Studia Administracyjne 8/2016 | ISSN: 2080-5209 | www.wnus.edu.pl/sa | DOI: 10.18276/sa.2016.8-08 | s. 109–122

Karol Sroka

Zamiejscowy Wydział Społeczno-Ekonomiczny w Gorzowie Wielkopolskim
Uniwersytet Szczeciński
e-mail: karol.sroka@usz.edu.pl

Podpis elektroniczny a identyfikacja i uwierzytelnianie

STRESZCZENIE

Istotnym etapem każdej transakcji wykonywanej w środowisku systemów teleinformatycznych jest identyfikacja stron i ich uwierzytelnienie. W artykule analizowano możliwość wykorzystania kwalifikowanego podpisu elektronicznego jako powszechnego narzędzia identyfikacji i uwierzytelniania.

SŁOWA KLUCZOWE

podpis elektroniczny, identyfikacja, uwierzytelnianie, administracja publiczna

Wprowadzenie

Funkcjonowanie współczesnych instytucji administrujących odbywa się z wykorzystaniem metod i środków technicznych teleinformatyki. Istotnym etapem każdej transakcji wykonywanej w środowisku systemów teleinformatycznych jest identyfikacja stron i ich uwierzytelnienie z adekwatnym do realizowanej usługi poziomem bezpieczeństwa. Identyfikacja to proces przypisania identyfikatora do osoby oraz potwierdzenie tożsamości osoby na podstawie identyfikatora. Proces uwierzytelnienia polega na wykazaniu, że użytkownik e-usługi posługujący się danym identyfikatorem jest faktycznie tą osobą, która została zadeklarowana i zidentyfikowana.

Obecnie brakuje uniwersalnych modeli uwierzytelnienia spełniających obowiązujące normy prawne i standardy techniczne, które byłyby akceptowane przez wystarczająco liczną grupę użytkowników. Skutkiem takiego stanu rzeczy jest rozwój nowych modeli uwierzytelnienia, funkcjonujących bez wystarczających podstaw prawnych lub normatywnych, jednak rozwijających się dzięki temu, że odpowiadają potrzebom swych twórców i odbiorców. Polskie instytucje administrujące i dostawcy usług elektronicznych oferują własne specyficzne procedury identyfikacji i uwierzytelniania. Są to różne procedury wykorzystujące login i hasło, a także tak zwane zdrapki, piny, puki, tokeny, karty, smsy i narzędzia

biometryczne[1]. W efekcie użytkownicy systemów teleinformatycznych muszą korzystać z wielu różnych identyfikatorów elektronicznych, środków i metod uwierzytelnienia.

W bankowości, w przypadku zdalnego zawierania nowej umowy, można ustalić tożsamość klienta na podstawie transakcji przeprowadzonej za pośrednictwem istniejącego rachunku klienta[2]. Najbardziej powszechną metodą identyfikacji i uwierzytelnienia użytkowników bankowości elektronicznej jest weryfikacja wydanego klientowi identyfikatora oraz statycznego hasła o określonej złożoności, które dodatkowo może być potwierdzane stosowanym w danym banku narzędziem autoryzacji (np. hasła jednorazowe). Procedury autoryzacji w polskich bankach polegają na przypisaniu określonego zakresu czynności użytkownika do jedno- lub dwuczynnikowego uwierzytelnienia, gdzie do jednoczynnikowego zalicza się najczęściej udane logowanie poprzez podanie poprawnej pary identyfikatora i hasła, a dwuczynnikowe jest wzbogacone o jednorazowe użycie stosowanej przez bank tak zwanej dodatkowej metody uwierzytelnienia.

Wobec bardzo małej liczby użytkowników profilu zaufanego oferowanego na platformie e-PUAP oraz bezpiecznego podpisu elektronicznego większość wniosków internetowych do projektu „Rodzina 500 plus" złożono za pośrednictwem systemów bankowych. Internauci wybrali znane i ergonomiczne rozwiązania z komercyjnych serwisów transakcyjnych, dostępne dla nich bez dodatkowych formalności. Opracowane na potrzeby urzędów serwisy internetowe pod względem wygody korzystania zdecydowanie ustępują sprawdzonym i rozwiniętym systemom bankowym[3].

Interesującym projektem w zakresie jednolitego elektronicznego identyfikatora jest system OpenID, który pozwala na wykorzystanie istniejącego konta do logowania się na wielu stronach internetowych, bez konieczności tworzenia nowych haseł. OpenID to system uwierzytelniania, w którym wystarczy jedno konto OpenID, by móc logować się na wszystkich serwisach wspierających OpenID[4].

Wydaje się, że optymalnym rozwiązaniem problemu identyfikacji byłoby dostarczenie użytkownikom sieci teleinformatycznych nowego elektronicznego dowodu osobistego w roli narodowego identyfikatora, który posiadałby w warstwie elektronicznej mechanizm potwierdzający, iż dokument został wydany przez uprawniony podmiot i nie jest sklonowany. Brakuje jednak aktualnych i szczegółowych informacji o realizacji tego projektu[5].

1 *Identyfikacja i uwierzytelnienie w usługach elektronicznych. Przewodnik Forum Technologii Bankowych przy Związku Banków Polskich*, red. T. Mielnicki (i in.), Warszawa 2013, s. 12.

