Rejent * rok 18 * nr 9(209)
wrzesień 2008 r.

Przemysław P. Polański

Podpisy elektroniczne w prawie polskim i wspólnotowym

1. Wstęp

Podpis elektroniczny, rozumiany jako podpis oparty o infrastrukturę klucza publicznego (podpis cyfrowy), miał stać się fundamentem rozwoju handlu elektronicznego. Widać to wyraźnie zarówno w samej dyrektywie o podpisie elektronicznym[1], jak i wypowiedziach doktryny prawa[2]. Jednakże podpis cyfrowy nie upowszechnił się jeszcze w obrocie maso-

---

[1] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, OJ L 13/12, 19.01.2000, recital 4 (dalej: dyrektywa o podpisie elektronicznym lub d.p.e.). Dyrektywa ta została wdrożona do polskiego porządku prawnego ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450 ze zm.) – dalej: ustawa o podpisie elektronicznym lub u.p.e. oraz wydanym na jej podstawie Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. Nr 128, poz. 1094) – dalej: rozporządzenie o warunkach technicznych lub r.w.t.). Ponadto wydano szereg uzupełniających rozporządzeń do ustawy, które pozostaną poza zakresem naszego zainteresowania.

[2] Por. np. M. D r o z d o w i c z, *(Nie)bezpieczny podpis elektroniczny*, PPH 2003, nr 1, s. 27; K. K o w a l i k - B a ń c z y k, *Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym*, Wolters Kluwer 2006, s. 143 i cytowana tam literatura.

wym[3]. Obrót prywatnoprawny nadal zdominowany jest przez kontrakty w formie papierowej. Natomiast obrót elektroniczny wytworzył alternatywne metody identyfikacji osoby składającej oświadczenie woli. Wymienić wystarczy choćby obowiązek rejestracji za pomocą nazwy użytkownika i hasła, który stanowi rodzaj podpisu elektronicznego, bowiem identyfikuje konkretnego użytkownika składającego oświadczenie woli. Jest wiele przyczyn tego zjawiska, począwszy od wysokiej ceny i małej dostępności technologii poprzez brak jednolitych standardów technologicznych po nieprzystosowanie urzędów do korzystania z podpisu cyfrowego.

Sytuacja ta jednak może niedługo ulec zmianie. Zasadniczym jej powodem może stać się duża aktywność ustawodawcy, który stworzył szereg regulacji w znaczący sposób zwiększających atrakcyjność korzystania z podpisu cyfrowego. Wśród najważniejszych obszarów wskazać należy na przesyłanie i doręczanie pism w relacji petent – administracja, podatki, zamówienia publiczne czy kontakty z Zakładem Ubezpieczeń Społecznych. Być może więc podpis cyfrowy upowszechni się przynajmniej w relacjach publicznoprawnych.

Celem tego artykułu jest analiza różnych rodzajów podpisu elektronicznego. Wokół tej problematyki narosło wiele nieporozumień, głównie za sprawą koncentrowania się na tzw. podpisie cyfrowym. W pierwszej części przedstawiono wieloznaczność pojęcia podpisu elektronicznego, a następnie poddano analizie konstrukcję podpisu elektronicznego wynikającą z dyrektywy o podpisie elektronicznym i jej wdrożenie do prawa polskiego.

2. Rodzaje podpisów elektronicznych

Podpis elektroniczny to pojęcie bardzo pojemne, obejmujące swoim zakresem wiele różnych technologii. Świadomy tego faktu był także prawodawca europejski, który w samym tytule dyrektywy 1999/93/WE mówi o wspólnotowych ramach prawnych dla podpisów elektronicz-

[3] Por. np. M. K u t y ł o w s k i, *Bezdroża koncepcji prawnych podpisu elektronicznego*, Prawo Teleinformatyczne 2007, nr 2, s. 4-8; D. S z o s t e k, M. Ś w i e r c z y ń s k i, *Prawne możliwości poszerzenia rynku podpisu elektronicznego w Polsce,* [w:] *Prawo umów elektronicznych*, red. J. Gołaczyński, Kraków 2006, s. 173-177. Zob. także zapis debaty o stanie rozwoju podpisu elektronicznego w Polsce w artykule *Jaka nowelizacja ustawy o e-podpisie jest Polsce potrzebna?* Prawo Teleinformatyczne 2007, nr 2, s. 9-18.

nych, a nie o jednym podpisie elektronicznym, jak polska ustawa. W praktyce obrotu można się spotkać z następującymi typami podpisu elektronicznego: podpis kryptograficzny (zwany cyfrowym), podpis mobilny, podpis biometryczny, własnoręczny podpis biometryczny, podpis skanowany, podpis hasłowy oraz podpis klawiaturowy[4]. Podkreślić należy, że wymienione poniżej typy podpisu opierają się najczęściej na wykorzystaniu danych osobowych w połączeniu lub logicznym powiązaniu ze składanym oświadczeniem woli. Co za tym idzie, sam numer identyfikacyjny czy klucz prywatny nie stanowi podpisu – musi bowiem dojść do jego połączenia z dokonywaną czynnością.

2.1. Podpis cyfrowy (kryptograficzny)

Podpis cyfrowy (kryptograficzny, asymetryczny) stanowi główny przedmiot dyskusji oraz podstawowy model dla tworzenia regulacji prawnych wykorzystujących tę technologię. Jej teoretyczne podstawy stworzyło dwóch naukowców ze Stanford University – W. Diffie i M. Hellman w 1976 r.[5], a najpowszechniej wykorzystywaną implementację R. Rivest, A. Shamir i R. Adelman, twórcy algorytmu RSA z 1977 r. Istotą podpisu asymetrycznego jest wykorzystywanie dwóch powiązanych ze sobą kluczy (prywatnego i publicznego), z których ten służący do podpisywania jest znany tylko podpisującemu (stąd nazwa klucz prywatny), a ten służący do weryfikacji dostępny jest dla każdego chcącego sprawdzić autentyczność podpisu (nazywany kluczem publicznym). Klucz publiczny zapisywany jest w cyfrowym certyfikacie, wystawianym albo przez prywatne podmioty, albo przez specjalne organy certyfikacyjne. Natomiast klucz prywatny zapisywany jest na specjalnej karcie mikroprocesorowej (i uaktywniany za pomocą hasła), dysku twardym lub innym informatycznym nośniku danych.

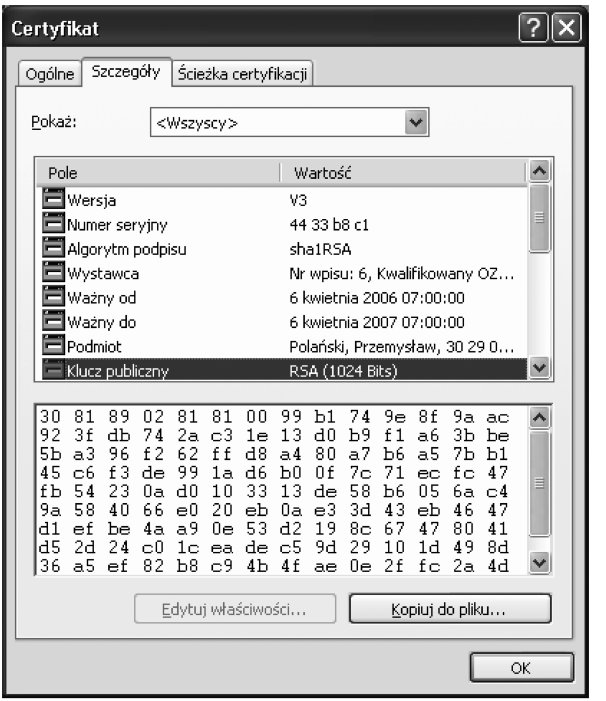
Jak założyli sami twórcy, podpis oparty o asymetryczne szyfrowanie nie jest bezwarunkowo bezpieczny (ang. *unconditionally secure*), lecz

---

[4] J. Janowski podaje następujące rodzaje podpisu elektronicznego: podpis kryptograficzny, podpis biometryczny, podpis skanowany, podpis klawiaturowy, podpis manualny, podpis PIN-owy, podpis hasłowy oraz podpis e-mailowy; zob. J. J a n o w s k i, *Podpis elektroniczny w obrocie elektronicznym*, Wolters Kluwer 2007, s. 39.

[5] W. D i f f i e, M.E. H e l l m a n, *New Directions in Cryptography*, „IEEE Transactions on Information Theory" November 1976, Nr IT-22(6).

obliczeniowo bezpieczny (ang. *computationally secure*)[6]. Przykładowo, bezpieczeństwo systemu opartego na algorytmie RSA opiera się na braku możliwości wyprowadzenia klucza prywatnego z klucza publicznego ze względu na ograniczenia mocy obliczeniowej komputerów, które nie są w stanie dokonać rozkładu bardzo dużych liczb pierwszych (a więc takich, które dzielą się tylko przez siebie i 1)[7]. Ponieważ moc komputerów się zmienia, konieczne staje się też wydłużanie długości klucza prywatnego i publicznego, by w istniejących warunkach nie można było wyliczyć klucza prywatnego, badając wszystkie możliwe kombinacje liczb.



[6] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, invited paper, 3 czerwca 1976 r., s. 31.

[7] Od strony matematycznej najbardziej przystępnie przedstawia to zagadnienie C.C. Clawson, *Mathematical Mysteries: The Beauty and Magic of Numbers*, Plenum Pr; Reissue edition 1996.

