Sylwia Kotecka

Rozdział 2. Podpis elektroniczny

1. Wprowadzenie

Komunikacja elektroniczna i handel elektroniczny wymagają innych instrumentów identyfikacji stron umowy niż te, które stosowano przy umowach sporządzanych na papierze i zawieranych tradycyjnie, w obecności stron. Nie można bowiem z całą stanowczością stwierdzić, czy podpis na piśmie otrzymanym np. drogą faksową jest autentyczny i czy został złożony własnoręcznie. Technicznie jest bowiem możliwe skopiowanie podpisu z innego dokumentu i przeniesienie go na dokument, który zostanie następnie przefaksowany, w taki sposób, że nie da się stwierdzić tego faktu.

Podpisy elektroniczne i usługi certyfikacyjne z nimi powiązane umożliwiają uwierzytelnianie danych i potwierdzanie tożsamości osób uczestniczących w transakcjach zawieranych na odległość. Zasadniczymi celami stawianymi przed podpisem elektronicznym są: bezpieczna i pewna weryfikacja osoby dokonującej elektronicznej czynności prawnej oraz brak możliwości zaprzeczenia uczestnictwa w elektronicznej czynności prawnej. Dokument elektroniczny obejmujący oświadczenie woli i opatrzony podpisem elektronicznym powinien mieć prawne znaczenie takie, jak dokument sporządzony na papierze i podpisany podpisem własnoręcznym. Dzięki używaniu tych instrumentów możliwe stało się proste i szybkie zawieranie umów między podmiotami znajdującymi się czy mającymi siedziby w różnych państwach, na różnych kontynentach. Jednakże rozbieżne reguły odnoszące się do prawnego uznawania podpisów elektronicznych i akredytacja podmiotów świadczących usługi certyfikacyjne w różnych krajach mogą stanowić poważną przeszkodę w komunikacji elektronicznej i handlu elektronicznym. Ma to ogromne znaczenie dla państw członkowskich Unii Europejskiej, ponieważ ich przepisy prawne nie powinny ograniczać swobodnego przepływu towarów i usług na rynku wewnętrznym.

2. Podpis własnoręczny

Dotychczas ustawodawca nie stworzył definicji pojęcia „podpis własnoręczny", pozostawiając jej wyjaśnienie nauce prawa i orzecznictwu sądowemu[1]. Według po-

[1] Zob. np. Z. Radwański, *Prawo cywilne – część ogólna*, s. 236; F. Rosengarten, *Podpis...*; S. Grzybowski (w:) *System prawa cywilnego. Część ogólna*, t. I, Ossolineum 1974, s. 327;

wszechnie wyrażanych poglądów przedstawicieli nauki prawa i judykatury podpis własnoręczny jest językowym znakiem graficznym, zawierającym co najmniej nazwisko podpisującego i stanowi na ogół afirmację dokumentu. Podpis własnoręczny uznano za najlepszy gwarant prawdziwości oświadczenia skierowanego do innego podmiotu, gdyż pewne ściśle osobiste cechy zawarte są w charakterze pisma, zatem przez jego grafologiczną ekspertyzę można stwierdzić, czy podpis jest autentyczny. Niemniej jednak w związku z rozwojem technologii pojawia się kilka kluczowych pytań: czy przymiot własnoręczności będzie posiadać podpis złożony za pomocą rysika spełniającego funkcję elektronicznego pióra na interfejsie dotykowym? Czy plik sporządzony na nośniku danych, podpisany podpisem własnoręcznym, zostanie uznany przez sąd w toczącym się postępowaniu cywilnym za dokument, któremu przysługują określone domniemania prawne (zob. art. 244 i art. 245 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[2])? Czy podpis może być nakreślony tylko ręką, czy także inną częścią ciała? Wobec tych wątpliwości należy przyjąć, że kluczowe zagadnienie dla zdefiniowania pojęcia podpisu powinno stanowić określenie jego funkcji, a nie sposobu realizacji, gdyż sama ich realizacja ma już charakter „techniczny". To funkcje przypisywane podpisowi własnoręcznemu pozostają statycznymi, niezmiennymi elementami formy pi-