2 Ustawa z dnia 16 listopada 2000 r o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, DzU nr 116, poz. 1216; tekst jedn. DzU z 2003 r., nr 153, poz. 1505; tekst jedn. DzU z 2010 r., nr 46, poz. 276.

3 M. Tomaszkiewicz, *Banki będą logować do urzędów*, www.antyradio.pl/Technologia/Internet/Banki-beda-logowac-do-urzedow-9088 (dostęp 19.06.2016).

4 Zob. http://openid.net/ (dostęp 24.04.2016).

5 Ministerstwo Administracji i Cyfryzacji, *Program zintegrowanej informatyzacji państwa*, Warszawa 2013, s. 4.

1. Procesy identyfikacji i uwierzytelniania – podstawowe pojęcia

Standardowo wyróżnia się następujące metody uwierzytelnienia:
- proste uwierzytelnianie z wykorzystaniem hasła lub innego akceptowanego przez komunikujące się strony kodu (ang. What is known by the parties),
- silne uwierzytelnienie z wykorzystaniem elementów pozostających w dyspozycji nadawcy (ang. What the sender has) (sprzętowy token, np. karta elektroniczna),
- uwierzytelnianie z wykorzystaniem cech nadawcy (ang. What the sender is) (cechy biometryczne)[6].

Uwierzytelnienie jednoczynnikowe oparte jest na jednym elemencie: „co znasz" albo „co posiadasz", natomiast kombinacja tych obu elementów to „uwierzytelnienie wieloczynnikowe" (ang. *multifactor authentication*). Standardowe uwierzytelnianie jednoczynnikowe polega na tym, że w procesie logowania potrzebna jest tylko jedna tajna informacja powiązana z użytkownikiem. Przykładowo w procesie uwierzytelnienia dwuczynnikowego często wykorzystuje się jednorazowy kod wysyłany jako wiadomość SMS albo generowany przez zainstalowaną na smartfonie aplikację powiązaną z konkretną usługą lub U2F – token (Uniwersal 2nd Factor) jako ekwiwalent dodatkowego zaszyfrowanego hasła[7].

Każda standardowa procedura uwierzytelnienia obejmuje trzy podstawowe procesy:
- proces rejestracji, czyli pozyskania i weryfikacji atrybutów tożsamości fizycznej, konstytuujących tożsamość elektroniczną w sposób wiążący ją możliwie jednoznacznie i wiarygodnie z tożsamością fizyczną,
- proces zarządzania danymi uwierzytelniającymi, zawierający między innymi proces wydania danych uwierzytelniających (po raz pierwszy), odnowienia, unieważnienia, zawieszenia,
- proces uwierzytelnienia.

Realizacja każdego z wymienionych procesów nie ma charakteru w pełni deterministycznego, to znaczy w wyniku realizacji danego procesu uzyskuje się rezultat, który z zadanym prawdopodobieństwem (z pewnym poziomem wiarygodności) odzwierciedla faktyczny związek pomiędzy tożsamością fizyczną i elektroniczną. Łączny poziom wiarygodności procesu uwierzytelnienia zależy od wszystkich wymienionych procesów, rozwiązań technicznych i organizacyjnych, związanych z realizacją dowolnego. Wspomniane procesy w sposób najbardziej kompleksowy i uniwersalny opisuje norma ISO 29115[8]. Dla każdej usługi realizowanej w formie elektronicznej określono dopuszczalny poziom wiarygodności odpowiadający akceptowalnym stratom, które mogą być poniesione w przypadku błędnego uwierzytelnienia. Określając poziom wiarygodności uwierzytelnienia w konkretnym modelu, analizuje się wszystkie procesy tworzące kompletną procedurę – począwszy od akwizycji i zarządzania danymi uwierzytelniającymi, po właściwy proces uwierzytelnienia, a także czynniki organizacyjne (m.in. otoczenie prawne, infrastrukturę, bezpieczeństwo,

6 M. Marucha-Jaworska, *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Wolters Kluwer SA, Warszawa 2015, s. 30.

7 J. Korn, *Wreszcie bezpieczne konta online*, „CHIP" 2016, nr 5, s. 96–97.

8 ISO/IEC 29115, *Information Technology – Security Techniques – Entity Authentication Assurance Framework*, Reference number ISO/IEC 29115:2013(E).

w tym bezpieczeństwo informacji, systemów IT). Struktura wiarygodności uwierzytelnienia jest to zestaw wszystkich, technicznych i organizacyjnych czynników wpływających na całkowity poziom wiarygodności uwierzytelnienia. Końcowy wynik zawsze jest równy najniższemu poziomowi osiągniętemu przez któryś z czynników (zasada „najsłabszego ogniwa"). Norma ISO 29115[9] definiuje poziomy wiarygodności w następujący sposób:

LoA 1[10] – minimalna wiarygodność lub jej brak. Nie wymaga użycia kryptografii.

LoA 2 – ograniczona wiarygodność deklarowanej tożsamości. Nie wymaga użycia kryptografii. Na tym poziomie wystarcza uwierzytelnienie jednoczynnikowe, jednak powinien być zastosowany bezpieczny protokół uwierzytelnienia, redukujący wpływ podsłuchania i ataków polegających na zgadywaniu. Przechowywane dane uwierzytelniające muszą być chronione.

LoA 3 – wysoka wiarygodność deklarowanej tożsamości. Poziom ten wymaga uwierzytelnienia wieloczynnikowego oraz użycia kryptografii.