Ze względów ekonomicznych nie podpisuje się całego komunikatu kluczem prywatnym, a jedynie jego matematyczny obraz, zwany skrótem albo sumą kontrolną (ang. *hash*, *message digest*). Funkcja skrótu generowana jest przez algorytmy takie jak SHA-1 czy wcześniejszy MD5, umożliwia wytworzenie sumy kontrolnej z podpisywanego tekstu, która jest równej długości dla dokumentu o dowolnej obszerności[8]. Algorytm skrótu z jednej strony musi zapewniać brak możliwości odtworzenia treści komunikatu, bazując jedynie na wartości sumy kontrolnej, a z drugiej winien zminimalizować możliwość wytworzenia dwóch różnych komunikatów o takiej samej sumie kontrolnej (bowiem wówczas nie byłoby wiadomo, który komunikat został podpisany). Co więcej, algorytmy skrótu muszą dać zupełnie różne rezultaty, nawet przy zmianie, dodaniu czy usunięciu zaledwie jednej litery. W efekcie osoba weryfikująca podpis cyfrowy sprawdza nie tylko, czy dana wiadomość została wysłana przez osobę posługującą się kluczem prywatnym, ale także, czy wiadomość ta została zmieniona w trakcie przesyłania. Najdrobniejsza bowiem zmiana podpisanego komunikatu spowoduje zmianę odpowiadającej mu sumy kontrolnej, przez co podpisany skrót z przesyłanej wiadomości oraz kontrolnie wyliczony skrót z otrzymanego komunikatu nie będą się zgadzać.

Jednakże omawiana technologia ma potencjalne słabości. Nie gwarantuje ona bezwzględnego bezpieczeństwa, m.in. ze względu na różne algorytmy implementujące ideę asymetrycznej kryptografii. Niektóre algorytmy, tak jak przedstawiony powyżej algorytm RSA, są relatywnie bezpieczne, ale szereg innych zostało obalonych jako mało odporne na ataki kryptonalityków. Przykładem uznanego za mało bezpieczny jest algorytm Merkle-Hellman[9].

Słabym punktem tej technologii jest także możliwość wygenerowania klucza prywatnego i publicznego przez osoby prywatne, a więc poza

---

[8] Rozporządzenie o warunkach technicznych i organizacyjnych z 2002 r. definiuje funkcję skrótu jako „funkcję odwzorowującą ciągi bitów na ciągi bitów o stałej długości, w której dla danej wartości funkcji jest obliczeniowo trudne wyznaczenie argumentu odwzorowywanego na tę wartość, a dla danego argumentu jest obliczeniowo trudne wyznaczenie drugiego argumentu odwzorowywanego na tę samą wartość;" (§ 2 pkt 3).

[9] Wikipedia, http://en.wikipedia.org/wiki/Public-key_cryptography#_note-3, ostatni dostęp: 25 lipca 2007 r.; zob. także B. S c h n e i e r, *Applied cryptography: protocols, algorithms, and source code in C*, New York, Wiley 1996.

systemem gwarantującym minimalny poziom bezpieczeństwa obrotu. Dla przykładu, dostępne programy komputerowe umożliwiają autogenerację ceryfikatów. Szereg korporacji wystawia swoim pracownikom własne certyfikaty klucza publicznego. Również publicznie dostępne oprogramowanie, takie jak PGP (ang. *Pretty Good Privacy*), umożliwia generację par kluczy i ich wykorzystywanie do cyfrowego podpisywania. Stąd też wymyślono wiele schematów umożliwiających przypisanie podpisującemu klucza publicznego przez odpowiednie organizacje (podmioty świadczące usługi certyfikacyjne), które najpierw weryfikowałyby jego tożsamość. Dopiero po przejściu takiej weryfikacji osoba ta otrzymywałaby zestaw kluczy asymetrycznych (z reguły zakodowanych na specjalnej karcie mikroprocesorowej – ang. *smartcard*).

Najpowszechniej dyskutowanym systemem umożliwiającym wiarygodnie przypisanie par kluczy do konkretnej osoby jest Infrastruktura Klucza Publicznego (ang. *Public Key Infrastructure* albo PKI). System PKI opiera się na łańcuchu podmiotów świadczących usługi certyfikacyjne, z których każdy uwierzytelniany jest przez podmiot znajdujący się wyżej w hierarchii, aż do podmiotu naczelnego, który sam się uwierzytelnia. Jednakże i ten system zarządzania certyfikatami ma swoje słabości, które związane są z infrastrukturą umożliwiającą weryfikację certyfikatu klucza publicznego. Widać to w szczególności w sytuacji, w której na skutek błędu lub celowego działania dojdzie lub nie dojdzie do zawieszenia lub unieważnienia certyfikatu.

W praktyce infrastruktura klucza publicznego wykorzystywana jest nie tylko do cyfrowego podpisywania dokumentów, ale także do szyfrowania transakcji. Bowiem ta sama para kluczy w odwrotnej konfiguracji może służyć do ukrycia treści komunikatu przed podsłuchującymi. Innymi słowy, jeśli wysyłający komunikat użyje klucza publicznego odbiorcy do zaszyfrowania wiadomości, wówczas tylko adresat będzie mógł ten komunikat odszyfrować. W modelowej sytuacji, aby zapewnić z jednej strony identyfikację i integralność, a z drugiej poufność przesyłanego komunikatu, można połączyć oba rozwiązania. Najpierw więc wysyłający podpisze swoim kluczem prywatnym skrót komunikatu, a następnie zaszyfruje komunikat i skrót kluczem publicznym odbiorcy. Odbiorca wówczas najpierw odszyfruje wiadomość i skrót swoim kluczem prywatnym, a następnie dokona własnego obliczenia skrótu wiadomości

i weryfikacji tożsamości wysyłającego. Jednakże ze względu na stosunkową czasochłonność korzystania z szyfrowania asymetrycznego stosuje się rozwiązania pośrednie. Zatem *de facto* standard zabezpieczeń transakcji w handlu elektronicznym znany pod nazwą protokołu SSL 3.0 (ang. *Secure Sockets Layer*) wymusza stosowanie cyfrowych certyfikatów przez serwery stron www. Dzięki temu serwery stron internetowych mogą otrzymać od przeglądarki klienta zaszyfrowany publicznym kluczem serwera klucz sesyjny, który będzie wykorzystywany do zaszyfrowania transakcji[10].

Podsumowując, podpis cyfrowy obejmuje w istocie szereg różnych technologii. Po pierwsze, różne podpisy kryptograficzne mogą wykorzystywać różne algorytmy szyfrujące oraz algorytmy skrótu. Po drugie, podpis cyfrowy może (ale nie musi) wykorzystywać instytucję podmiotów świadczących usługi certyfikacyjne. Po trzecie, do korzystania z tej technologii nie jest konieczne wykorzystywanie kart mikroprocesorowych do zapisywania tam klucza prywatnego – można bowiem klucz ten przechowywać w „bezpiecznym" katalogu na dysku twardym, na karcie SIM telefonu czy karcie RFID. Po czwarte, w różny sposób mogą być weryfikowane powiązania pomiędzy kluczem prywatnym i publicznym podpisującego. W rezultacie podpis cyfrowy oferuje różne poziomy identyfikacji użytkownika oraz integralności komunikacji. Bez względu jednak na siłę wykorzystywanych algorytmów oraz technologię przechowywania kluczy, w ostatecznym rozrachunku najwięcej zależy od tego, jak zabezpieczony jest klucz prywatny, czyli np. od stopnia skomplikowania hasła, które służy do jego uruchomienia oraz od dostępności metod weryfikacji podpisu w czasie rzeczywistym.

---

[10] Szerzej na ten temat, B. C a n v e l, *Password Interception in a SSL/TLS Channel,* 2003, dostępny pod: http://lasecwww.epfl.ch/memo_ssl.shtml, ostatni dostęp: 22 kwietnia 2003 r.; A.O. F r e i e r, P. K a r l t o n, P.C. K o c h e r, *The SSL Protocol version 3.0. Internet Draft,* 1996, dostępny pod: http://home.netscape.com/eng/ssl3/ssl-toc.html, ostatni dostęp: 17 czerwca 2006 r.; A.K. G h o s h, *E-commerce security. Weak Links, Best Defences*, New York, John Wiley & Sons, Inc. 1998 Zob. także Wikipedia, http://en.wikipedia.org/wiki/Secure_Socket_Layer, ostatni dostęp: 25 lipca 2007 r. O jednym z przykładów udanych ataków na ten system pisze: Z. G o ł ę b i e w s k i, M. K u t y ł o w s k i, F. Z a g ó r s k i, *Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks,* The 5th International Conference on Cryptology and Network Security (CANS) 2006, LNCS 4301, (Springer Verlag 2006), s. 191-202.

Na zakończenie należy dodać, że termin „podpis cyfrowy" nie wydaje się najwłaściwszy, ponieważ sugeruje, że inne podpisy składane za pomocą komputera nie są cyfrowe – co jest oczywistym błędem. Każdy bowiem komunikat generowany przez komputer lub za jego pomocą jest komunikatem cyfrowym, a więc reprezentowalnym w kodzie binarnym (zero-jedynkowym). Lepiej więc używać terminu podpis kryptograficzny albo asymetryczny, ponieważ idea podpisu cyfrowego opiera się o kryptografię asymetryczną, która w odróżnieniu od szyfrowania symetrycznego posługuje się dwoma powiązanymi ze sobą kluczami, a nie jednym. Jednakże ze względu na powszechne posługiwanie się terminem podpis cyfrowy (ang. *digital signature*), w niniejszym artykule również będziemy się nim posługiwać na oznaczenie podpisu złożonego z wykorzystaniem technologii szyfrowania asymetrycznego.