K. Górska, *Zachowanie zwykłej formy pisemnej czynności prawnej*, Warszawa 2007, s. 104 i n.; J. Kaspryszyn, *Podpis własnoręczny jako element zwykłej formy pisemnej czynności prawnych*, Warszawa 2007; A. Bieliński, *Charakter prawny podpisu w polskim prawie cywilnym materialnym i procesowym*, Warszawa 2007; A. Oleszko, *Podpis własnoręczny jako element formalny aktu notarialnego obejmującego czynność prawną (część pierwsza)*, Rej. 2001, nr 6, s. 30; F. Wejman, *Wprowadzenie do cywilistycznej problematyki ustawy o podpisie elektronicznym*, Pr. Bank. 2002, nr 2, s. 45; J. Gwiazdomorski, *Podpis na testamencie holograficznym*, NP 1962, nr 7–8, s. 943–954; E. Skowrońska, *Jeszcze o podpisie na testamencie holograficznym*, NP 1982, nr 5–6, s. 55–63; F. Rosengarten, *Podpis na testamencie*, NP 1983, nr 3, s. 136–138; A. Szpunar, *Forma podpisu na testamencie własnoręcznym*, Rej. 1993, nr 3–4, s. 9–23; P. Machnikowski, *Weksel własny in blanco*, Warszawa 2002, s. 81; M. Czarnecki, L. Bagińska, *Prawo wekslowe i czekowe. Komentarz*, Warszawa 2005, s. 128 i nast.; A. Kańczuga, *Podpisy na wekslu*, Rej. 1994, nr 5, s. 92; T. Komosa, W. Opalski, *Prawo wekslowe. Prawo czekowe. Komentarz*, Warszawa 1997, s. 26; J. Jacyszyn, A. Wittlin, S. Zakrzewski, *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 r.*, Warszawa 2002, s. 65; F. Rosengarten, *Parafa a podpis*, Pal. 1973, z. 11, s. 70; M. Pazdan, *Statut kontraktowy a język kontraktu*, AUNC 1990, z. 205; M. Pazdan, *Język kontraktu – jego znaczenie i wyznaczenie*, PPHZ 1988, t. 12, s. 35; P. Mostowik, W. Żukowski, *Ustawa o języku polskim. Komentarz*, Warszawa 2001; M. Spyra, *Ustawa o języku polskim – konsekwencje dla obrotu cywilnoprawnego*, TPP 2000, nr 1–2, s. 33; A. Opalski, *Ustawa o języku polskim – zagrożenie dla obrotu prawnego z zagranicą*, M. Praw. 2000, nr 4, s. 227; uchwała SN z dnia 2 października 2002 r., III PZP 17/02, OSNAPiUS 2003, Nr 20, poz. 481, z częściowo aprobującą glosą A. Świątkowskiego i T. Liszcz; postanowienie SN z dnia 17 sierpnia 2000 r., II CKN 894/00, LEX nr 51989; orzeczenie SN z dnia 17 kwietnia 1967 r., II PZ 22/67, NP 1967, nr 12, s. 1720–1722 z glosą J. Krajewskiego; uchwała SN z dnia 28 kwietnia 1973 r., III CZP 78/72, OSN 1973, Nr 12, poz. 207; orzeczenie SN z dnia 3 czerwca 1992 r., OSN 1992, poz. 147; uchwała SN z dnia 30 grudnia 1993 r., III CZP 146/93, OSNC 1994, nr 5, poz. 94; uchwała SN z dnia 23 kwietnia 1960 r., III CO 8/60, OSN 1961, nr 1, poz. 27, uchwała SN z dnia 30 grudnia 1993 r., III CZP 146/93, OSN 1994, Nr 5, poz. 94.

[2] Dz.U. Nr 43, poz. 296 z późn. zm.; dalej: k.p.c.

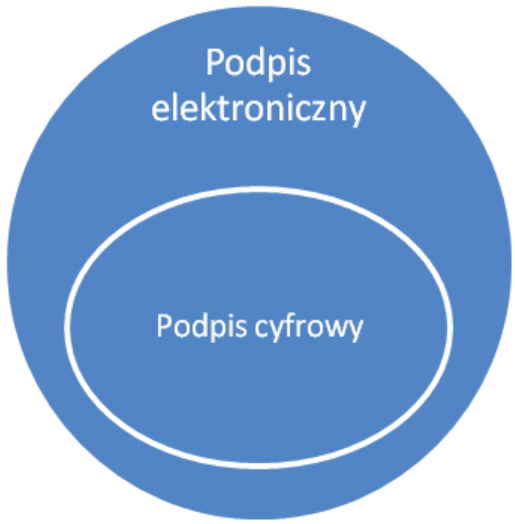
semnej czynności prawnej (zob. art. 78 § 1 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[3]), podczas gdy np. technika składania podpisu jest elementem dynamicznym, ulegającym konsekwentnym zmianom, stale towarzyszącym postępowi cywilizacji. Wątpliwe jest zatem utożsamianie ogólnego pojęcia podpisu jedynie z językowym znakiem graficznym złożonym własnoręcznie.

3. Podpis elektroniczny (*electronic signature*) i podpis cyfrowy (*digital signature*)

Z woli ustawodawcy podpis elektroniczny stanowi odmianę podpisu, chociaż technicznie odległą od tradycyjnego jego skreślania. Podpis elektroniczny obejmuje wiele różnych metod służących identyfikacji. W literaturze można spotkać dwa określenia: podpis elektroniczny i podpis cyfrowy, przy czym są to dwa różne rodzaje podpisów.

Podpis elektroniczny obejmuje wszelkie metody w postaci elektronicznej służące potwierdzeniu tożsamości osoby dokonującej czynności prawnej, np.: PIN-y, hasła dostępu, numery kart kredytowych, zeskanowany podpis własnoręczny, „podpis klawiaturowy" pod e-mailem. Taki podpis elektroniczny nie gwarantuje pewnej identyfikacji osoby z uwagi na łatwość jego „podrobienia", np. „wycięcia" zeskanowanego podpisu własnoręcznego z jednego dokumentu i przeniesienie go na inny dokument.

Rys. 1. Podpis cyfrowy oparty na technikach kryptograficznych jest pojęciem węższym niż podpis elektroniczny, którym może być m.in. zeskanowany podpis własnoręczny.



[3] Dz.U. Nr 16, poz. 93 z późn. zm.; dalej: k.c.

Podpis cyfrowy jest natomiast węższą kategorią podpisu elektronicznego. Oparty jest na zaawansowanych technikach kryptograficznych, które gwarantują autentyczność podpisu cyfrowego, jak i pewne przypisanie go podmiotowi, który taki podpis złożył (cechę tę określa się mianem niezaprzeczalności podpisu cyfrowego). Podpis cyfrowy pełni podobne funkcje do podpisu własnoręcznego. Podpis cyfrowy, jakim opatrywane mogą być dokumenty elektroniczne, powinien być łatwy w użyciu dla jego posiadacza, ale trudny do podrobienia przez inną osobę, a także na trwałe powiązany z podpisywanym dokumentem w taki sposób, aby każda próba modyfikacji treści dokumentu bądź próba przeniesienia podpisu na inny dokument mogła być łatwo wykryta.

Akty prawne, w tym polskie, posługują się – w większości przypadków błędnie – jedynie pojęciem „podpis elektroniczny", ale w istocie skutki prawne nadają podpisowi cyfrowemu i ten właśnie rodzaj podpisu regulują. Wobec tego, że ustawa z dnia 18 września 2001 r. nosi tytuł „o podpisie elektronicznym"[4], w niniejszym skrypcie także będzie używane pojęcie „podpis elektroniczny" zamiast – „podpis cyfrowy". W literaturze prawniczej daje się zauważyć duże niezrozumienie tematyki podpisu elektronicznego, w tym pojęć „podpisywanie", „szyfrowanie", „kodowanie", „identyfikacja", „uwierzytelnienie", „autoryzacja", które zostaną poniżej przedstawione.