LoA 4 – bardzo wysoka wiarygodność deklarowanej tożsamości. Ten poziom jest zbliżony do LoA 3, ale dodatkowo wymaga fizycznej obecności przy rejestracji osoby oraz użycia odpornych na manipulacje tokenów sprzętowych (np. kart elektronicznych z mikroprocesorem) przechowujących sekrety lub kryptograficzne klucze prywatne. Protokół uwierzytelnienia musi chronić kryptograficznie wszelkie dane identyfikujące osobę i inne wrażliwe dane.

2. Procesy identyfikacji i uwierzytelniania w systemach teleinformatycznych administracji publicznej

W Unii Europejskiej prowadzona jest rozległa reforma ram prawnych i standaryzacyjnych kwestii dotyczących między innymi podpisu elektronicznego. Celem tych prac jest zniesienie istniejących barier w swobodnym przepływie usług oraz wprowadzenie jednolitego traktowania i uznawania usług zaufania na rynku międzynarodowym, zwłaszcza przez instytucje sektora publicznego.

Organy Unii Europejskiej wspierają rozwój takich projektów, jak IDABC[11], STORK[12], Netcards[13], które dotyczą wykorzystania jednej elektronicznej tożsamości w wielu obszarach czy współdzielenia wyniku uwierzytelnienia (tzw. *Single-Sign-On*)[14]. Oprócz standar-

9 *Ibidem*, s. 6–8.

10 Ang. *Level of Assurance* (LoA). – poziom wiarygodności.

11 IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens*) – program interoperatywnego świadczenia ogólnoeuropejskich usług eGovernment dla administracji publicznej, przedsiębiorstw i obywateli. IDABC wykorzystuje możliwości oferowane przez technologie informacyjne i komunikacyjne, aby wspierać międzynarodowe usługi sektora publicznego dla obywateli i przedsiębiorstw w całej zjednoczonej Europie.

12 Secure idenTity acrOss boRders linKed 2.0 – projekt, którego celem jest osiągnięcie interoperacyjności systemów elektronicznej tożsamości funkcjonujących lub mających zostać wdrożonych w krajach UE, www.eid-stork2.eu/index.php?option=com_content&view=article&id=398&Itemid=134 (dostęp 4.01.2016).

13 NetCards umożliwia weryfikację uprawnień obywateli Unii Europejskiej do świadczeń medycznych.

14 *Identyfikacja i uwierzytelnienie w usługach elektronicznych…*, s. 2–132.

du amerykańskiego NIST SP 800-53[15] istnieje także pierwsza norma międzynarodowa ISO 29115[16], umożliwiająca ponadnarodową standaryzację procedur uwierzytelnienia.

W opublikowanym w ostatnich miesiącach przez Ministerstwo Cyfryzacji dokumencie *Kierunki Działań Strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych* zauważono znaczenie przyjęcia jednolitego standardu cyfrowej identyfikacji obywateli oraz stworzenia możliwości bezpiecznego elektronicznego potwierdzania tożsamości w kontakcie z administracją. W celu realizacji tego zadania rozważana jest możliwość wykorzystania systemów i kanałów usługodawców komercyjnych do przyspieszenia upowszechnienia elektronicznej identyfikacji obywateli, a zarazem budowy bramy, także mobilnej, do różnych usług (bankowych, finansowych, administracji, służby zdrowia oraz innych usług użyteczności publicznej). W kontekście cyfrowej identyfikacji rozważa się powrót do koncepcji dowodu osobistego z warstwą elektroniczną posiadającego następujące funkcjonalności: identyfikacja, uwierzytelnianie, podpis elektroniczny, dokument podróżny zgodny z ICAO, ewentualnie ratunkowe dane medyczne czy biometrię[17]. Zdaniem Minister Anny Streżyńskiej dotychczasowy wysiłek i środki włożone w cyfryzację państwa zostały w dużym stopniu zmarnotrawione. Jako przykłady niefunkcjonujących, kluczowych i kosztownych programów wskazała program pl.ID, ePUAP[18].

Według aktualnego stanu prawnego elektroniczna identyfikacja w systemach teleinformatycznych administracji publicznej jest możliwa z wykorzystaniem bezpiecznego podpisu elektronicznego lub profilu zaufanego ePUAP, a w perspektywie także dowodu osobistego z warstwą elektroniczną zawierającego klucze kryptograficzne. Należy jednak podkreślić, że obecne uwarunkowania prawne ograniczają obszar stosowalności bezpiecznego podpisu elektronicznego do identyfikacji w procesach uwierzytelnienia dokumentów w formie elektronicznej.

3. Podpis elektroniczny

Ustawa o podpisie elektronicznym[19] definiuje podpis elektroniczny jako dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Natomiast bezpieczny podpis elektroniczny określa jako podpis elektroniczny, który:

– jest przyporządkowany wyłącznie do osoby składającej ten podpis,

15 *Security and Privacy Controls for Federal Information Systems and Organizations JOINT TASK FORCE TRANSFORMATION INITIATIVE*, National Institute of Standards and Technology 2013.

16 Zob. www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en (dostęp 20.12.2016.).

17 Ministerstwo Cyfryzacji, *Kierunki Działań Strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych*, https://mc.gov.pl/aktualnosci/kierunki-dzialan-strategicznych-ministra-cyfryzacji-w-obszarze-informatyzacji-uslug-0 (dostęp 1.04.2016).