2.2. Podpis mobilny

Podpis mobilny to szczególna postać podpisu cyfrowego. Podstawowa różnica polega na tym, że jest on składany przy pomocy telefonu komórkowego, a nie specjalnego czytnika kart i komputera[11] oraz że kartę mikroprocesorową zastępuje karta SIM (ang. *Subscriber Identity Module*)[12]. Biorąc pod uwagę fakt, że telefony komórkowe są bardziej rozpowszechnione niż komputery oraz to, że karta SIM, posiadając własną pamięć i procesor, identyfikuje abonenta, wybór tej technologii do przechowywania klucza publicznego wydaje się jak najbardziej uzasadniony.

Póki co, podpis mobilny jest na dość wczesnym etapie rozwoju, choć pojawiły się już udane implementacje, m.in. w Finlandii, Turcji oraz w republikach nadbałtyckich. Od 1999 r. istnieje konsorcjum firm mSign, rozwijające standardy w zakresie mobilnego podpisu. Rozpowszechnienie tego systemu będzie wymagało współpracy z istniejącymi podmiotami świadczącymi usługi certyfikacyjne albo stworzenie nowych wystawców kwalifikowanych certyfikatów. Być może to właśnie podpis mobilny stanie się technologią, która spopularyzuje ideę elektronicznego podpisu.

---

[11] Nie zmienia tego fakt, że wiele telefonów komórkowych to w istocie komputery, z własną pamięcią i nowoczesnym systemem operacyjnym.

[12] Karta SIM jest w istocie także kartą mikroprocesorową, ale specjalnego zastosowania. Służy przede wszystkim do identyfikacji abonenta.

2.3. Podpis biometryczny

Biometria to nauka zajmująca się badaniem metod identyfikacji ludzi w oparciu o cechy fizyczne (np. linie papilarne, siatkówka i tęczówka oka, geometria dłoni, twarz) lub sposób zachowania (np. dynamika pisma odręcznego, badanie sposobu mówienia, dynamika pisania na klawiaturze). Metod identyfikacji ludzi w oparciu o cechy biometryczne jest dużo więcej, by wspomnieć chociażby o analizie DNA, układu żył na rękach, sposobie chodzenia, zapachu czy badaniu ucha. Jednakże nie wszystkie z tych metod są odpowiednie do identyfikacji podmiotów składających oświadczenia woli w obrocie elektronicznym.

Jednym z problemów związanych ze stosowaniem podpisu biometrycznego są potencjalne konsekwencje związane z kradzieżą wzorca podpisu z bazy danych. Gdyby przyjąć, że taki wzorzec chronić będzie dostęp do rachunków bankowych czy nieruchomości, wówczas nieuprawnione uzyskanie takiego podpisu może mieć skutki trudne do odwrócenia. Jednakże dzisiejsze bazy danych zawierające tego typu informacje szyfrują podpisy biometryczne i stosują inne technologie utrudniające wykradzenie tego typu danych. Niemniej jednak technologie dostępne dla przeciętnych konsumentów wciąż nie zapewniają wysokiego poziomu bezpieczeństwa[13].

Podpis biometryczny na razie jest stosowany w bardzo ograniczonym zakresie i koncentruje się na wykorzystywaniu takich danych antropomorficznych podpisującego, jak linie papilarne, twarz i tęczówka oka. Próby wykorzystania innych metod, np. badania dynamiki pisania na klawiaturze w celu zdalnej identyfikacji piszącego, nie wychodzą poza fazy laboratoryjne[14]. Na rynku polskim pojawiło się już dość dużo kom-

---

[13] Tak, Wikipedia, http://en.wikipedia.org/wiki/Biometric_signature, ostatni dostęp: 26 lipca 2007 r. zob. także B. S c h n e i e r, *Applied cryptography: protocols, algorithms, and source code in C*, New York-Wiley 1996.

[14] Por. A. K a p c z y ń s k i, *Analiza możliwości wykorzystania behawioralnych metod biometrycznych w kontroli logicznej niestacjonarnej sesji egzaminacyjnej,* dostępny pod adresem: http://www.zsi.pwr.wroc.pl/zsi/missi2004/pdf/Kapczynski%20ADrian.pdf, ostatni dostęp: 27 lipca 2007 r., który przedstawia teoretycznie model zastosowania tej metody oraz metodę własnoręcznego podpisu biometrycznego do zdalnej identyfikacji studentów w procesie egzaminowania przez Internet.

puterów przenośnych oraz palmtopów, które wykorzystują skanery linii papilarnych do identyfikacji użytkownika. Jednakże skanery te póki co mają za zadanie zapewnić ochronę przed nieautoryzowanym uruchomieniem komputera, nie służą natomiast do składania podpisów elektronicznych. Pojawiły się już także pióra elektroniczne, które wykorzystują metody badania dynamiki podpisu do identyfikacji podpisującego.

Metody biometryczne wykorzystywane są już przez organy administracji publicznej w Polsce i wielu krajach na świecie[15], m.in. do identyfikacji właścicieli paszportów i dowodów osobistych. Dane biometryczne mogą też w znaczący sposób wzmocnić podpis kryptograficzny, bowiem, jak to już zostało podkreślone powyżej, podpis ten składany jest i tak za pomocą hasła, które może zostać skradzione lub odgadnięte. Jednakże technologia podpisu biometrycznego koncentruje się na identyfikacji podpisującego, a nie na metodach zajmujących się zapewnieniem integralności danych. Wydaje się, że z tego też względu paszporty biometryczne będą korzystać z podpisu cyfrowego w celu zapewnienia integralności danych biometrycznych zawartych w paszporcie.

2.4. Własnoręczny podpis biometryczny

Własnoręczny podpis biometryczny to szczególny typ podpisu biometrycznego, który opiera się na badaniu dynamiki pisma odręcznego. Podpis ten składa się za pomocą specjalnego bezprzewodowego pióra oraz podkładki (tablet) podłączonej do komputera bądź wbudowanej w przenośny komputer. Ze względu na zasadnicze podobieństwo do tradycyjnego sposobu podpisywania dokumentów może stać się on prawdziwym surogatem podpisu tradycyjnego – stąd też wyróżnienie tego typu podpisu. Co więcej, zebrane informacje o charakterystyce podpisywania się mogą pozwolić na uzyskanie jeszcze większej pewności co do faktu złożenia podpisu przez daną osobę niż podpis kryptograficzny, bowiem ten ostatni może zostać po prostu wykradziony wraz z kartą mikropro-

[15] Por. P. de H e r t, *Biometrics: legal issues and implications.* Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, styczeń 2005, s. 5, dostępny pod: http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf, ostatni dostęp: 27 lipca 2007 r.

cesorową. Dostępne są już pióra elektroniczne, które umożliwiają składanie takich podpisów. Pojawiły się także rozwiązania technologiczne, które wykorzystują algorytmy skrótu (ang. *hash*) oraz znakowanie czasem do zapewnienia integralności podpisywanego dokumentu[16]. Również i przenośne komputery, szczególnie palmtopy, posiadają wbudowaną technologię obsługi pisma własnoręcznego.

2.5. Podpis hasłowy

Kombinacja nazwy użytkownika i hasła (podpis hasłowy) to jeden z najwcześniejszych i wciąż najpopularniejszych sposobów identyfikacji użytkowników w sieci. W zależności od segmentu rynku podpis hasłowy jest generowany i przesyłany użytkownikom przez podmioty profesjonalne (np. elektroniczne banki, organy administracji publicznej) albo tworzony przez samych użytkowników (np. aukcje elektroniczne, sklepy internetowe). Weryfikacja użytkownika następuje poprzez porównanie nazwy użytkownika i hasła ze wzorcem zapisanym w bazie danych.

Ze względu na fakt, że podpis taki może być stosunkowo łatwo wykradziony, wpisywanie hasła jest zwyczajowo ukrywane gwiazdkami lub innymi znakami. Co więcej, zwyczajem staje się wymóg stosowania coraz trudniejszych do złamania haseł. Coraz częściej wymaga się, by hasła były określonej długości (tzn. nie krótsze niż np. 6 znaków), łączyły w sobie zarówno liczby, jak i litery, nie zawierały danych osobowych podpisującego oraz były zmieniane co jakiś czas. Ponadto zwyczajowo szyfruje się przesyłanie tego typu danych, aby uniemożliwić podsłuchującemu ich odczytanie z sieci Internetu[17]. Choć powyższe metody nie gwarantują pełnego bezpieczeństwa, z powodzeniem są one stosowane do identyfikacji uczestników obrotu elektronicznego od początku rozwoju handlu elektronicznego, czyli od połowy lat 90-tych XX wieku.

---

[16] Zob. np. http://www.motiontouch.com/products/signature/faqs/default.asp#q6, 26 lipca 2007 r.

[17] Szerzej na temat zwyczajów w bankowości elektronicznej: P.P. P o l a n s k i, *Customary Law of the Internet: In the Search of the Supranational Cyberspace Law*, The Hague, T.M.C. Asser Press 2007; P.P. P o l a n s k i, *Evidencing trade usages: the case of encryption practices in Internet banking*, [w.] *Business Law & Technology: Present and Emerging Trends, Volume 1.*, red. S.M. Kierkegaard IAITL 2006; P. P o l a ń s k i, *Zwyczaje cyberprzestrzeni*, Prawo Teleinformatyczne 2007, nr 1.

W sytuacji, w której wymagany jest zwiększony poziom bezpieczeństwa, podpis hasłowy łączony jest z dodatkowymi metodami. Przykładowo, polska bankowość elektroniczna, która korzysta z podpisu hasłowego, wzmacnia tego rodzaju system poprzez wymóg stosowania tzw. haseł jednorazowych, by móc dokonać przelewu (np. Inteligo) albo by móc wejść do systemu bankowości elektronicznej (np. Bank Ochrony Środowiska). Hasła te dystrybuowane są albo na kartach haseł jednorazowych (papierowych lub plastikowych), albo w formie tzw. tokenu, czyli specjalnego urządzenia, które „generuje" takie jednorazowe liczby.

