapowiedziano, że w niedalekiej przyszłości będzie przedstawiony zestaw kryptosystemów post-kwantowych. Do tego czasu użytkownicy powinni używać algorytmów wykorzystujących krzywe eliptyczne oraz RSA z kluczami minimum 3072 bitów[65].

Można zatem przyjąć, że stosowanie algorytmów dopuszczonych do użytkowania na podstawie standardu ETSI TS 119 312 V1.2.1 (2017-05) jest wystarczająco bezpieczne w perspektywie określonej w tymże standardzie. Dopuszcza się stosowanie algorytmów RSA lub DSA o długości kluczy nie mniejszej niż 2048 bitów do podpisu i uwierzytelnienia, albo ECDSA o długości krzywej nie krótszej niż 256 bitów (przy czym do podpisu i do uwierzytelnienia należy używać dwóch różnych par kluczy) oraz funkcji skrótu SHA-2 (co najmniej SHA-256). W perspektywie długoterminowego używania i tym samym możliwości pojawienia się doniesień o wykryciu podatności funkcji SHA-2 zaleca się implementację algorytmu SHA-3. W celu zwiększenia szybkości działania przy podpisie i weryfikacji podpisu sugeruje się użycie krzywych eliptycznych jako algorytmu podpisu.

Mimo wielu doniesień o próbach złamania procedur kryptograficznych, z których się korzysta, tworząc podpisy elektroniczne, można z całą odpowiedzialnością stwierdzić, że jego realizacja przy użyciu zalecanych algorytmów kryptograficznych jest nadal bardzo skutecznym i sprawdzonym sposobem zapewnienia integralności dokumentów elektronicznych i uwierzytelnienia ich pochodzenia.

Istotnym czynnikiem wpływającym na poziom bezpieczeństwa informacji przetwarzanej w systemach teleinformatycznych są ludzie. Według danych publikowanych przez działający w strukturach Naukowej i Akademickiej Sieci Komputerowej zespół CERT Polska średnia dzienna liczba zainfekowanych komputerów w polskich sieciach wynosiła w 2016 r. około 20 tys.[66]. Pomimo tak dużej liczby incydentów, bardzo wysoko ocenia się skuteczność dostępnych metod programowych i technicznych środków ochrony w tym podpisu elektronicznego. Zdecydowanie najsłabszym elementem systemów bezpieczeństwa jest czynnik ludzki[67]. Wydaje się, że jest to spowodowane m.in. brakiem w programach kształcenia kierunków studiów związanych z transakcjami cyfrowymi wystarczającej ilości zagadnień dotyczących omawianej problematyki bezpieczeństwa informacji[68]. Tymczasem bezpieczne korzystanie ze środków technicznych i programowych współczesnej teleinformatyki nie jest możliwe bez zrozumienia istoty ich funkcjonowania.

65 B. Schneler, *NSA Plans for a Post-Quantum World*, online: https://www.lawfareblog.com/nsa-plans-post-quantum-world, (dostęp 20.09.2018).

66 *Krajobraz bezpieczeństwa polskiego internetu 2016. Raport roczny z działalności CERT Polska*, NASK CERT.pl, online: https://www.cert.pl/PDF/Raport_CP_2017.pdf (dostęp 17.09.2018) s. 7.

67 A. Wilkowski, *O bezpieczeństwie internetowym*, „Studia Ekonomiczne" Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach 2015, nr 242, s. 242–243.

68 G. Wierczyński, W.R. Wiewiórowski, *Informatyka prawnicza. Nowoczesne technologie informacyjne w pracy prawników i administracji publicznej*, Wolters Kluwer, Warszawa 2016, s. 17.

Bibliografia

Anderson R., *Inżynieria zabezpieczeń*, tł. P. Carlson, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.

Barker E., Roginsky A., *Transitions. Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, (NIST Special Publication 800-131A Computer Security Division Information Technology Laboratory), U.S. Department of Commerce, National Institute of Standards and Technology, January 201, online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-131a.pdf (dostęp 2.02.2019).

Bartyzel K., *Kryptografia asymetryczna i jej zastosowanie w algorytmach komunikacji*, docplayer.pl online: https://docplayer.pl/7557429-Kryptografia-asymetryczna-i-jej-zastosowanie.html (dostęp 2.02.2019).

Blake I., Seroussi G., Smart N., *Krzywe eliptyczne w kryptografii*, tł. W. Kraśkiewicz, Wydawnictwa Naukowo-Techniczne, Warszawa 2004.

Chaber P., *Rozporządzenie eIDAS wprowadza nowy rozdział w budowaniu e-usług*, Portal Innowacji online: http://www.pi.gov.pl/PARP/chapter_86197.asp?soid=D1547EEB6C0A40B8804E897C-FDED2A7E (dostęp 30.08.2016).

Chmielowiec A., *Ataki na algorytm RSA*, CMM SIGMA, online: andrzej.chmielowiec.cmmsigma.eu/data/ataki_na_rsa.pdf (dostęp 6.09.2018).

Czekaj J., *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012.

Janowski J., *Podpis elektroniczny w obrocie prawnym*, Wolters Kluwer, Warszawa 2007.

Kossowski R., *Podpis cyfrowy klasyfikacja i standardy*, „Prawo Europejskie" 2003, nr 10.

Kotlarz P., *Jak wzrost mocy obliczeniowej i postęp w badaniach matematycznych zagraża współczesnym rozwiązaniom bezpieczeństwa informatycznego*, XII Konferencja PLOUG Zakopane 2006, online: http://www.ploug.org.pl/wp-content/uploads/ploug-konferencja-12-09_Kotlarz.pdf (dostęp 20.09.2018).