18 A. Streżyńska, *Program Rodzina 500+ testem dla e-administracji*, Konferencja Perspektywy rozwoju Polski Cyfrowej na lata 2016–2020, Warszawa 2016, www.polskieradio.pl/42/273/Artykul/1584407,Strezynska-program-Rodzina-500-testem-dla-eadministracji (dostęp 1.04.2016).

19 Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, DzU z 2001 r., nr 130, poz. 1450 (powoływana dalej jako ustawa o podpisie elektronicznym).

- jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna[20].

Podpisem elektronicznym w rozumieniu ustawy o podpisie elektronicznym jest zatem każda elektroniczna forma identyfikacji osób fizycznych, w tym na przykład e-mail, która ujawniałaby dane personalne osoby nadawcy, dane personalne załączone do listu w poczcie elektronicznej, hasło jednorazowe wraz z innymi danymi przekazywanymi podczas logowania do serwera bankowego.

Proces składania bezpiecznego podpisu elektronicznego obejmuje procedurę wyznaczenia funkcji skrótu dokumentu oraz zaszyfrowanie obliczonej wartości tej funkcji z wykorzystaniem klucza prywatnego osoby składającej podpis.

Pierwszy etap to obliczenie skrótu podpisywanego dokumentu elektronicznego. Wygenerowanie z podpisywanego pliku tak zwanego 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. Zatem argumentem jednokierunkowej funkcji skrótu *H(M)* jest wiadomość *M* o dowolnej długości. Wartością tej funkcji jest liczba *h* o ustalonej długości $h = H(M)$. Jednokierunkowe funkcje skrótu mają następujące własności: dla danego *M* łatwo jest obliczyć *h*, dla danego *h* nie jest praktycznie możliwe obliczenie *M* (brak możliwości wygenerowania dwóch wiadomości o takim samym skrócie), dla danego *M* nie jest praktycznie możliwe znalezienie takiego *M'* różnego od *M*, że $H(M) = H(M')$ (brak możliwości wygenerowania dwóch wiadomości o takim samym skrócie[21]). Bezpieczna kryptograficznie funkcja skrótu powinna zapewniać brak możliwości odtworzenia danych wejściowych na podstawie skrótu. Uznanie funkcji 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[22]. W przypadku podpisu elektronicznego stosuje się funkcję skrótu SHA-2[23]. Zastosowanie funkcji skrótu zapewnia możliwość weryfikacji integralności podpisanego dokumentu. Jakakolwiek zmiana dokumentu powoduje bowiem istotną zmianę wartości funkcji skrótu[24].

Następnie obliczony skrót jest szyfrowany z wykorzystaniem asymetrycznego algorytmu kryptograficznego z użyciem klucza prywatnego, zapisanego na karcie kryptograficznej.

20 Zob. art. 3 ustawy o podpisie elektronicznym.

21 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Poznań 2001, s. 81.

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

23 SHA-1 (*Secure Hash Algorithm*) jest jednokierunkową funkcją skrótu zaprojektowaną przez National Security Agency (NSA) i opublikowaną przez National Institute of Standards and Technology (NIST). Wytwarza ona skrót o długości 160 bitów z wiadomości o dowolnym rozmiarze, nie większym niż 264 bitów.

24 R. Poznański, D. Wachnik, *Podpis elektroniczny – prawo i rzeczywistość* „Czas Informacji" 2011, nr 2 (7), s. 25.

Warunkiem wykonania tej operacji jest jej uwierzytelnienie kodem PIN. Najpopularniejszym asymetrycznym algorytmem kryptograficznym stosowanym do szyfrowania obliczonej wartości funkcji skrótu jest algorytm RSA. Został on zaprojektowany w 1977 roku przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jest to algorytm szyfrowania asymetrycznego, którego istotnymi elementami są dwa klucze: publiczny, jawny oraz prywatny, niejawny i chroniony. Bezpieczeństwo szyfrowania algorytmem RSA wynika z trudności faktoryzacji dużych liczb złożonych[25]. W ostatnich latach często pojawiają się informacje o próbach uzyskania klucza prywatnego na podstawie klucza publicznego w algorytmie RSA. Wydaje się jednak, że obecnie nie jest to w praktyce realne zagrożenie w odniesieniu do kluczy o długości co najmniej 2048 bitów[26].

Klucz publiczny umożliwia jedynie zaszyfrowanie danych i praktycznie uniemożliwia ich odczytanie, nie musi więc być chroniony. Drugi klucz – prywatny – przechowywany pod nadzorem, służy do odczytywania informacji zakodowanych za pomocą klucza publicznego. Możliwe jest także zaszyfrowanie wiadomości za pomocą tajnego klucza prywatnego, a następnie jej odszyfrowanie za pomocą klucza publicznego. To właśnie ta cecha sprawia, że RSA może zostać wykorzystany do cyfrowego podpisywania dokumentów[27].

Zaszyfrowana funkcja skrótu jest dołączana do oryginalnego dokumentu. Dodatkowo do dokumentu oraz zaszyfrowanego skrótu dołączany zostaje certyfikat zawierający dane osoby składającej podpis oraz jej klucz publiczny. Zgodnie z informacją publikowaną przez Narodowe Centrum Certyfikacji, które pełni funkcję głównego urzędu certyfikacji dla infrastruktury bezpiecznego podpisu elektronicznego, w Polsce pięć firm oferuje wydawanie certyfikatów kwalifikowanych i zestawów do składania bezpiecznego podpisu elektronicznego[28]. Infrastruktura Klucza Publicznego (PKI) to szeroko pojęty kryptosystem, w skład którego wchodzą urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów (użytkownicy), oprogramowanie i sprzęt. Infrastruktura klucza publicznego tworzy hierarchiczną strukturę zaufania, której podstawowym dokumentem jest certyfikat klucza publicznego[29].