Podpis hasłowy nie jest uniwersalną metodą identyfikacji użytkowników wobec różnych podmiotów działających w Internecie. Trudno jest go także wykorzystać do podpisywania oświadczeń woli tworzonych w pełni przez użytkowników (np. e-mail), a nie predefiniowanych przez system informatyczny (np. formularze na stronach e-banku). Jednakże doskonale sprawdza się w systemach zamkniętych, takich jak usługi elektroniczne oferowane przez konkretny bank czy urząd administracji publicznej. Choć nie zapewnia integralności danych, w połączeniu z szyfrowaniem danych wystarcza do personalizacji usług. Stosowany jest w praktycznie wszystkich aplikacjach handlu elektronicznego, w tym do składania podpisu cyfrowego wykorzystującego karty mikroprocesorowe.

2.6. Podpis klawiaturowy

Podpis klawiaturowy to najprostszy z możliwych podpisów elektronicznych. Do jego złożenia wystarczy podpisanie się pod dokumentem czy wiadomością elektroniczną przez piszącego. Oczywiście ta metoda gwarantuje bardzo niski poziom bezpieczeństwa, ponieważ każdy mający dostęp do komputera może teoretycznie podszyć się w ten sposób pod inną osobę. Jednakże w pewnych warunkach taki podpis może zostać uznany za wystarczający dla potrzeb identyfikacji podpisującego. Czynniki, które zwiększają wiarygodność tak złożonego podpisu, to np. wysłanie wiadomości elektronicznej z określonego adresu poczty elektronicznej, która dodatkowo identyfikuje użytkownika, przesłanie takiej wiadomości wraz z kopią poprzedniej korespondencji, co zwiększa prawdopodobieństwo, że wysyłającym jest osoba, która wcześniej korespondowała z adresatem, szyfrowanie komunikacji, stosowanie nagłówków firmowych, czy potwierdzanie faktu przesłania komunikatu drogą elektroniczną.

Nie da się jednak ukryć, że ta metoda podpisywania jest najmniej wiarygodna ze wszystkich dotychczas przedstawionych. Nie gwarantuje ani identyfikacji użytkownika, ani integralności wiadomości. W przeciwieństwie bowiem do innych metod identyfikacji, takich jak podpis hasłowy, dla jego złożenia nie jest wymagana żadna szczególna wiedza prócz imienia i nazwiska podpisującego. Ta metoda jest jednak powszechnie wykorzystywana w codziennej korespondencji za pomocą poczty elektronicznej.

2.7. Podpis skanowany

Podpis skanowany to nic innego jak cyfrowa wersja podpisu wytworzona za pomocą skanera, który tworzy komputerowy obraz podpisu złożonego na papierze. Jest on obarczony podobnymi wadami jak podpis klawiaturowy. Wystarczy bowiem dostęp do listu podpisanego przez osobę, której podpis chcemy podrobić, by móc go zeskanować i dołączyć do wiadomości. Jednak ta metoda jest bardzo rzadko wykorzystywana w praktyce. Dużo częściej skanuje się cały list i przesyła drogą elektroniczną. Wówczas powstają problemy podobne do tych, które wiążą się z wykorzystywaniem urządzeń faksujących.

3. Ramy prawne dla podpisu elektronicznego w UE i Polsce

Ramy prawne dla podpisu elektronicznego wyznacza dyrektywa 1999/93/WE o podpisach elektronicznych[18] i wdrażająca ją do prawa polskiego ustawa z dnia 18 września 2001 r. o podpisie elektronicznym[19]. Celem omawianej dyrektywy jest ułatwienie użytkowania podpisów elektronicznych oraz przyczynienie się do ich uznania prawnego (art. 1). Unia Europejska sięgnęła po instrument harmonizacji po to, by uniknąć fragmentacji rodzącego się dopiero obrotu elektronicznego i przyspieszyć rozwój tego segmentu rynku. Stało się tak dlatego, że pomimo istniejących już międzynarodowych wzorców dotyczących podpisu elektronicznego,

---

[18] Patrz przypis 1. Istotna jest także decyzja Komisji adoptująca trzy standardy przyjęte przez Europejski Komitet Standaryzacyjny w *CEN Workshop Agreement (CWA). Commission Decision of 14 July 2003on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council*, OJ L 175/45, 15 lipca 2003 r.

[19] Ustawa z dnia 18 września 2001 r. (Dz.U. Nr 130, poz. 1450 z późn. zm.).

by wymienić tylko Prawo Modelowe UNCITRAL o handlu elektronicznym z 1996 r.[20] oraz Prawo Modelowe UNCITRAL o podpisach elektronicznych[21], niektóre państwa członkowskie zdecydowały się na własną regulację podpisu.

Warto także zwrócić uwagę na to, że Unia Europejska postrzega podpis elektroniczny jako istotny element ułatwiania korzystania ze swobód rynku wewnętrznego. Przede wszystkim podpis elektroniczny postrzegany jest jako technologia, która może wzmocnić swobodny przepływ usług, oferując szeroki wachlarz zastosowań w zakresie m.in. usług wystawiania i zarządzania certyfikatami, a także usług dotyczących rejestrowania, znakowania czasem, prowadzenia spisów, obliczania lub konsultacji związanych z podpisami elektronicznymi (punkt 9 d.p.e.). Ponadto dyrektywa ma służyć określeniu zasadniczych wymogów dla produktów podpisu elektronicznego, by wspierać zaufanie do nowych technologii i zapewnić swobodny przepływ towarów (punkt 5 d.p.e.). Twórcy dyrektywy zwracają również uwagę na ułatwienia, jakie niesie ze sobą podpis elektroniczny dla osób korzystających ze swobody przepływu osób w kontekście komunikacji z urzędami państwa członkowskiego innego niż to, w którym obywatele i rezydencji UE mają swoje stałe miejsce zamieszkania (punkt 7 d.p.e.).

---

[20] UNCITRAL, *General Assembly Resolution 51/162 of 16 December 1996 – UNCITRAL Model Law on Electronic Commerce with Guide to Enactment with additional Art. 5 bis as adopted in 1998,* 1996, dostępny pod: http://daccessdds.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement, ostatni dostęp: 11 lipca 2007 r. Rozwiązania modelowe zostały następnie przyjęte w najnowszej konwencji o kontraktach elektronicznych. Patrz: UNCITRAL, *General Assembly Resolution 60/21 – United Nations Convention on the Use of Electronic Communications in International Contracts,* A/RES/60/21, 2005, dostępny pod: http://daccessdds.un.org/doc/UNDOC/GEN/N05/488/80/PDF/N0548880.pdf?OpenElement, ostatni dostęp: 25 lutego 2006. Na ten temat patrz: P.Polanski, *UNCITRAL za i przeciw*, Prawo Teleinformatyczne 2007, nr 1; P.P. P o l a n s k i, *Convention on e-contracting: the rise of international law of electronic commerce?* Proceedings of the 19th Bled eCommerce Conference „eValues", Bled, Slovenia 5-7 June 2006; P.P. P o l a n s k i, *The new regime for international electronic contracting*. Proceedings of the 17th Australasian Conference on Information Systems, Adelaide, Australia 6-8 December 2006.

[21] UNCITRAL, *General Assembly Resolution 56/80 – Model Law on Electronic Signatures with Guide to Enactment,* 2001, dostępny pod: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf, ostatni dostęp: 15 lipca 2007 r.

3.1. Podpis elektroniczny (zwykły)

Zgodnie z definicją zawartą w dyrektywie, podpisem elektronicznym są „dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia" (ang. *method of authentication*) (art. 2 pkt 1 dyrektywy). Innymi słowy, podpis elektroniczny to dane w formie elektronicznej, które mają identyfikować autora komunikatu (gr. *ó* – autentyczny od *authentes*, czyli autora[22]). Jednakże kontrowersyjnym zagadnieniem jest kwestia uwiarygodniania treści dokumentu. Posłużenie się w polskiej wersji językowej dyrektywy niejednoznacznym terminem „uwierzytelnienie"[23] prowadzi do niepotrzebnych sporów interpretacyjnych. Niektórzy autorzy przyjmują restryktywną wykładnię tego pojęcia i argumentują, że zwykły podpis elektroniczny musi identyfikować autora, jak również zabezpieczać treść[24]. Większość jednak zdaje się przyjmować szerszą wykładnię tego terminu, pomijającą aspekt zapewnienia integralności treści[25]. Wydaje się, że anglojęzyczny zwrot *authentication* w obszarze nowych technologii jest równoznaczny z pojęciem identyfikacji, a nie rozciąga się już na problematykę autentyczności „podpisywanych" danych[26]. I w ten sposób należy rozumieć polskie tłumaczenie dyrektywy 1999/93/WE.

Mając powyższe na uwadze należy stwierdzić, że definicja podpisu elektronicznego jest bardzo szeroka, co pozwala sprostać założeniom zasady

---

[22] Patrz Wikipedia, http://en.wikipedia.org/wiki/Authentication, ostatni dostęp: 22 lipca 2007 r.

[23] Słownik Naukowy PWN podaje następujące definicje terminu „uwierzytelniać": 1. „uczynić coś wiarygodnym", 2. „stwierdzić autentyczność dokumentu lub podpisu, zgodność z prawem jakiejś czynności prawnej", 3. „zaopatrzyć kogoś w dokumenty stwierdzające powierzenie mu funkcji dyplomatycznej", http://sjp.pwn.pl/lista.php?co=uwierzytelnienie, ostatni dostęp: 22 lipca 2007 r.