Kozieł G., *Podpis elektroniczny – rozwiązania techniczne i uwarunkowania prawne,* „Kolegium Analiz Ekonomicznych" 2014, nr 33, s. 265–280.

Kutyłowski M., *Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny*, CBKE e-Biuletyn 2004, nr 3, online: http://www.bibliotekacyfrowa.pl/dlibra/doccontent?id=24750 (dostęp 2.02.2019).

Maciejewska-Szałas M., *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, C.H. Beck, Warszawa 2014.

Marucha-Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Wolters Kluwer, Warszawa 2015.

Nowakowski W., *O bezpieczeństwie algorytmu RSA*, „Elektronika" 2012, nr 2.

Nowakowski W., Poznański R., *Podpis elektroniczny – zasady działania*, „Elektronika" 2010, nr 7.

Poznański R., Wachnik D., *Podpis elektroniczny – prawo i rzeczywistość*, „Czas Informacji" 2011, nr 2.

Schneier B., *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, tł. R. Rykaczewski, R. Sobczak, P. Szpryngier, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.

Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*, tł. A. Grażyński, Helion, Gliwice 2011.

Stevens M., Bursztein E., Karpman P., Albertini A., Markov Y., *The first collision for full SHA-1*, CWI Amsterdam, Google Research, online: https://shattered.io/static/shattered.pdf (dostęp 30.08.2018).

Wierczyński G., Wiewiórowski W.R., *Informatyka prawnicza. Nowoczesne technologie informacyjne w pracy prawników i administracji publicznej*, Wolters Kluwer, Warszawa 2016.

Wilkowski A., *O bezpieczeństwie internetowym*, „Studia Ekonomiczne" Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach 2015, nr 242.

Zwolińska A., Szostek D., *E-pieczęć uwierzytelni firmowe i urzędowe dokumenty*, „Rzeczypospolita" 23.03.2016, online: https://www.rp.pl/Opinie/303239980-E-pieczec-uwierzytelni-firmowe-i-urzedowe-dokumenty.html (dostęp 21.08.2018).

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 transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, (Dz.Urz. U.E. L 257/73, 28.08.2014).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r., w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. nr 159, poz. 948).

Rozporządzenie Wykonawcze Komisji (UE) 2015/1502 dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.Urz. UE L. 235 z 9.09.2015, s. 112).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r., nr 30, poz. 168; Dz.U. z 2017 r., poz. 1257; z 2018 r., poz. 149, 650).

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (uchylona) (Dz.U. z 2001 r., nr 130, poz. 1450).

Ustawa z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz.U. z 2004 r., nr 16, poz. 144).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r., nr 64, poz. 565; z 2017 r., poz. 570; z 2018 r., poz. 1000).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., nr 182, poz. 1228).

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz. 1579).

Raporty, rejestry, wykazy i inne dokumenty

Digital Signature Standard (DSS), FIPS PUB 186-4, online: http://dx.doi.org/10.6028/NIST.FIPS.186-4 (dostęp 2.02.2019).

Electronic Signatures and Infrastructures (ESI);Cryptographic Suites, ETSI TS 119 312 V1.2.1 (2017-05), online: https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf (dostęp 2.02.2019).

IBM Building First Universal Quantum Computers for Business and Science, online: https://www-03.ibm.com/press/us/en/pressrelease/51740.wss (dostęp 31.08.2018).

International Telecommunication Union, telecommunication standardization sector of ITU, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks Recommendation ITU-T X.509*, 10/2016, online: https://www.itu.int/rec/T-REC-X.509-201610-I/en (dostęp 9.09.2018).

Komunikat Ministra Cyfryzacji z dnia 1 marca 2018 r. w sprawie wycofania algorytmu SHA-1 w zastosowaniach związanych z zaawansowanym podpisem i pieczęcią elektroniczną, NBP, online: https://www.nccert.pl/komunikaty2018.htm#k2018 (dostęp 19.08.2018).

Krajobraz bezpieczeństwa polskiego internetu 2016. Raport roczny z działalności CERT Polska, NASK CERT.pl, online: https://www.cert.pl/PDF/Raport_CP_2017.pdf (dostęp 17.09.2018).

NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition, online: https://csrc.nist.gov/projects/hash-functions/sha-3-project (dostęp 1.09.2018).

PKI NBP – Polityka Certyfikacji dla certyfikatów „ESCB Podpis" OID: 1.3.6.1.4.1.31995.1.2.2.1 wersja 1.8, NBP Departament Bezpieczeństwa, online: https://www.nbp.pl/pki/PC_podpis.pdf (dostęp 2.02.2019).

Polityka Certyfikacji Narodowego Centrum Certyfikacji OID: 1.3.6.1.4.1.31995.3.3.3, wersja 3.3, Departament Bezpieczeństwa NBP, online: https://www.nccert.pl/dokumenty.htm#dPolityka (dostęp 5.08.2018).

Rejestr podmiotów kwalifikowanych świadczących usługi certyfikacyjne, Narodowe Centrum Certyfikacji, online: http://www.nccert.pl (dostęp 19.08.2018).

Secure Hash Standard (SHS), FIPS PUB 180-4, online: http://dx.doi.org/10.6028/NIST.FIPS.180-4.

Security requirements for cryptographic modules, FIPS PUB 140-2 online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf (dostęp 2.02.2019).

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (dostęp 1.09.2018).

E-Signature Security Requirements for Digital Transactions

SUMMARY

The European Union is reforming the legal and standardization conditions for electronic signatures. The aim of this work is to introduce uniform treatment and recognition of trust services on the international market, especially by public sector institutions. One of the effects of this process may be the dissemination and increase of the areas of applicability of procedures and electronic signature infrastructure. The article attempts to identify the most important factors determining the security of using these tools.

KEYWORDS

electronic signature, electronic document, public administration