Niejednokrotnie dokonywano porównania cech podpisu własnoręcznego i elektronicznego, stawiając temu drugiemu następujące zarzuty: podpis elektroniczny oparty na technikach kryptograficznych nie ma w żadnym razie postaci graficznej ani nie jest elektronicznym zapisem znaku graficznego, wobec tego żaden biegły nie jest w stanie stwierdzić, od kogo pochodzi złożony podpis elektroniczny. Także dokument elektroniczny jest całkowicie pozbawiony charakterystycznych indywidualnych cech powiązanych z osobowością składającego podpis. Zarzuty te są całkowicie nieuzasadnione! Według ustawy o podpisie elektronicznym tożsamość osoby składającej podpis elektroniczny jest ustalana za pomocą certyfikatu służącego do weryfikacji tego podpisu, a nie opinii biegłego, o czym będzie jeszcze mowa.

4. Dokumenty papierowe

Po krótkim porównaniu podpisu własnoręcznego z podpisami elektronicznym i cyfrowym, przyszła pora na przyjrzenie się dokumentom papierowym i elektronicznym.

W ustawodawstwie można znaleźć definicję pojęcia „dokument". Kodeks karny[5] w art. 115 § 14 definiuje dokument jako każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą

---

4 Dz.U. Nr 130, poz. 1450 z późn. zm.

5 Ustawa z dnia 6 czerwca 1997 r., Dz.U. Nr 88, poz. 553 z późn. zm.

w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne. W ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[6] dokumentem jest każda utrwalona informacja niejawna (art. 2 pkt 3). W prawie cywilnym natomiast nie znajdziemy definicji dokumentu, możemy ją zrekonstruować na podstawie wypowiedzi przedstawicieli nauki prawa i orzecznictwa. Przyjmuje się, że dokument musi składać się z trzech elementów: nośnika, którym najczęściej jest papier, oświadczenia woli i podpisu wystawcy. Takie ujęcie odpowiada wąskiej koncepcji dokumentu. Zgodnie z szeroką koncepcją dokumentem może być każdy przedmiot zawierający oświadczenie woli, także taki, na którym nie widnieje podpis wystawcy.

Problemem jest zapewnienie integralności treści dokumentu papierowego, to znaczy cechy, na podstawie której można stwierdzić, czy nie usunięto z dokumentu pewnych fragmentów, nie dodano nowych bądź ich nie zmieniono. Treść dokumentu papierowego, np. umowy o znacznej objętości, podpisanego przez jedną stronę i przedstawionego drugiej stronie do podpisu może istotnie różnić się od treści dokumentu rzeczywiście uzgodnionej przez obie strony. Podpis własnoręczny nie jest zatem gwarantem integralności dokumentu papierowego. Ponadto nieuczciwy kontrahent ma możliwość wydrukowania kolejnych stron do już podpisanego dokumentu i traktowania ich jak autentycznych, czyli pochodzących od obu stron. Dokument papierowy posiada zwykle jeden oryginał (np. akt notarialny, akt stanu urodzenia, wyrok), dzięki czemu często zachodzi konieczność ponoszenia wysokich kosztów związanych z jego fizyczną ochroną, przechowywaniem w bezpiecznym miejscu. Weryfikacja podpisu własnoręcznego złożonego na papierowym dokumencie jest bardzo powierzchowna i opiera się na (irracjonalnym przecież) przekonaniu, że podpis na dokumencie rzeczywiście złożyła ta osoba, która powinna to zrobić.

5. Dokumenty elektroniczne

Elektroniczny obrót prawny rządzi się nieco innymi prawami niż obrót tradycyjny, „papierowy". W transakcjach dokonywanych za pomocą Internetu często ważne jest uwierzytelnienie samego nadawcy dokumentu, czyli pozyskanie informacji o tożsamości jego autora, niekoniecznie powiązane z uwierzytelnieniem treści dokumentu, czyli powiązania między osobą autora dokumentu a treścią dokumentu. Niekiedy treść dokumentu jest weryfikowana przez inne czynności, np. deklaracja dotycząca powinności w zakresie podatku za posiadanie psa może być skutecznie uwierzytelniona przez dokonanie przelewu kwoty podatku z własnego rachunku bankowego. W przypadku obrony przed spamem istnieje konieczność szybkiej weryfikacji nadsyłanych zapytań, podań,

[6] Dz.U. Nr 182, poz. 1228 z późn. zm.

wniosków w celu odfiltrowania niepożądanych treści, bez względu na to, kto jest ich autorem – weryfikacja autora dokumentu nie jest zatem konieczna.

Przechowywanie dokumentów elektronicznych napływających w sekwencji (np. elektronicznych podań do urzędu gminy) pozwala na nadawanie im niefałszowalnych numerów seryjnych. Dzięki takiemu rozwiązaniu uniemożliwione jest generowanie dokumentów z datą wsteczną, posiadających numery seryjne inne niż wynikające z fizycznej kolejności ich powstawania. Dzięki technikom kryptograficznym możliwa jest zatem weryfikacja następstwa, czyli uwierzytelnienie sekwencji wymienianych komunikatów i danych, a także wykrywanie brakujących lub nadmiarowych komunikatów.

Manipulacja zawartością podpisanego cyfrowo dokumentu jest wprawdzie możliwa, ale wykrycie manipulacji jest bardzo proste, tanie i niezawodne. Podpisany dokument elektroniczny może posiadać wiele oryginałów (rozumianych w sensie technologicznym – w świecie elektronicznym nie można bowiem mówić o oryginale i kopii), co umożliwia jego przechowywanie i weryfikację w wielu niezależnych miejscach. Weryfikacja podpisu elektronicznego jest w praktyce jednoznaczna, ale odnosi się tylko do tego, czy do wygenerowania podpisu elektronicznego użyto określonego klucza prywatnego. O kluczach prywatnym i publicznym będzie mowa w dalszej części opracowania.