[24] Tak J. Jacyszyn, *Podpis elektroniczny w praktyce notarialnej*, Rejent 2003, nr 12, s. 109.

[25] Tak wydaje się, np. J. Jacyszyn, J. Przetocki, A. Wittlin, S. Zakrzewski, *Podpis elektroniczny. Komentarz do ustawy z dnia 18 września 2001 r.*, Warszawa 2002, s. 49.

[26] Por. Wikipedia, http://en.wikipedia.org/wiki/Authentication, ostatni dostęp: 22 lipca 2007 r., szczególnie następujący fragment: *In computer security, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program.*

neutralności technologicznej[27], nakazującej równe traktowanie wszystkich technologii informatycznych. W efekcie każde dane w formie elektronicznej[28] związane w jakiś sposób z podpisywanym komunikatem (poprzez dodanie do komunikatu bądź logiczne z nim powiązanie), które uwierzytelniają komunikat, będą podpisem elektronicznym (dalej: zwykłym podpisem elektronicznym). I tak przykładem takiego podpisu elektronicznego, w którym dane w formie elektronicznej są dodawane do innych danych elektronicznych, może być podpis złożony pod wiadomością e-mailową (podpis klawiaturowy) czy też dołączony do takiej wiadomości zeskanowany podpis tradycyjny (podpis skanowany). Natomiast wykorzystanie numeru PIN do złożenia oświadczenia woli na stronie internetowej banku lub sklepu bądź też do podjęcia środków z bankomatu będzie przykładem podpisu elektronicznego utworzonego poprzez logiczne powiązanie danych elektronicznych z innymi danymi elektronicznymi w sposób umożliwiający autoryzację transakcji. Oczywiście bardziej zaawansowane rodzaje podpisów elektronicznych, takie jak podpis cyfrowy (oparty o infrastrukturę klucza publicznego) czy podpis biometryczny (oparty o cechy podpisującego), są również przykładami podpisu elektronicznego – jednakże ustawodawca europejski przewidział szczególne traktowanie tych technologii, o czym poniżej.

Polska ustawa o podpisie elektronicznym w zasadniczym zakresie przejęła definicję podpisu elektronicznego z dyrektywy 1999/93/WE, niestety nie bez istotnej różnicy. Otóż zgodnie z art. 3 pkt 1 podpis elektroniczny to „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". W polskiej ustawie podpis musi służyć identyfikacji osoby go składającej, a nie być szeroko pojętą metodą uwierzytelnienia. Mówi się wyraźnie o identyfikacji osoby, co

[27] Dyrektywa o podpisach elektronicznych, punkt 8. Podobnie, J. J a c y s z y n, J. P r z e t o c k i, A. W i t t l i n, S. Z a k r z e w s k i, *Podpis elektroniczny…,* s. 49-50.

[28] Dane w formie elektronicznej należy rozumieć szeroko i nie ograniczać tylko do danych reprezentowanych w kodzie binarnym (choć bez wątpienia to najważniejsza technologia), ale także do danych wykorzystujących inne sposoby reprezentacji informacji. J. J a c y s z y n, J. P r z e t o c k i, A. W i t t l i n, S. Z a k r z e w s k i, *Podpis elektroniczny…*, s. 49-50. Amerykańska ustawa o podpisie elektronicznym [sec 2. *Uniform Electronic Transactions Act (1999)*] mówi wyraźnie, że podpis elektroniczny może być sygnałem, symbolem lub procesem. Por. M. D r o z d o w i c z, *Nie(bezpieczny)…*, s. 27.

prowadzi do zawężenia definicji zawartej w dyrektywie, która nie zawiera takiego ograniczenia[29]. Warto w tym miejscu zasygnalizować, że w ustawie czeskiej i austriackiej przyjęto inne rozwiązanie, w którym mówi się o podpisie elektronicznym jako o danych elektronicznych, które są dołączane do innych danych elektronicznych albo są z nimi związane logicznie i służą uwierzytelnieniu, a więc ustaleniu tożsamości sygnatariusza[30].

W literaturze przedmiotu pojawiły się głosy aprobujące polską definicję podpisu, zwracając uwagę na podstawową funkcję podpisu, jaką jest identyfikacja osoby fizycznej oraz wpływ Praw Modelowych UNCITRAL z 1996 i 2001 r.[31] Sympatyzując z potrzebą tworzenia bardziej liberalnych reguł na poziomie wspólnotowym, dodatkowo wspartych przez równie uniwersalne ujęcie podpisu w najnowszej konwencji UNCITRAL o kontraktach elektronicznych[32], należy podkreślić jednak konieczność wypełnienia zobowiązania osiągnięcia celu nałożonego przez dyrektywę (art. 249 TWE). A tak odmienne ujęcie podpisu elektronicznego może spowodować szereg problemów związanych z funkcjonowaniem rynku wewnętrznego.

Po pierwsze, powstają trudności ze stosowaniem pojęcia podpisu elektronicznego do zautomatyzowanego sposobu zawierania umów, w którym do transakcji dochodzi wyłącznie za pomocą oprogramowania. Szczególne problemy mogą powstać na tle korzystania z systemów Elektronicznej Wymiany Danych (ang. *Electronic Data Interchange (*EDI*)*)[33]. Systemy te opierają się na dwustronnie zautomatyzowanej komunikacji profesjonalnej, w której oświadczenia woli składane są przez

---

[29] Jednakże przyjęcie, że pojęcie uwierzytelnienia odnosi się zarówno do identyfikacji autora, jak i uwierzytelnienia autentyczności dokumentu, prowadzi do wniosku, że polska ustawa przyjęła w tym zakresie szerszą definicję podpisu elektronicznego od dyrektywy. Tak J. J a c y s z y n, *Podpis...*, s. 109.

[30] Za D. S z o s t e k, *Czynność prawna a środki komunikacji elektronicznej*, Kraków 2004, s. 237.

[31] Tak, W.J. K o c o t, *Wpływ Internetu na prawo umów*, Warszawa 2004, s. 344 i 352.

[32] Por. przypis 6.

[33] R. C l a r k, *Electronic Data Interchange (EDI): An Introduction,* December 1998, dostępny pod: http://www.anu.edu.au/people/Roger.Clarke/EC/EDIIntro.html, ostatni dostęp: 15 lipca 2007 r.

odpowiednio zaprogramowane aplikacje korzystające z jednakowych standardów reprezentacji informacji, a nie przez identyfikowalne osoby fizyczne. Powstaje więc uzasadniona obawa, że tego typu technologie nie będą uznane za wypełniające założenia polskiej definicji podpisu elektronicznego[34]. Jest to sytuacja o tyle kuriozalna, że systemy EDI wykorzystywane są powszechnie w praktyce handlowej od lat 70-tych XX wieku, a polskie rozporządzenie o e-fakturach zrównało pod względem skutków prawnych ten sposób składania oświadczeń woli z bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego, kwalifikowanego certyfikatu[35].

Po drugie, różne wymogi dla zwykłego podpisu elektronicznego w Polsce i pozostałych krajach unijnych i tak stawiają naszą administrację i przedsiębiorców przed wymogiem respektowania innych podpisów elektronicznych ze względu na zasadę państwa pochodzenia zapisaną w dyrektywie o podpisach elektronicznych oraz w dyrektywie o handlu elek-

---

[34] Por. W.J. K o c o t, *Wpływ Internetu...*, s. 352-354. Autor zauważa, że wobec faktu, iż treść umowy jest kształtowana przez programy komputerowe, a z technicznego punktu widzenia nie dochodzi do wymiany dokumentów, „pojawiają się zasadnicze wątpliwości, czy zawieranie umów w sposób zautomatyzowany z zachowaniem elektronicznej postaci formy pisemnej jest *de lege lata* możliwe." s. 354. Por. także M. Ś w i e r c z y ń s k i, *Podpis elektroniczny,* [w:] *Prawo Internetu*, red. P. Podrecki, Warszawa 2004, s. 67. O możliwości zastosowania podpisu elektronicznego w stosunku do osób prawnych – zob. D. S z o s t e k, *Czynność prawna...*, s. 238-243.

[35] Rozporządzenie Ministra Finansów z dnia 14 lipca 2005 r. w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, a także przechowywania oraz udostępniania organowi podatkowemu lub organowi kontroli skarbowej tych faktur (Dz.U. Nr 133, poz. 1119) (dalej: rozporządzenie o e-fakturach), wdrażające postanowienia dyrektywy Rady 2001/115/WE z dnia 20 grudnia 2001 r. zmieniającej dyrektywę 77/388/EWG w celu uproszczenia, modernizacji i harmonizacji ustanowionych warunków fakturowania w zakresie podatku od wartości dodanej (Dz.Urz. UE L 15/24 z 17.01.2002 r.). § 4 rozporządzenia o e-fakturach stanowi: „Faktury mogą być wystawiane, przesyłane i przechowywane w formie elektronicznej, pod warunkiem że autentyczność ich pochodzenia i integralność ich treści będą zagwarantowane: 1) bezpiecznym podpisem elektronicznym w rozumieniu art. 3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450, z późn. zm. 3), weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub 2) poprzez wymianę danych elektronicznych (EDI) zgodnie z umową w sprawie europejskiego modelu wymiany danych elektronicznych, jeżeli zawarta umowa, dotycząca tej wymiany, przewiduje stosowanie procedur gwarantujących autentyczność pochodzenia faktury i integralność danych" (przypisy pominięto).

tronicznym[36]. A by uniknąć zasygnalizowanych powyżej problemów, należy skorzystać z zasady prowspólnotowej wykładni prawa krajowego i postulować dokonanie rozszerzającej wykładni pojęcia „osoby składającej podpis elektroniczny" w świetle celów dyrektywy 1999/93/WE i objęcie nią jak najszerszej grupy desygnatów tego pojęcia występujących w obrocie.