W skład zestawu do składania bezpiecznego 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[30].

Weryfikacja dokumentu w formie elektronicznej uwierzytelnionego podpisem elektronicznym polega na porównaniu wartości funkcji skrótu obliczonej przez autora dokumentu z wartością funkcji skrótu wyznaczoną przez adresata dokumentu i ponownym obliczeniu

25 R. Anderson, *Inżynieria zabezpieczeń*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005, s. 122–123.

26 Cryptology ePrint Archive: Report 2016/086, Cryptology ePrint Archive: Report, 14.04.2016.

27 W. Nowakowski, *Algorytm RSA – podstawa podpisu elektronicznego*, „Elektronika" 2010, nr 6, s. 169.

28 Narodowe Centrum Certyfikacji, *Rejestr podmiotów kwalifikowanych świadczących usługi certyfikacyjne*, www.nccert.pl (dostęp 11.04.2016).

29 S. Dziembowski, *Infrastruktura klucza publicznego*, www.mimuw.edu.pl (dostęp 14.04.2016).

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

skrótu z dokumentu. Jeśli rozszyfrowany przy pomocy 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 odpowiedni organ – Zaufana Trzecia Strona (*Trusted Third Party*), której zadaniem jest wydawanie i zarządzanie certyfikatami, poświadczającymi autentyczność danego klucza publicznego. Certyfikat cyfrowy zawiera unikalny 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. Art. 21 ustawy o podpisie elektronicznym stanowi, że „certyfikat jest ważny w okresie w nim wskazanym". Po tym czasie staje się nieważny i podpisy złożone po upłynięciu terminu ważności są automatycznie weryfikowane negatywnie. Możliwe jest także unieważnienie lub zawieszenie certyfikatu. Fakt ten zostaje odnotowany i opublikowany na tak zwanej liście CRL[31]. Cyfrowy podpis pod dokumentem wraz z dołączonym certyfikatem oznacza, że właściciel certyfikatu złożył podpis i tym samym zna treść dokumentu.

Certyfikat kwalifikowany może być wydany jedynie osobie fizycznej. Do wydania certyfikatu kwalifikowanego niezbędne jest potwierdzenie tożsamości osoby ubiegającej się o bezpieczny podpis elektroniczny, co wymaga 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[32].

Czas złożenia podpisu elektronicznego w wielu zastosowaniach ma decydujące znaczenie. Ustawa o podpisie elektronicznym w art. 3 pkt 16 definiuje „znakowanie czasem" jako „usługę polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę". Zgodnie z art.7 ust. 3 ustawy o podpisie elektronicznym: „Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi". Bez oznaczania czasem nie można przeprowadzić długookresowej weryfikacji podpisu elektronicznego, co istotnie utrudnia archiwizację dokumentów w formie elektronicznej.

Dyrektywa 1999/93/WE posługuje się pojęciem *uwierzytelnienia*, natomiast polska ustawa o podpisie elektronicznym – *identyfikacji*[33]. Ta rozbieżność wynika z faktu, że doku-

31 Zgodnie z normą PN-I-02000:2002 jest to brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie. Właściwość ta dotyczy podmiotu podpisującego wiadomość za pomocą bezpiecznego podpisu weryfikowanego kwalifikowanym certyfikatem.

32 *Podpis elektroniczny*, www.podpiselektroniczny.czest.pl (dostęp 14.04.2016).

33 Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz. Urz. UE, 13/t. 24 PL, 239): „Artykuł 2. Definicje. Do celów niniejszej dyrektywy: 1. „podpis elektroniczny" oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia".

menty Europejskiego Komitetu Normalizacyjnego[34] określają cztery podstawowe funkcje podpisu elektronicznego, gdzie identyfikacja jest najszersza z możliwych:

– identyfikacja (ang. identification),
– uwierzytelnienie (ang. authentication),
– oświadczenie wiedzy (ang. declaration of knowledge),
– oświadczenie woli (ang. declaration of will).

Podpisy składane w celu **identyfikacji** (*signatures for identification*) służą wyłącznie do udowodnienia posiadania klucza prywatnego (*proof-of-possession of the private key*). Podpisy i certyfikaty służą w tym przypadku tylko do uwierzytelnienia w systemie i identyfikacji osoby starającej się o dostęp na przykład do serwera, bazy danych i tym podobnych. Identyfikacja opiera się na podpisaniu losowych danych przesłanych przez żądający identyfikacji serwer i weryfikacji tak złożonego podpisu cyfrowego. W przypadku poprawności żądający uwierzytelnienia ma pewność, że zweryfikował osobę, która posiada dany klucz prywatny. Unikalność klucza oraz jego poufność pozwalają przyjąć, że zweryfikowana jest uprawniona osoba. Taka metoda uwierzytelnienia może zostać uznana za wystarczającą do celów identyfikacji, ale nie do celów oświadczenia woli. Decyzja 511 Komisji Europejskiej z 14 lipca 2003 roku rekomenduje niełączenie certyfikatów wskazujących na podpisy elektroniczne jako oświadczenie woli z jakimikolwiek innymi zastosowaniami, na przykład „identyfikacją"[35].