6. Kryptologia

Jak wspomniano, podpis cyfrowy oparty jest na technikach kryptograficznych, warto więc je pokrótce omówić.

Kryptologię dzieli się na: kryptografię, czyli naukę o układaniu systemów kryptograficznych oraz kryptoanalizę – naukę o ich łamaniu. Współcześnie kryptologia jest uznawana za gałąź zarówno matematyki, jak i informatyki. Kryptologia jest blisko związana z teorią informacji, inżynierią oraz bezpieczeństwem komputerowym. Ma ona szerokie zastosowanie w społeczeństwach rozwiniętych technicznie, wykorzystuje się ją np. w rozwiązaniach zapewniających bezpieczeństwo kart debetowych, haseł komputerowych i handlu elektronicznego.

Nazwa „kryptografia" pochodzi od dwóch greckich słów: *kryptos* oznaczający „ukryty" i *logos* – oznaczający „słowo". Kryptografię można określić jako umiejętność konsekwentnego przekształcenia tekstu pisanego, zrozumiałego dla wszystkich (czyli tekstu jawnego) w tekst szyfrowany (kryptogram, szyfrogram, tekst ukryty), zrozumiały dla odbiorcy, znającego umówiony sposób odczytywania (szyfr, klucz kryptograficzny). Rozwój kryptografii i metod uwierzytelnienia doprowadził do rozszerzenia uwierzytelnienia o posiadany element uwierzytelniania („co masz"), np. token. Konieczność posługiwania się numerem wygenerowanym przez token spotykany jest np. w bankowości elektronicznej. Jeśli osoba trzecia podsłucha hasło, nie będzie mogła wygenerować ko-

lejnego numeru identycznego z tym, który będzie wytworzony przy użyciu naszego tokenu. Jeśli skradnie token, zazwyczaj nie będzie znać hasła. Musiałaby podsłuchać hasło i skraść token, co jest dużo trudniejsze i mniej prawdopodobne. Ostatnio wprowadzane jest zabezpieczenie biometryczne, np. odcisk palca („kim jesteś"), jednak z kryptograficznego punktu widzenia jest to odmiana zabezpieczenia typu „co masz".

Kryptografia nie zajmuje się wyłącznie szyfrowaniem i deszyfrowaniem tekstów. Po pierwsze, dane przekazywane są najczęściej w postaci binarnej (zapisanej za pomocą zer i jedynek), co umożliwia również obróbkę takich danych jak dźwięk czy obraz, a nie tylko danych tekstowych. Po drugie, równie ważne jak zapewnianie poufności danych jest ich: integralność, czyli niezmienność danych w czasie, uwierzytelnianie oznaczające pewność co do ich pochodzenia oraz niezaprzeczalność rozumiana jako fakt, że nadawca nie może wyprzeć się tego, że był nadawcą wiadomości. Ponadto kryptografia znajduje zastosowanie m.in. w: podpisie cyfrowym czy głosowaniu elektronicznym (*e-voting*).

Kryptografia od dawna pozostawała w kręgu zainteresowań służb wywiadowczych i policyjnych, przyciąga też uwagę obrońców praw człowieka, ponieważ jest ona pomocna w utrzymywaniu prywatności, a ewentualne prawne jej ograniczenia wiążą się z umniejszeniem możliwości zachowania prywatności. Można znaleźć we współczesnej historii kontrowersyjne przepisy prawne dotyczące kryptografii, szczególnie od momentu pojawienia się niedrogich komputerów, dzięki którym dostęp do kryptografii na zaawansowanym poziomie stał się powszechny.

Pora na zapoznanie się z kilkoma ważnymi dla kryptografii pojęciami. Tekst jawny oznacza wiadomość przed jej zaszyfrowaniem. Mianem „szyfrowanie" określamy proces zamiany tekstu jawnego na szyfrogram. Szyfr (algorytm kryptograficzny) z kolei oznacza funkcję matematyczną wykorzystywaną do szyfrowania tekstu jawnego lub jego deszyfrowania. Najpopularniejsze standardy szyfrowania opierają się na trudności rozłożenia dużej liczby pierwszej na czynniki pierwsze. Zazwyczaj jedna funkcja wykorzystywana jest do szyfrowania, a inna do deszyfrowania wiadomości. Szyfrogram (kryptogram, tekst ukryty) to wiadomość zaszyfrowana. Deszyfrowanie jest procesem odwrotnym do szyfrowania i oznacza zamianę szyfrogramu na tekst jawny. Wraz z algorytmami dodatkowo używa się kluczy, od których zależy wynik szyfrowania i deszyfrowania. Algorytm z kluczem to taki, w którym do zaszyfrowania oraz odszyfrowania wiadomości wykorzystywane są klucze. Bezpieczeństwo wiadomości oparte jest zatem na kluczu.

Współcześnie wyróżnia się dwa główne nurty kryptografii: kryptografię symetryczną i asymetryczną. W kryptografii symetrycznej nadawca i odbiorca wiadomości używają tego samego klucza do szyfrowania i deszyfrowania (rzadziej: różnych kluczy, ale łatwych do wyliczenia – jeden na podstawie drugiego). Niemniej jednak dla pojedyn-

czych wiadomości bądź ich grup mogą być używane różne klucze. Istotną wadą szyfrów symetrycznych są trudności z przekazywaniem kluczy i ich przechowywaniem, czyli w zarządzaniu kluczami. W przypadku idealnym każda para komunikujących się stron do przekazania każdej wiadomości powinna użyć innego klucza, wobec czego liczba potrzebnych kluczy rosłaby wraz z kwadratem liczby uczestników wymiany informacji. Wobec tego, aby umożliwić wydajną i bezpieczną pracę, szybko pojawi się potrzeba zastosowania złożonych schematów zarządzania kluczami. Zatem konieczność sekretnego przekazania klucza pomiędzy stronami, bez istniejącego wcześniej bezpiecznego kanału komunikacji pomiędzy nimi, stanowiłaby poważną przeszkodę.