Zwykły podpis elektroniczny wywołuje skutki określone w art. 5 ust. 2 dyrektywy. Zgodnie z tym postanowieniem nie można odmówić podpisowi elektronicznemu skuteczności prawnej i dopuszczalności jako dowodu w postępowaniu sądowym jedynie dlatego, że jest w formie elektronicznej bądź nie wykorzystuje innych technologii wspomnianych w dyrektywie. Podobnie wygląda implementacja tego postanowienia w polskiej ustawie. Zgodnie z art. 8 „nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego". Oznacza to, że każdy zwykły podpis elektroniczny będzie mógł być dopuszczony jako dowód w postępowaniu sądowym, nie gwarantując jednak jego uznania w konkretnej sprawie. Wszystkie omówione powyżej rodzaje podpisu elektronicznego są zwykłym podpisem elektronicznym w rozumieniu art. 5 ust. 2 dyrektywy i art. 8 ustawy.

3.2. Bezpieczny (zaawansowany) podpis elektroniczny

Przedstawione powyżej przykłady zwykłego podpisu elektronicznego mają różną moc dowodową – od słabej w przypadku zwykłego podpisu klawiaturowego przez silniejszą w przypadku stosowania podpisu hasłowego po bardzo silną w przypadku podpisu cyfrowego. Zdając sobie sprawę ze zróżnicowania dostępnych technologii pod kątem ich wiarygodności i chcąc zapewnić niektórym z nich bardziej uprzywilejowane miejsce, dyrektywa 1999/93/WE wprowadziła definicję bezpiecznego (ang. *advanced*) (*sic!*) podpisu elektronicznego, który musi spełnić szereg

[36] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce)*, OJ L 178/1 z 12.11.2000 r.

dodatkowych wymagań w stosunku do zwykłego podpisu elektronicznego. Zgodnie z art. 2 pkt 2 dyrektywy o podpisach elektronicznych „»bezpieczny podpis elektroniczny« oznacza podpis elektroniczny spełniający następujące wymogi: a) przyporządkowany jest wyłącznie podpisującemu, b) umożliwia ustalenie tożsamości podpisującego, c) stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą i d) jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych może zostać wykryta."

Dwa pierwsze wymogi wydają się niepotrzebnym powtórzeniem. Skoro bezpieczny podpis elektroniczny ma umożliwiać ustalenie tożsamości podpisującego, to musi być on wyłącznie jemu przyporządkowany. Innymi słowy, ustalenie tożsamości podpisującego czyni zbędnym kwestię badania, czy podpis ten był wyłącznie jemu podporządkowany. Wynika stąd, że pierwszy element definicji jest w zasadzie zbędny. Istotniejsze jednak jest to, że nie wszystkie technologie podpisu elektronicznego spełniają te warunki. Otóż zwykły podpis pod wiadomością zapewnia stosunkowo słabe możliwości wiarygodnego ustalenia tożsamości podpisującego, bowiem każdy mógłby wpisać określone imię i nazwisko. Z kolei z pewnością warunek ten spełnia podpis biometryczny, podpis cyfrowy, a także podpis za pomocą nazwy użytkownika i hasła.

Jeszcze bardziej niejasny jest wymóg środków, które podpisujący może mieć pod swoją wyłączną kontrolą. Chodzi zapewne o środki technologiczne, takie jak klawiatura komputera, bezprzewodowe pióro, czytnik linii papilarnych, karta mikroprocesorowa itp. Nie jest jednak klarowne, czy środki te muszą być przez cały czas w posiadaniu podpisującego (np. domowy komputer, czytnik i karta mikroprocesorowa), czy też chodzi tu o kontrolę nad tymi środkami w momencie składania podpisu (np. klawiatura w bankomacie). W efekcie nie jest jasne, czy podpis złożony za pomocą hasła i numeru klienta w kafejce internetowej spełnia ten warunek, czy też nie. Jak się jednak okaże dalej, wymóg ten nie będzie odgrywał praktycznego znaczenia, a to ze względu na konieczność posiadania tzw. bezpiecznego urządzenia do składania podpisu elektronicznego dla wywołania skutków równoważnych podpisowi własnoręcznemu.

Ostatnim wymogiem bezpiecznego podpisu elektronicznego jest to, by umożliwiał on sprawdzenie integralności podpisywanych danych. Nie każda

z przedstawionych powyżej technologii podpisu elektronicznego zapewnia tego rodzaju możliwość. Z pewnością warunku tego nie spełniają podpis skanowany czy podpis hasłowy. Sytuacja nie jest jasna w odniesieniu do podpisu biometrycznego, bowiem ta technologia koncentruje się na identyfikacji użytkownika, a nie integralności danych. Z drugiej strony, warunek ten, a co za tym idzie i wszystkie poprzednie kryteria bezpiecznego podpisu elektronicznego, spełnia podpis cyfrowy, ze względu na stosowaną w nim funkcję skrótu, która jest podpisywana kluczem prywatnym, a także podpis mobilny oraz własnoręczny podpis biometryczny (pod warunkiem, że zapewnia możliwość sprawdzenia integralności danych).

Bezpieczny podpis elektroniczny w polskiej ustawie to taki podpis elektroniczny, który: „a) jest przyporządkowany wyłącznie do osoby składającej ten podpis, b) 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, c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna." (art. 3 pkt 2 ustawy).

Polska ustawa wymaga m.in. zastosowania bezpiecznych urządzeń oraz danych służących do składania podpisu elektronicznego, które są zdefiniowane w ustawie i uszczegółowione w rozporządzeniu wykonawczym o warunkach technicznych[37]. Dane służące do składania podpisu zdefiniowane są szeroko, jako „niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego" (art. 3 ust. 4). Dyrektywa wyjaśnia, że może być to np. klucz prywatny lub kod. Natomiast bezpieczne urządzenie służące do składania podpisu elektronicznego to „sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu przy wykorzystaniu danych służących do składania podpisu i spełniające wymagania określone w ustawie" (art. 3 ust. 6 i 7). Ustawa precyzuje w art. 18, że bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej: „1) uniemożliwiać pozyskiwanie danych służących do składania podpisu lub poświadczenia elektronicznego, 2) nie zmieniać

[37] Zob. przypis 1.

danych, które mają zostać podpisane lub poświadczone elektronicznie, oraz umożliwiać przedstawienie tych danych osobie składającej podpis elektroniczny przed chwilą jego złożenia, 3) gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ze złożeniem podpisu elektronicznego, 4) zapewniać łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian w urządzeniu do składania podpisu lub poświadczenia elektronicznego." Rozporządzenie wykonawcze o warunkach technicznych tworzy nową siatkę pojęciową (m.in. komponent techniczny[38], oprogramowanie podpisujące[39], oprogramowanie publiczne[40], atrybut podpisu[41], moduł kluczowy[42], bezpieczna ścieżka[43], bezpieczny kanał[44] itd.) i nakłada dalsze obowiązki w związku ze stosowaniem bezpiecznych urządzeń. Bezpiecz-

[38] § 2 pkt 6 komponent techniczny – sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

[39] § 2 pkt 7 oprogramowanie podpisujące – oprogramowanie, które przygotowuje dane, które mają zostać podpisane lub poświadczone elektronicznie, i przesyła je do komponentu technicznego.

[40] § 2 pkt 9 oprogramowanie publiczne – oprogramowanie podpisujące, do którego w normalnych warunkach eksploatacji może mieć dostęp każda osoba fizyczna; oprogramowaniem publicznym nie jest w szczególności oprogramowanie używane w mieszkaniu prywatnym, lokalu biurowym lub telefonie komórkowym.

[41] § 2 pkt 4 atrybut podpisu – dodatkowe dane, które są podpisywane razem z podpisywanymi danymi lub do nich logicznie dołączane, a w szczególności: a) wskazanie kwalifikowanego certyfikatu lub kwalifikowany certyfikat służący do weryfikacji podpisu elektronicznego, b) oznaczenie czasu, c) format zawartości, umożliwiający w szczególności ustalenie sposobu kodowania podpisanych elektronicznie danych.

[42] § 2 pkt 11 moduł kluczowy – urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury lub dane służące do składania bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych, lub klucze chroniące te dane, lub przechowujące części tych kluczy lub danych.