Podpisy składane w celu **uwierzytelnienia** (*signatures for authentication*) są składane całkowicie automatycznie bez świadomości i ingerencji osoby składającej i nie służą do składania oświadczeń woli.

Podpisy składane jako **oświadczenie wiedzy** (*signatures for declaration of knowledge*) nie służą do składania oświadczeń woli. Podpis ten służy na przykład do potwierdzenia zapoznania się z dokumentem czy odebrania dokumentu, nie stanowi jednak dowodu, że został on zatwierdzony, czyli że zawiera treść zaakceptowaną przez podpisującego.

Podpisy składane pod oświadczeniem woli (*signatures as declaration of will*) stanowią dowód złożenia oświadczenia woli. Powinny być składane po zaznajomieniu się z treścią podpisywanego dokumentu oraz zgodne z intencją jego podpisania, a także pod pełną kontrolą podpisującego. Podpisy te są składane między innymi w oparciu o certyfikat, który w polu *keyUsage* zawiera tylko bit *contentCommitment*.

Każdy rodzaj podpisu elektronicznego może zatem stanowić dowód, ale tylko nieliczne mogą potwierdzać oświadczenie woli. Tak więc podpis w celu identyfikacji może stanowić dowód uzyskania dostępu do danej bazy danych przez konkretną osobę dysponującą kluczem prywatnym w określonym czasie. Podpis celem uwierzytelnienia stanowi dowód zapoznania się z treścią dokumentu.

34 Pkt. 4.2.2 *Guide on the Use of Electronic Signatures*, CEN WORKSHOP AGREEMENT, CWA 14365-1, ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14365-01-2004-Mar.pdf (dostęp 14.04.2016).

35 Decyzja Komisji z dnia 14 lipca 2003 r. w sprawie publikacji numerów referencyjnych dla powszechnie uznanych norm dotyczących produktów podpisu elektronicznego zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE (Dz. Urz. UE L 163/19).

4. Rodzaje podpisu elektronicznego według projektu rozporządzenia eIDAS

W ostatnich latach w Unii Europejskiej prowadzona jest rozległa reforma ram prawnych i standaryzacyjnych kwestii dotyczących między innymi podpisu elektronicznego. Celem tych prac jest zniesienie istniejących ograniczeń w swobodnym przepływie usług oraz wprowadzenie jednolitego traktowania i uznawania usług zaufania na rynku międzynarodowym, zwłaszcza przez instytucje sektora publicznego. W 2014 roku ukazało się rozporządzenie Parlamentu Europejskiego Rady Unii Europejskiej w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym[36] powoływane dalej jako rozporządzenie eIDAS (ang. *electronic identification and trust services*)[37]. Założeniem rozporządzenia eIDAS jest zapewnienie wspólnej podstawy interakcji elektronicznej pomiędzy przedsiębiorstwami, obywatelami i organami publicznymi w celu ułatwienia korzystania z usług internetowych o charakterze transgranicznym. Istotne jest także zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania. Rozporządzenie eIDAS definiuje usługi identyfikacji uczestników komunikacji elektronicznej obowiązujące na terenie całej UE oraz wprowadza usługi zaufania stanowiące mechanizm zabezpieczenia różnego rodzaju transakcji elektronicznych.

W celu zapewnienia realizacji założeń rozporządzenia eIDAS określono warunki uznawania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego oraz ustanowiono ramy prawne dla:

- podpisów elektronicznych,
- pieczęci elektronicznych,
- elektronicznych znaczników czasu,
- dokumentów elektronicznych,
- usług potwierdzonych doręczeń elektronicznych,
- usług certyfikacyjnych do celu uwierzytelniania witryn internetowych.

W zakresie środków identyfikacji elektronicznej rozporządzenie eIDAS określa 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. Rozporządzenie eIDAS poprzez rozdział elektronicznej identyfikacji oraz usług zaufania określa kompetencje i odpowiedzialności w zakresie budowania tych usług:

1. Usługi elektronicznej identyfikacji mają być oparte o scentralizowany system będący tylko i wyłącznie pod kontrolą rządu, a każdy kraj członkowski powinien określić, które z tych usług są przez niego gwarantowane.

36 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, 28.8.2014).

37 P. Chaber, *Rozporządzenie eIDAS wprowadza nowy rozdział w budowaniu e-usług* www.pi.gov.pl/PARP/chapter_86197.asp?soid=D1547EEB6C0A40B8804E897CFDED2A7E (dostęp 13.03.2016).

2. Usługi zaufania – skierowane przede wszystkim do podmiotów komercyjnych, świadczących je za opłatą, gdzie o ich jakości będzie świadczył nadzór i kontrola odpowiednich organów, ale zakres i modele biznesowe świadczenia tych usług będą podlegały prawom rynku.

Definicja podpisu elektronicznego zawarta w dyrektywie 93/99/EC i sformułowana w polskiej ustawie o podpisie elektronicznym nie uwzględnia wszystkich funkcji podpisu elektronicznego zawartych w dokumencie CWA 14365[38]. Autorzy publikacji *Identyfikacja i uwierzytelnienie w usługach elektronicznych* definiują podpis elektroniczny jako „dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny, uwierzytelnienia tej osoby lub składania przez nią różnego rodzaju oświadczeń"[39]. Zaproponowana definicja znacznie rozszerza obszary stosowalności podpisu elektronicznego, ponieważ uwzględnia możliwość wykorzystania podpisu elektronicznego w procesach identyfikacji, uwierzytelnienia, oświadczenia wiedzy i oświadczenia woli.