Kryptografia asymetryczna z dwoma różnymi kluczami została odkryta dopiero w latach 70. XX w. W 1976 r. Whitfield Diffie i Martin Hellman zaproponowali ideę kryptografii z kluczem publicznym (nazywaną również kryptografią z kluczem asymetrycznym), w której używa się dwóch matematycznie związanych ze sobą kluczy. Jeden z nich nazywany jest kluczem publicznym, drugi – kluczem prywatnym. Klucze to ciągi liczb wzajemnie pierwszych, czyli nie mających innego wspólnego podzielnika niż 1. Obliczenie klucza prywatnego na podstawie klucza publicznego, mimo że możliwe, jest praktycznie niewykonalne. Zamiast tego oba klucze generowane są poufnie jako para. Klucz prywatny w kryptografii asymetrycznej służy do wykonywania zastrzeżonej czynności, którego rozpowszechnienie zagraża bezpieczeństwu systemu, dlatego znany jest jedynie osobie, której został przypisany. Klucz publiczny w kryptografii asymetrycznej umożliwia wykonywanie czynności, do których nie chcemy ograniczać dostępu i który z tego powodu może być dowolnie rozpowszechniany. Należy tylko w sposób bezpieczny udostępnić klucze publiczne i ich uwierzytelnianie.

Do podpisu cyfrowego zastosowanie znalazła także funkcja skrótu. Funkcja skrótu (inaczej: funkcja haszująca) to matematyczna funkcja, która przyporządkowuje dowolnie dużej liczbie (wiadomości) krótką, zwykle posiadającą stały rozmiar wartość (tzw. skrót wiadomości). Jednokierunkowość funkcji *f* oznacza, że dla dowolnych danych wejściowych *x* obliczenie *f(x)* jest łatwo wykonalne (za pomocą standardowego sprzętu obliczeniowego), a dla losowo wybranego y znalezienie jakichkolwiek danych wejściowych, dla których $y = f(x)$, jest praktycznie niewykonalne (przy pomocy hipotetycznie dostępnej technologii i sprzętu obliczeniowego, bez względu na ponoszone koszty). W przypadku funkcji haszujących wartości *f(x)* mają ściśle określoną długość, typowo jest to co najmniej 160 bitów. Jednokierunkowość zastąpiona jest nieco silniejszą własnością bezkonfliktowości, co oznacza, że nie jest praktycznie możliwe znalezienie jakichkolwiek wartości *x* oraz *x'* takich, aby $f(x) = f(x')$.

7. Zastosowania podpisu cyfrowego

Podpis cyfrowy znajduje zastosowanie do szyfrowania wiadomości, podpisywania wiadomości oraz jednoczesnego szyfrowania i podpisywania wiadomości. Jak przebiega podpisywanie wiadomości podpisem elektronicznym? Wymagane jest użycie dwóch algorytmów: jeden służy do podpisywania. Jest nim klucz prywatny autora wiadomości („sekret"), którego używa się do przetwarzania wiadomości, a właściwie wartości funkcji skrótu wiadomości. Drugi klucz (klucz publiczny) służy do weryfikacji, bowiem za pomocą klucza publicznego autora wiadomości sprawdza się, czy podpis elektroniczny pasuje do wiadomości.

W celu wykonania operacji szyfrowania i cyfrowego podpisania wiadomości nadawca kluczem publicznym odbiorcy wiadomości szyfruje ją, a swoim kluczem prywatnym podpisuje ją. Odbiorca natomiast swoim kluczem prywatnym deszyfruje wiadomość, a kluczem publicznym nadawcy sprawdza, czy podpis nadawcy pasuje do wiadomości. Szyfrowanie wiadomości daje pewność co do tego, że wiadomość odebrała osoba, której klucz publiczny został użyty do jej zaszyfrowania oraz pewność co do tego, że nadawcą jest osoba, której klucz publiczny posłużył do jej deszyfrowania. Znajomość algorytmu i szyfrogramu bez dostępu do klucza nie pozwoli na odtworzenie tekstu jawnego.

8. Identyfikacja, uwierzytelnienie i autoryzacja

Podpis elektroniczny spełnia pewne funkcje, stąd konieczne jest zdefiniowanie pewnych pojęć. Definicje pojęć: „uwierzytelnienie" i „autoryzacja" znajdują się w podstawowej normie kryptograficznej: ISO/IEC CD 9798-1, do której odwołują się algorytmy uwierzytelniania i autoryzacji. Dla pełnej jasności wypada także zdefiniować pojęcie „identyfikacji".

Identyfikacja to zadeklarowanie swojej tożsamości przez użytkownika (np. przez podanie loginu). Zadeklarowana (ale jeszcze niezweryfikowana) tożsamość jest potwierdzana w procesie uwierzytelnienia (np. przez podanie hasła). Uwierzytelnianie jest procesem polegającym na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych. Pierwotnie uwierzytelnianie odbywało się w oparciu o tzw. wiedzę uwierzytelniającego się podmiotu (potocznie: „co wiesz"). Wiedzą tą było hasło (np. login i hasło, do tej pory wykorzystywane do logowania się do systemów operacyjnych komputerów i serwisów internetowych). Uwierzytelnianie często ma miejsce przed procesem autoryzacji.