[43] § 2 pkt 12 bezpieczna ścieżka – łącze zapewniające wymianę między oprogramowaniem podpisującym a komponentem technicznym informacji związanych z uwierzytelnieniem użytkownika komponentu technicznego, zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

[44] § 2 pkt 13 bezpieczny kanał – łącze zapewniające wymianę między oprogramowaniem podpisującym a komponentem technicznym informacji związanych z przekazywaniem danych, które mają być podpisane lub poświadczone elektronicznie, zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

ne urządzenie ma uniemożliwiać odtworzenie jakichkolwiek danych na nim zawartych poprzez analizę fizyczną urządzenia. W przypadku stosowania haseł do złożenia podpisu, co jest standardem w przypadku podpisu cyfrowego składanego za pomocą karty mikroprocesorowej, należy zapewnić zwyczajową możliwość zmiany hasła oraz jego zablokowania po kilkukrotnym nieudanym zarejestrowaniu[45]. Natomiast w przypadku stosowania publicznie dostępnego oprogramowania do składania i weryfikacji podpisów, takiego jak PGP, konieczne jest stosowanie bezpiecznej ścieżki oraz szyfrowania danych. Rozporządzenie nakłada jeszcze więcej o wiele bardziej szczegółowych wymogów, zarówno na tzw. komponent techniczny (np. bezpieczna obudowa, testy pamięci i kluczy, zarządzenie urządzeniem), jak i na stosowane oprogramowanie (np. stosowanie dopuszczonych algorytmów szyfrujących oraz funkcji skrótu, niszczenie danych służących do składania podpisu po zakończeniu transmisji), co nie będzie dokładniej analizowane w niniejszym artykule[46]. Już bowiem analiza powyższych przepisów prowadzi do wniosku, że większość technologii zwykłego podpisu elektronicznego nie będzie spełniać warunków nałożonych przez polskie prawo. Nie tylko podpis klawiaturowy czy skanowany, ale także podpis hasłowy będą wyłączone ze względu na wymogi bezpiecznego urządzenia do składania podpisu elektronicznego. Warunki te może spełnić tylko podpis cyfrowy, w tym mobilny podpis cyfrowy, oraz podpis biometryczny, szczególnie własnoręczny podpis biometryczny.

W odniesieniu do polskiej implementacji definicji bezpiecznego podpisu elektronicznego trzeba wskazać na trzy zasadnicze różnice w stosunku do dyrektywy. Po pierwsze, w naszej definicji tzw. bezpiecznego podpisu elektronicznego znalazł się m.in. wymóg złożenia go przy użyciu bezpiecz-

---

[45] Szerzej na ten temat patrz np. P. P o l a n s k i, *Rola i znaczenie zwyczaju w transakcjach elektronicznych*, [w.] *Kolizyjne aspekty zobowiązań elektronicznych*, red. J. Gołaczyński, Kraków 2007; P.P. P o l a n s k i, *Custom as a Source of Supranational Internet Commerce Law (PhD Thesis),* The University of Melbourne, July 2003, dostępny pod: http://eprints.unimelb.edu.au/, ostatni dostęp: 1 czerwca 2007 r.; P.P. P o l a n s k i, *Customary Law of the Internet: In the Search for a Supranational Cyberspace Law*, The Hague, T.M.C. Asser Press 2007; P. P o l a ń s k i, *Zwyczaje cyberprzestrzeni*, Prawo Teleinformatyczne 2007, nr 1.

[46] Szerzej, patrz rozdział II: Rozporządzenia o warunkach technicznych.

nych urządzeń służących do składania podpisu elektronicznego, co stanowi błędne wdrożenie definicji zawartej w dyrektywie 1999/93/WE. Pojęcie bezpiecznych urządzeń nie występuje w definicji bezpiecznego podpisu elektronicznego w dyrektywie, a dopiero przy określaniu przesłanek równoważności takiego podpisu z podpisem własnoręcznym. Po drugie, owe bezpieczne urządzenia do składania podpisu elektronicznego muszą pozostawać pod kontrolą podpisującego, a nie tylko mogą pozostawać, jak zakłada dyrektywa. Doktryna zwróciła uwagę na tę zmianę i uznała ją za zasadniczy błąd implementacyjny, ponieważ technicznymi metodami nigdy nie da się spełnić tego warunku[47]. Po trzecie, polski ustawodawca usunął drugą przesłankę bezpiecznego podpisu elektronicznego i przeniósł ją do definicji zwykłego podpisu elektronicznego.

Należy podkreślić z całą stanowczością, że dodanie nowego kryterium do definicji zawartej w dyrektywie stanowi istotny błąd implementacyjny, który skutkować może utrudnieniem obrotu elektronicznego wewnątrz Wspólnoty i w konsekwencji odpowiedzialnością państwa polskiego za naruszenie prawa wspólnotowego. Trudno znaleźć jakiekolwiek racjonalne powody, dla których ustawodawca miałby zmieniać definicje zawarte w dyrektywach, poza przypadkami, w których nie ulegnie zmianie krąg desygnatów, a jedynie ułatwi się przekaz treści. Takie zmiany niezwykle utrudniają harmonizację przepisów państw członkowskich. A podmiotom działającym na rynku wspólnotowym nie pozostaje nic innego jak próba powołania się na zasadę skutku bezpośredniego dyrektywy wobec naszego państwa lub dokonania wykładni naszej definicji w świetle tej zawartej w dyrektywie.

Na koniec należy wspomnieć o skutkach, jakie wywołuje bezpieczny podpis elektroniczny. Należałoby się spodziewać większych ułatwień w postępowaniu dowodowym czy w odniesieniu do równoważności takiego podpisu z podpisem własnoręcznym. Jednakże ani w dyrektywie, ani w polskiej ustawie nie znajdziemy przepisów, które przyznawałyby bezpiecznemu podpisowi elektronicznemu jakąś szczególną pozycję, wyższą od tej zagwarantowanej dla zwykłego podpisu elektronicznego. Można

[47] Por. np. W.J. K o c o t, *Wpływ Internetu...*, s. 354; D. S z o s t e k, *Prawne aspekty podpisu elektronicznego,* [w:] *Handel elektroniczny*, red. J. Barta, R. Markiewicz, Kraków 2005, s. 180.

traktować to jako pewnego rodzaju niekonsekwencję ustawodawcy wspólnotowego, trudno bowiem racjonalnie uzasadnić wyróżnienie tej kategorii podpisów. Konstatacji tej nie zmienia fakt, że to właśnie bezpieczny podpis elektroniczny jest fundamentem tzw. kwalifikowanego podpisu elektronicznego, na którym skupia się cała uwaga doktryny i praktyki.

3.3. Kwalifikowany podpis elektroniczny

Choć dyrektywa nie wyróżnia *expressis verbis* trzeciego typu podpisu, to jednak takie wyróżnienie jest uzasadnione dodatkowymi wymogami, jakie nałożył ustawodawca europejski na bezpieczny podpis elektroniczny, by mógł być on zrównany pod względem skutków prawnych z podpisem własnoręcznym. Aby osiągnąć ten cel, bezpieczny podpis elektroniczny w rozumieniu prawa wspólnotowego musi wykorzystywać kwalifikowany certyfikat oraz bezpieczne urządzenie do składania podpisu elektronicznego. Obydwa pojęcia są zdefiniowane w dyrektywie i polskiej ustawie.

Certyfikat to „zaświadczenie elektroniczne, za pomocą którego dane służące do weryfikacji podpisu są przyporządkowane osobie i potwierdzają tożsamość tej osoby." Natomiast certyfikat kwalifikowany oznacza certyfikat spełniający dwa rodzaje wymogów. Po pierwsze, certyfikat kwalifikowany musi spełniać pewne minimum treściowe określone w załączniku I dyrektywy. Po drugie, musi być on wystawiony przez podmiot świadczący usługi certyfikacyjne, który z kolei spełnia wymogi ustanowione w załączniku II dyrektywy.

Certyfikat kwalifikowany musi zawierać następującą treść: „a) wskazanie, że dany certyfikat został wystawiony jako certyfikat kwalifikowany; b) dane określające podmiot świadczący usługi certyfikacyjne i państwo, w którym ma swoją siedzibę; c) nazwę podpisującego lub pseudonim, który można jako taki rozpoznać; d) zastrzeżenie szczególnej cechy podpisującego, włączane, gdy jest to stosowne, w zależności od przeznaczenia certyfikatu; e) dane służące do weryfikacji podpisu, które odpowiadają danym służącym do składania podpisu kontrolowanym przez podpisującego; f) dane dotyczące początku i końca okresu ważności certyfikatu; g) kod identyfikacyjny certyfikatu; h) bezpieczny podpis elektroniczny wystawiającego podmiotu świadczącego usługi certyfikacyjne; i) w odpowiednim przypadku, ograniczenia zakresu użycia cer-

tyfikatu oraz j) w odpowiednim przypadku, granice wartości transakcji, do których można stosować certyfikat".

Certyfikat kwalifikowany musi być także wystawiony przez taki podmiot świadczący usługi certyfikacyjne, który powinien spełnić szereg wymogów, m.in. zapewnić wiarygodność infrastrukturze podpisu poprzez sprawdzenie za pomocą stosownych środków zgodnych z prawem krajowym tożsamości i, w odpowiednim przypadku, cech szczególnych osoby, dla której wydaje kwalifikowany certyfikat. Interesujące jest to, że dyrektywa unijna, a także polska ustawa, nie uzależniają świadczenia usług certyfikacyjnych od uprzedniego zezwolenia, a wprowadzają system dobrowolnej akredytacji. Jednakże przykład Polski pokazuje, że system ten jest skrajnie sformalizowany, a zagraniczne i nawet wspólnotowe podmioty świadczące usługi certyfikacyjne nie są uznawane przez polski porządek prawny. Jest tak ze względu na wymóg, żeby zagraniczny podmiot świadczący usługi certyfikacyjne spełniał albo wymogi przewidziane polskim prawem i uzyskał stosowną gwarancję bądź akredytację w UE, albo został wpisany do krajowego rejestru takich podmiotów, albo został uznany (podmiot lub certyfikat) w drodze umowy międzynarodowej zawartej przez Wspólnotę Europejską a państwem trzecim lub organizacją międzynarodową (art. 4 u.p.e.). Polskie rozwiązanie stoi w sprzeczności z zasadą państwa pochodzenia zawartą w dyrektywie, zgodnie z którą „Państwa Członkowskie nie mogą ograniczać świadczenia usług certyfikacyjnych pochodzących z innych Państw Członkowskich w dziedzinach objętych tą dyrektywą" (art. 4 d.p.e.).