Nowe rozporządzenie eIDAS oparte jest na całkowicie nowym podejściu do kwestii funkcji podpisów elektronicznych w rozumieniu dyrektywy 93/99/EC. W projekcie eIDAS funkcję „identyfikacji" przypisano do osobnej kategorii, a pozostałe rodzaje podpisów elektronicznych podzielono na „podpis elektroniczny", który jest zawsze składany przez osobę fizyczną i „pieczęć elektroniczną", która jest składana przez osobę prawną („automatycznie" przez sprzęt i/lub oprogramowanie):

– identyfikacja elektroniczna – oznacza proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną,
– uwierzytelnianie – oznacza proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych,
– podpis elektroniczny – oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu,
– pieczęć elektroniczna – oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane, aby zagwarantować pochodzenie i integralność powiązanych danych.

Unormowania zawarte w art. 27 rozporządzenia eIDAS dotyczące stosowania podpisów elektronicznych w usługach publicznych zobowiązują państwa do wprowadzenia możliwości weryfikacji podpisów zaawansowanych z innych państw. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie (wydanym w jednym państwie członkowskim) jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach (art. 25 ust. 3).

38 CEN Workshop Agreement CWA 14365-1, *Guide on the Use of Electronic Signatures – Part 1: Legal and Technical Aspects, European Committee for Standardization Comité Européen de Normalisation Europäisches Komitee für Normung, Management Centre: rue de Stassart, 36 B-1050 Brussels*, March 2004.

39 *Identyfikacja i uwierzytelnienie w usługach elektronicznych…*, s. 30.

Planuje się stosowanie przepisów *Rozporządzenia eIDAS* w wewnętrznym porządku prawnym państw członkowskich od 1 lipca 2016 roku. Do 13 stycznia 2018 roku państwa UE wprowadzą w prawie krajowym dyrektywę w sprawie usług płatniczych[40], która wymaga zastosowania elektronicznej identyfikacji oraz tworzy usługi zaufanej trzeciej strony. Druga połowa 2018 roku to termin wejścia w życie obowiązkowego respektowania mechanizmu notyfikacji eID przez wszystkie państwa członkowskie. Kwestie identyfikacji elektronicznej i usług zaufania były dotychczas uregulowane w ustawie o podpisie elektronicznym. Ustawę, która pozwoli dostosować polski porządek prawny do rozporządzenia eIDAS, przygotowują resorty rozwoju i cyfryzacji.

Podsumowanie

Uwzględniając, że profil zaufany nie jest narzędziem dedykowanym do uwierzytelnienia e-usług, jedyną funkcjonującą w Polsce uniwersalną metodą uwierzytelnienia, która mogłaby być powszechnie stosowana w obecnych i przyszłych systemach teleinformatycznych, jest kwalifikowany podpis elektroniczny wykorzystujący asymetryczne algorytmy kryptograficzne. Należy podkreślić, że w pełni realizuje wymagania najwyższego poziomu wiarygodności LoA 4.

Aktualne uwarunkowania prawne ograniczają obszar jej stosowalności do uwierzytelnienia dokumentów w formie elektronicznej. Ze względu na swoją moc prawną (równoważną podpisowi odręcznemu) oraz obowiązek prezentacji podpisywanych danych podpisującemu, nie powinno się go stosować do uwierzytelnienia, gdzie następuje podpisanie nieznanego dla podpisującego ciągu danych. Zatem nie powinien być stosowany do uwierzytelnienia *on-line* do usług elektronicznych, gdyż jest to narzędzie do składania wyłącznie oświadczeń woli (pole *key usage* określone jako *non repudiation/content commitment* – niezaprzeczalność). Ponadto podpis kwalifikowany nadal nie jest powszechnie stosowanym narzędziem[41]. Oczywiście możliwe jest wykorzystanie certyfikatów niekwalifikowanych, ale liczba użytkowników certyfikatów jest znikoma.

Należy jednak zauważyć scharakteryzowane wcześniej zalety wykorzystywania asymetrycznych algorytmów kryptograficznych w procesach identyfikacji i uwierzytelniania w tym stosunkowo proste wsparcie dla mechanizmów niezaprzeczalności. Trzeba także brać pod uwagę zagrożenia wiążące się z tą technologią. Jednym z istotniejszych wśród nich jest aspekt poufności klucza prywatnego. Jego pozyskanie przez atakującego ma katastrofalne skutki – podpisy składane przez napastnika z wykorzystaniem skompromitowanego klucza prywatnego będą bowiem nierozróżnialne pod względem technicznym i prawnym od podpisów elektronicznych legalnego właściciela. Jeśli ma on świadomość kompromitacji swojego klucza prywatnego, powinien niezwłocznie unieważnić swój certyfikat, jednak do

40 Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz. Urz. UE, L 319/1, 5.12.2007).