Autoryzacja jest funkcją bezpieczeństwa, która potwierdza, czy dany podmiot jest uprawniony do korzystania z żądanego zasobu (jest to swoista kontrola dostępu). Dla określenia uprawnień danego podmiotu konieczne jest najpierw stwierdzenie jego tożsamości, dlatego w typowym zastosowaniu autoryzacja następuje dopiero po potwierdze-

niu tożsamości podmiotu za pomocą identyfikacji i uwierzytelnienia. Zatem użytkownik bankowości internetowej, który zalogował się na swoje konto za pomocą loginu i hasła (uwierzytelnił) autoryzuje przelew za pomocą podpisu cyfrowego składanego za pomocą hasła jednorazowego.

9. Rozwój regulacji prawnych dotyczących podpisu elektronicznego

W maju 1995 r. w Stanach Zjednoczonych Ameryki Północnej uchwalono pierwszą na świecie ustawę o podpisie elektronicznym. Była nią ustawa o podpisie elektronicznym stanu Utah (*Utah Digital Signature Act*). Rok później Komisja ONZ do spraw Międzynarodowego Prawa Handlowego (UNCITRAL) w art. 7 ustawy modelowej o handlu elektronicznym (*UNCITRAL Model Law on Electronic Commerce*)[7] wspomniała o podpisie elektronicznym. Dnia 5 lipca 2001 r. uchwalono Modelowe prawo o podpisie elektronicznym (*UNCITRAL Model Law on Electronic Signatures)*[8]. Dnia 22 lipca 1997 r. w Niemczech uchwalono pierwsze w Europie przepisy o podpisie elektronicznym (art. 3 ustawy o usługach informacyjnych i komunikacyjnych – *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste, tzw. Multimediagesetz*). Została ona zastąpiona w 2001 r. nową ustawą z powodu niezgodności z dyrektywą Unii Europejskiej dotyczącą podpisów elektronicznych. W 1997 r. we Włoszech uchwalono ustawę o podpisie elektronicznym, w sierpniu 1999 r. – ustawę portugalską, dnia 19 sierpnia 1999 r. –austriacką *Bundesgesetz über elektronische Signaturen*.

9.1. Dyrektywa nr 1999/93/UE

Niezwykle istotnym aktem prawnym jest dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[9], która powinna być zaimplementowana do prawa wewnętrznego państw członkowskich UE do dnia 19 lipca 2001 r.[10] Dyrektywa ta zawiera

---

7 Zob. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (wg stanu na dzień 28 września 2011 r.).

8 Ustawa modelowa o podpisach elektronicznych, przyjęta przez Zgromadzenie Ogólne ONZ w rezolucji 56/80 na XXXIX sesji w grudniu 2001 r. Przekład projektu z 2000 r. wraz z wprowadzeniem J. Gaweł, M. Świerczyński, *Podpis elektroniczny*. *Wprowadzenie*, „Kwartalnik Prawa Prywatnego" 2001, z. 1, s. 208–212.

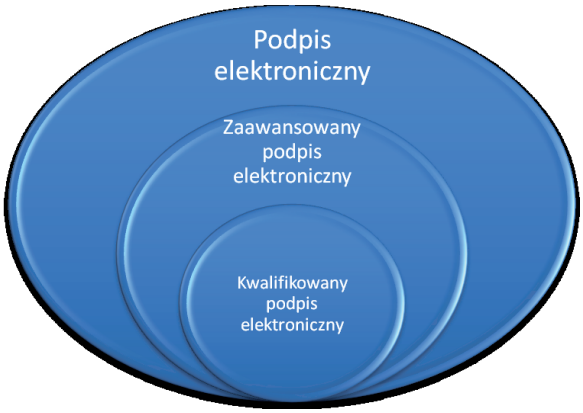
9 Dz.Urz. UE seria L nr 13 z dnia 19 stycznia 2000 r., s. 12.

10 Implementacja to proces wprowadzania dyrektywy do porządków prawnych państw członkowskich. Państwa członkowskie dysponują swobodą w zakresie wyboru formy i środków (w szczególności wyboru organu, formy aktu, procedury prawodawczej), co do wprowadzenia dyrektywy do krajowego systemu prawnego. Dyrektywy wiążą państwa członkowskie w odniesieniu do rezultatu, który ma być osiągnięty. Cel dyrektywy powinien zostać ustalony w wyniku interpretacji wszystkich postanowień dyrektywy, także przy uwzględnieniu jej preambuły. Implementacja najczęściej obejmuje proces stanowienia prawa krajowego,

28 punktów preambuły uzasadniających wydanie dyrektywy, 15 artykułów regulujących m.in. definicje, dostęp do rynku dla podmiotów świadczących usługi certyfikacyjne, skutki prawne podpisów elektronicznych, odpowiedzialność podmiotów świadczących usługi certyfikacyjne, a także 4 załączniki: nr I: „Wymogi dotyczące certyfikatów kwalifikowanych", nr II: „Wymogi wobec podmiotów świadczących usługi certyfikacyjne, wystawiających certyfikaty kwalifikowane", nr III: „Wymogi dotyczące bezpiecznych urządzeń służących do składania podpisu elektronicznego", nr IV: „Zalecenia dotyczące bezpiecznej weryfikacji podpisu".

Celem dyrektywy jest ułatwienie stosowania podpisów elektronicznych oraz przyczynienie się do ich uznania prawnego. Dyrektywa miała stworzyć wspólnotowe ramy dla stosowania podpisu elektronicznego, umożliwiające swobodny, transgraniczny przepływ związanych z nim produktów i usług oraz zapewniających uznawanie jego skuteczności prawnej w podstawowym zakresie. W jej treści stwierdzono, że „*należy zapewnić, aby zaawansowane podpisy elektroniczne opierające się na kwalifikowanym certyfikacie i które zostały wygenerowane za pomocą bezpiecznych urządzeń spełniały w odniesieniu do danych istniejących w postaci elektronicznej wymóg prawny podpisu w taki sam sposób, jak podpisy odręczne spełniają ten wymóg w odniesieniu do danych istniejących na papierze oraz by były dopuszczalne jako dowód w postępowaniu sądowym*". Według pkt 8 preambuły do dyrektywy, szybki rozwój technologiczny i globalny charakter Internetu wymagają podejścia, które uwzględnia różne technologie i usługi pozwalające na uwierzytelnianie danych drogą elektroniczną.