Zgodnie z prawem wspólnotowym podpis równoważny własnoręcznemu musi prócz kwalifikowanego certyfikatu korzystać także z bezpiecznego urządzenia służącego do składania podpisów, które zgodnie z definicją oznacza urządzenie służące do składania podpisów, spełniające wymogi załącznika III dyrektywy. Takie urządzenia muszą zapewnić „właściwe środki techniczne i proceduralne", w tym co najmniej, że: „a) dane służące do składania podpisu użyte do złożenia podpisu praktycznie pojawiają się tylko raz oraz zapewniona jest ich poufność; b) dane służące do składania podpisu użyte do złożenia podpisu nie mogą, przy zachowaniu rozsądnego zabezpieczenia, być pozyskane oraz podpisy są chronione przed fałszowaniem przy użyciu dostępnej technologii; c) dane służące do składania podpisu użyte do złożenia podpisu chronione są przez

uprawnionego podpisującego się w sposób godny zaufania przed użyciem przez innych." Ponadto bezpieczne urządzenia nie mogą zmieniać danych służących do składania podpisu (np. klucza prywatnego) i umożliwiają przedstawienie tych danych podpisującemu przed złożeniem podpisu. Zgodność bezpiecznych urządzeń służących do składania podpisu ze wskazanymi wyżej wymogami stwierdzać ma właściwy organ publiczny lub prywatny, wskazany przez państwo członkowskie (art. 3 ust. 4 d.p.e.). Jednakże wskazane przez dyrektywę wymagania organizacyjne i techniczne nie obejmują całego środowiska systemowego, w którym działa urządzenie.

Istniejące ramy prawne dla podpisu elektronicznego zdecydowanie faworyzują technologie oparte o infrastrukturę klucza publicznego. Dyrektywa, choć formalnie kładzie nacisk na zasadę neutralności technologicznej, zrównuje pod względem skutków prawnych podpis własnoręczny jedynie z bezpiecznym podpisem elektronicznym (ang. *advanced electronic signatures*)[48], wykorzystującym kwalifikowany certyfikat i złożonym za pomocą bezpiecznego urządzenia służącego do składania podpisów[49]. Z kolei kwalifikowany certyfikat musi być wystawiony przez podmiot świadczący usługi certyfikacyjne, który musi spełniać rozbudowane wymogi prawne. Z pewnością to jeden z zasadniczych powodów braku akceptacji podpisu elektronicznego przez rynek, istnieje bowiem wiele prostszych i tańszych metod przypisania klucza publicznego konkretnej osobie: autopublikacja klucza, poświadczenie wydane przez zaufaną osobę trzecią czy też wystawienie klucza przez organ publiczny w oparciu o identyfikator osoby podpisującej, np. PESEL[50]. Inne rodzaje podpisów elektronicznych nie będą odnosiły podobnego skutku – nie można jednakże odmówić im skuteczności prawnej i dopuszczalności jako dowodu w postępowaniu sądowym z tego tylko względu, że są w formie elektronicznej, nie wykorzystują certyfikatów czy bezpiecznych urządzeń do składania podpisu[51].

W porównaniu ze stopniem szczegółowości scharakteryzowanych powyżej nakazów zawartych w naszej ustawie i rozporządzeniu, dyrektywa

---

[48] Por. np. D. Szostek, M. Świerczyński, *Prawne możliwości...*, s. 180-184.

[49] Art. 5 ust. 1 pkt a dyrektywy o podpisie elektronicznym. Por. krytyczne uwagi do redakcji tego artykułu w D. Szostek, *Czynność prawna...* s. 234-235.

[50] Szerzej M. Kutyłowski, *Bezdroża koncepcji...*, s. 5 i nast.

[51] Por. art. 5 ust. 2 dyrektywy o podpisie elektronicznym.

wspólnotowa jawi się jednak jako instrument wyjątkowo przejrzysty i technologicznie neutralny. W tym miejscu można jeszcze dodać, że zgodnie z art. 3 ust 7 dyrektywy, państwa członkowskie mogą poddać stosowanie podpisów elektronicznych w sektorze publicznym ewentualnym wymogom dodatkowym. Wymogi te muszą być obiektywne, przejrzyste, proporcjonalne, niedyskryminujące i mogą odnosić się jedynie do szczególnych cech danych zastosowań. Wymagania te nie mogą także stanowić przeszkód w ponadgranicznych usługach dla obywatela. Patrząc jednak na naszą implementację dyrektywy unijnej, trudno wyobrazić sobie jeszcze bardziej skomplikowany system.

W polskim prawie wymagania co do bezpiecznych urządzeń służących do elektronicznego podpisywania, treści kwalifikowanego certyfikatu, jak i wymogów, które musi spełnić podmiot świadczący takie usługi, są jeszcze bardziej rozbudowane, co widać na przykładzie problematyki bezpiecznych urządzeń. Natomiast skutki zwykłego, bezpiecznego i kwalifikowanego podpisu elektronicznego określone są w art. 5 ust. 2 i art. 8 u.p.e. Zgodnie z art. 5 ust. 2 u.p.e. „dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej." W obrocie cywilnoprawnym identyczną funkcję pełni art. 78 § 2 k.c.[52], który przewiduje, że dla zachowania zwykłej formy pisemnej wystarczy złożenie bezpiecznego podpisu elektronicznego weryfikowanego za pomocą kwalifikowanego certyfikatu. Należy zwrócić uwagę, że nowelizacja kodeksu cywilnego pominęła wymóg ważności kwalifikowanego certyfikatu, jednakże wymóg ten obowiązuje ze względu na obowiązek prowspólnotowej wykładni prawa krajowego[53]. Chociaż sama dyrektywa nie nakazuje *expressis*

[52] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 1964 r. Nr 16, poz. 93 ze zm.).

[53] Problematyka statusu art. 5 § 2 u.p.e. jest kontrowersyjna. Niektórzy autorzy argumentują, że wymóg ważności certyfikatu obowiązuje ze względu na fakt, iż art. 5 u.p.e. stanowi *lex specialis* wobec regulacji kodeksowej – tak W.J. K o c o t, *Wpływ Internetu...*, s. 355. Wydaje się jednak, że powinno być dokładnie odwrotnie, skoro ustawa o podpisie elektronicznym ma znacznie szerszy zakres zastosowania.

verbis stosowania ważnego certyfikatu, wymóg taki wynika pośrednio z obowiązków nałożonych na podmioty świadczące usługi certyfikacyjne, które muszą m.in. zapewnić świadczenie usług szybkiego i bezpiecznego zarządzania oraz pewnego i natychmiastowego odwołania certyfikatu oraz zapewnić dokładne określenie daty i godziny jego wystawienia lub cofnięcia. Co więcej, przyjęcie odmiennego punktu widzenia prowadziłoby do rezultatów absurdalnych, ponieważ infrastruktura klucza publicznego jest tak skonstruowana, aby uznawać tylko ważne certyfikaty.

Z kolei art. 8 ustawy dopuszcza stosowanie wszelkich technik identyfikujących osobę podczas dokonywania czynności prawnej jako podpisów elektronicznych. Zgodnie z tym przepisem, „nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego." Oznacza to, że w polskim prawie dopuszczalne są wszystkie omówione w tym artykule technologie podpisu elektronicznego.

4. Podsumowanie

Prawodawca europejski i ustawodawca polski są świadomi istnienia różnych technologii, które mogą być wykorzystane do podpisywania dokumentów w obrocie elektronicznym. Z tego też powodu prawo europejskie i polska ustawa o podpisie elektronicznym nakazuje wzięcie pod uwagę innych technologii niż wyraźnie preferowany podpis kryptograficzny i dopuszczenie ich jako dowodów w postępowaniach sądowych. Co więcej, tym różnym technologiom składania podpisów nie można odmówić skutku prawnego – od najmniej wiarygodnego w postaci podpisu klawiaturowego czy zeskanowanego, po stosunkowo bezpieczne, poczynając od podpisu hasłowego, przez różnorakie formy podpisu biometrycznego i podpisu cyfrowego.

Jednakże tylko dokument opatrzony bezpiecznym podpisem cyfrowym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu został zrównany pod względem skutków prawnych z dokumentem podpisanym odręcznie. Polski ustawodawca wprowadza nawet trzy odrębne domniemania dotyczące kwalifikowanego podpisu elektronicznego. Po

pierwsze, stanowi on „dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny". Po drugie, nie można powoływać się, że „nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny". Po trzecie, polska ustawa, dopuszczając wykorzystanie kwalifikowanego podpisu cyfrowego do znakowania czasem, stworzyła domniemanie, że „podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usług".

Póki co jednak podpis elektroniczny nie jest szeroko stosowany ani w obrocie prywatnoprawnym, ani w obrocie publicznoprawnym, pomimo wielu aktów prawnych dopuszczających jego stosowanie. Ustawa o podpisie elektronicznym nałożyła wręcz obowiązek umożliwienia wnoszenia podmiotom prywatnym podań opatrzonych podpisem elektronicznym. Zgodnie z art. 58 § 2 „w terminie do dnia 1 maja 2008 r. organy władzy publicznej umożliwią odbiorcom usług certyfikacyjnych wnoszenie podań i wniosków oraz innych czynności w postaci elektronicznej w przypadkach, gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru". Jednakże przepis ten został już raz znowelizowany, wydłużając okres dostosowawczy organów władzy publicznej o blisko 2 lata. Niestety po raz kolejny nie udało się dotrzymać ustawowego terminu, a to ze względu na wciąż bardzo słabo przygotowaną kadrę urzędniczą oraz niewielką popularność podpisu cyfrowego.