41 Zgodnie z danymi dostępnymi na stronie Ministerstwa Gospodarki liczba aktywnych certyfikatów kwalifikowanych w lutym 2015 r. wynosiła 318182 (dostęp 1.01.2016).

tego czasu napastnik może składać w jego imieniu oświadczenia woli. Bardziej bezpieczne rozwiązanie podpisów elektronicznych opartych o asymetryczne algorytmy kryptograficzne polega na przechowywaniu klucza prywatnego w specjalnym tokenie sprzętowym. Wykonywanie operacji matematycznych odbywa się również w tokenie, stąd klucz prywatny do podpisów nie jest eksportowany do aplikacji. Należy podkreślić, iż zastosowanie kryptografii asymetrycznej i PKI wraz z tokenem sprzętowym pozwala na osiągnięcie najwyższego poziomu wiarygodności uwierzytelnienia.

Wydaje się, że po korekcie uwarunkowań prawnych w sposób umożliwiający wykorzystywanie certyfikatów kwalifikowanych w procesach uwierzytelnienia podpis elektroniczny mógłby odgrywać w Polsce rolę powszechnego narzędzia identyfikacji i uwierzytelniania uczestników transakcji elektronicznych.

Bibliografia

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

CEN Workshop Agreement CWA 14365-1, *Guide on the Use of Electronic Signatures – Part 1: Legal and Technical Aspects, European Committee for Standardization Comité Européen de Normalisation Europäisches Komitee für Normung, Management Centre: rue de Stassart, 36 B-1050 Brussels*, March 2004.

Chaber P., *Rozporządzenie eIDAS wprowadza nowy rozdział w budowaniu e-usług*, www.pi.gov.pl/PARP/chapter_86197.asp?soid=D1547EEB6C0A40B8804E897CFDED2A7E (dostęp 13.03.2016).

Cryptology ePrint Archive: Report 2016/086, Cryptology ePrint Archive: Report, 14.04.2016.

Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz. Urz. UE, L 319/1, 5.12.2007).

Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz. Urz. UE, 13/t. 24 PL, 239).

Dziembowski S., *Infrastruktura klucza publicznego*, www.mimuw.edu.pl (dostęp 14.04.2016).

Guide on the Use of Electronic Signatures, CEN Workshop Agreement, CWA 14365-1, ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14365-01-2004-Mar.pdf (dostęp 20.12.2016).

Identyfikacja i uwierzytelnienie w usługach elektronicznych. Przewodnik Forum Technologii Bankowych przy Związku Banków Polskich, red. T. Mielnicki (i in.), Warszawa 2013.

Korn J., *Wreszcie bezpieczne konta online*, „CHIP" 2016, nr 5, s. 96–97.

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

Ministerstwo Administracji i Cyfryzacji, *Program zintegrowanej informatyzacji państwa*, Warszawa 2013.

Ministerstwo Cyfryzacji, Kierunki Działań Strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych, https://mc.gov.pl/aktualnosci/kierunki-dzialan-strategicznych-ministra-cyfryzacji-w-obszarze-informatyzacji-uslug-0 (dostęp 1.04.2016).

Narodowe Centrum Certyfikacji, *Podpis elektroniczny i usługi zaufania – nowe przepisy wejdą w życie 1 lipca 2016 r.*, www.nccert.pl/komunikaty2016.htm#k2016 (dostęp 24.04.2016).

Narodowe Centrum Certyfikacji, *Rejestr podmiotów kwalifikowanych świadczących usługi certyfikacyjne*, www.nccert.pl (dostęp 20.12.2016).

Norma ISO/IEC 29115, *Information Technology — Security Techniques — Entity Authentication Assurance Framework*, Reference number ISO/IEC 29115:2013(E).

Nowakowski W., *Algorytm RSA – podstawa podpisu elektronicznego*, „Elektronika" 2010, nr 6, s. 169–170.

Nowakowski W., Poznański R., *Podpis elektroniczny – zasady działania*, „Elektronika" 2010, nr 7, s. 265–267.

Podpis elektroniczny, www.podpiselektroniczny.czest.pl (dostęp 14.04.2016).

Poznański R., Wachnik D., *Podpis elektroniczny – prawo i rzeczywistość*, „Czas Informacji" 2011, nr 2 (7), s. 48–54.

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, 28.8.2014).

Secure idenTity acrOss boRders linKed 2.0 STORK, www.eid-stork2.eu/index.php?option=com_content&view=article&id=398&Itemid=134 (dostęp 4.01.2016).

Security and Privacy Controls for Federal Information Systems and Organizations Joint Task Force Transformation Initiative, National Institute of Standards and Technology 2013, www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en (dostęp 20.12.2016).

Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Poznań 2001.

Streżyńska A., *Program Rodzina 500+ testem dla e-administracji*, Konferencja Perspektywy rozwoju Polski Cyfrowej na lata 2016–2020, Warszawa 2016, www.polskieradio.pl/42/273/Artykul/1584407,Strezynska-program-Rodzina-500-testem-dla-eadministracji (dostęp 1.04.2016).

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU nr 116, poz. 1216; tekst jedn. DzU z 2003 r., nr 153, poz. 1505; tekst jedn. z DzU z 2010 r., nr 46, poz. 276).

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

ELECTRONIC SIGNATURE, IDENTIFICATION AND AUTHENTICATION

SUMMARY

An important stage of each transaction carried out in an environment of IT systems is to identify the parties and their authentication. The article analyzed the possibility of using a qualified electronic signature as a general tool for identification and authentication.

KEYWORDS

electronic signature, identification, authentication, public administration

Translated by Karol Sroka