Dyrektywa wyróżnia trzy rodzaje podpisów elektronicznych, przedstawione na poniższym rysunku:



tj. transpozycję w postaci działalności legislacyjnej. Samo uzgodnienie tekstu przepisów z wzorcem wspólnotowym nie wypełni przesłanek prawidłowej implementacji, jeżeli praktyka ich stosowania nie będzie prowadziła do osiągania zamierzonych przez dyrektywę celów. Dlatego też szersze rozumienie „realizowania" prawa wspólnotowego (procesu implementacji) obejmuje także etap stosowania (przestrzegania) aktów implementacyjnych przez sądy i inne organy państw członkowskich. Implementacja dyrektyw prowadzi do harmonizacji prawa państw członkowskich.

Zostały one wyróżnione z uwagi na różnice w poziomie bezpieczeństwa, różnice w zastosowanej technice oraz skutki prawne.

Zgodnie z dyrektywą podpis elektroniczny to dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia. Definicję tą wypełniają m.in. PIN, zeskanowany podpis odręczny, napisanie na końcu e-maila imienia i nazwiska („podpis klawiaturowy").

Zaawansowanym podpisem elektronicznym według dyrektywy jest podpis elektroniczny spełniający następujące wymogi: przyporządkowany jest wyłącznie podpisującemu, umożliwia ustalenie tożsamości podpisującego, stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą i jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna. Dyrektywa nie preferuje żadnej technologii wytwarzania podpisu elektronicznego, ale w praktyce definicja ta dotyczy głownie podpisów elektronicznych opartych na infrastrukturze klucza publicznego, o której dalej. Obecna technologia umożliwia stwierdzenie, że dokument elektroniczny został zmieniony, ale nie wskazuje, jaka konkretnie treść dokumentu została zmieniona. Jest to cecha zwana integralnością dokumentu elektronicznego.

Kwalifikowany podpis elektroniczny, zgodnie z dyrektywą, to zaawansowany podpis elektroniczny oparty o kwalifikowany certyfikat i złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu.

10. Ustawa o podpisie elektronicznym

10.1. Zakres zastosowania

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi. Przepisy ustawy stosuje się do podmiotów świadczących usługi certyfikacyjne, mających siedzibę lub świadczących usługi na terytorium Rzeczypospolitej Polskiej. Ustawa o podpisie elektronicznym definiuje usługi certyfikacyjne, którymi są: wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym.

10.2. Podmioty świadczące usługi certyfikacyjne

Usługi certyfikacyjne mogą być świadczone tylko przez przedsiębiorcę w rozumieniu przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[11], Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną

[11] Dz.U. z 2007 r. Nr 155, poz. 1095, z późn. zm.

z usług, o których mowa w art. 3 pkt 13 ustawy. Natomiast kwalifikowany podmiot świadczący usługi certyfikacyjne to podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Schemat wydawania podpisów elektronicznych w Polsce jest oparty na infrastrukturze klucza publicznego – *PKI* (ang. *Public Key Infrastructure)*. PKI to szeroko pojęty kryptosystem, w skład którego wchodzą urzędy certyfikacyjne, urzędy rejestracyjne, subskrybenci certyfikatów (odbiorcy usług certyfikacyjnych), oprogramowanie i sprzęt. Do podstawowych funkcji infrastruktury klucza publicznego należą: generowanie kluczy kryptograficznych, weryfikacja tożsamości subskrybentów, wystawianie certyfikatów, weryfikacja certyfikatów, podpisywanie wiadomości, szyfrowanie wiadomości, potwierdzanie tożsamości i znakowanie czasem. Kluczowym elementem infrastruktury klucza publicznego jest urząd certyfikacji, który pełni rolę zaufanej trzeciej strony w stosunku do wystawców i użytkowników certyfikatów. W Polsce instytucją certyfikującą pozostałych wystawców certyfikatów jest Narodowe Centrum Certyfikacji (zob. https://www.nccert.pl/).

Prowadzenie działalności w zakresie świadczenia usług certyfikacyjnych nie wymaga uzyskania zezwolenia ani koncesji. Organy władzy publicznej i Narodowy Bank Polski mogą świadczyć usługi certyfikacyjne wyłącznie na użytek własny lub innych organów władzy publicznej. Jednostka samorządu terytorialnego może świadczyć usługi certyfikacyjne na zasadach niezarobkowych także dla członków wspólnoty samorządowej.

Podmiot świadczący usługi certyfikacyjne lub zamierzający podjąć taką działalność może wystąpić o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Świadczenie usług certyfikacyjnych w charakterze kwalifikowanego podmiotu świadczącego usługi certyfikacyjne wymaga uzyskania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne i uzyskania zaświadczenia certyfikacyjnego wykorzystywanego do weryfikowania poświadczeń elektronicznych tego podmiotu, wydanego przez ministra właściwego do spraw gospodarki. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne prowadzi minister właściwy do spraw gospodarki. Rejestr jest jawny i publicznie dostępny, w tym również w formie elektronicznej.

Podmioty świadczące usługi certyfikacyjne są obowiązane do stosowania polityki certyfikacji, czyli szczegółowych rozwiązań, w tym technicznych i organizacyjnych, wskazujących sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów. Polityka certyfikacji obejmuje w szczególności: 1) zakres jej zastosowania, 2) opis sposobu tworzenia i przesyłania danych elektronicznych, które zostaną opatrzone poświadczeniami elektronicznymi przez podmiot świadczący usługi certyfikacyjne, 3) maksymalne okresy ważności certyfikatów, 4) sposób identyfikacji i uwierzytelnienia

osób, którym wydawane są certyfikaty, i podmiotu świadczącego usługi certyfikacyjne, 5) metody i tryb tworzenia oraz udostępniania certyfikatów, list unieważnionych i zawieszonych certyfikatów oraz innych poświadczonych elektronicznie danych, 6) opis elektronicznego zapisu struktur danych zawartych w certyfikatach i innych danych poświadczanych elektronicznie, 7) sposób zarządzania dokumentami związanymi ze świadczeniem usług certyfikacyjnych.

10.3. Rodzaje podpisów elektronicznych

Ustawa *de facto* wyróżnia tylko dwa rodzaje podpisów elektronicznych: podpis elektroniczny oraz bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu.

Podpisem elektronicznym w rozumieniu ustawy są 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.

Bezpieczny podpis elektroniczny to podpis elektroniczny, który: jest przyporządkowany wyłącznie do osoby składającej ten podpis, 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 i jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Ustawa o podpisie elektronicznym nie reguluje zaawansowanego podpisu elektronicznego, który normuje dyrektywa. Zamiar polskiego ustawodawcy był taki, by bezpieczny podpis elektroniczny stanowił odpowiednik podpisu zaawansowanego. Jednakże w ustawie w zupełnie nieuzasadniony sposób rozszerzono definicję funkcjonalną zaawansowanego podpisu elektronicznego, uzupełniając ją o warunek zrealizowania funkcji podpisu za pomocą bezpiecznego urządzenia. Według dyrektywy zaawansowany podpis elektroniczny może zostać złożony przy użyciu bezpiecznego urządzenia lub oprogramowania, a nie tylko i wyłącznie przy jednoczesnym użyciu tych dwóch elementów, jak nakazuje polska ustawa. Żadne urządzenie weryfikujące nie może sprawdzić, czy podpis został złożony przy użyciu bezpiecznego urządzenia, gdyż w sensie funkcjonalnym może rozpoznać jedynie zaawansowany podpis elektroniczny. Nie ma równoważności między pojęciami „zaawansowany podpis elektroniczny" i „bezpieczny podpis elektroniczny".

10.4. Inne zdefiniowane pojęcia

Osobą składającą podpis elektroniczny jest jedynie osoba fizyczna posiadająca urządzenie służące do składania podpisu elektronicznego, która działa w imieniu wła-

snym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej. Jak widać, osoby prawne i inne jednostki organizacyjne nie mogą mieć swojego podpisu elektronicznego – mają je osoby fizyczne będące piastunami ich organów. Dlatego w literaturze przedmiotu zgłaszana jest potrzeba wprowadzenia pieczęci elektronicznej, którą mogłyby dysponować jednostki nie będące osobami fizycznymi. Takie rozwiązanie niewątpliwie ułatwiłoby np. automatyczne wystawianie dużej ilości faktur elektronicznych. Zgodnie z rozporządzeniem Ministra Finansów z dnia 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej[12] autentyczność pochodzenia i integralność treści faktury są zachowane, w szczególności, w przypadku wykorzystania bezpiecznego podpisu elektronicznego w rozumieniu art. 3 pkt 2 ustawy o podpisie elektronicznym, weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu.

Skoro tak skonstruowano pojęcie osoby składającej podpis elektroniczny, odbiorcą usług certyfikacyjnych jest więc tylko osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych lub w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne.

Kluczem prywatnym zostały nazwane w ustawie dane służące do składania podpisu elektronicznego (tzw. klucz prywatny)[13]. Są nimi niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego. Kluczem publicznym, czyli danymi służącymi do weryfikacji podpisu elektronicznego[14], są niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane do identyfikacji osoby składającej podpis elektroniczny.

Warto przytoczyć także definicję bezpiecznego urządzenia służącego do składania podpisu elektronicznego z uwagi na skutki prawne bezpiecznego podpisu elektronicznego. Jest nim urządzenie służące do składania podpisu elektronicznego, spełniające wymagania określone w ustawie. Jak już wspomniano na początku rozdziału, do weryfikacji podpisu elektronicznego służy także certyfikat, czyli elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej

---

12 Dz.U. Nr 249, poz. 1661.

13 Nie należy mylić z kluczem służącym do szyfrowania wiadomości! O szyfrowaniu była mowa wcześniej.

14 Nie należy mylić z kluczem służącym do deszyfrowania wiadomości! O deszyfrowaniu była mowa wcześniej.

osoby. „Odmianą" certyfikatu jest kwalifikowany certyfikat, a więc certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie.

Weryfikacja bezpiecznego podpisu elektronicznego to czynności, które pozwalają na identyfikację osoby składającej podpis elektroniczny oraz pozwalają stwierdzić, że podpis został złożony za pomocą danych służących do składania podpisu elektronicznego przyporządkowanych do tej osoby, a także że dane opatrzone tym podpisem nie uległy zmianie po złożeniu podpisu elektronicznego.

Podmiot świadczący usługi certyfikacyjne wydaje certyfikat na podstawie umowy. Umowa o świadczenie usług certyfikacyjnych powinna być sporządzona w formie pisemnej pod rygorem nieważności. Nieważność umowy o świadczenie usług certyfikacyjnych nie powoduje nieważności certyfikatu, jeżeli przy jego wydaniu zostały spełnione wymogi określone w art. 14 ust. 2 i 5 oraz uzyskano zgodę, o której mowa w art. 14 ust. 7 ustawy. Podmiot świadczący usługi certyfikacyjne przed jej zawarciem jest obowiązany poinformować na piśmie lub w formie dokumentu elektronicznego w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[15], w sposób jasny i powszechnie zrozumiały, o dokładnych warunkach użycia tego certyfikatu, w tym o sposobie rozpatrywania skarg i sporów, a w szczególności o istotnych jego warunkach obejmujących: zakres i ograniczenia jego stosowania, skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu, informację o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i ich znaczeniu. W przypadku wydawania certyfikatów niebędących certyfikatami kwalifikowanymi, informacja powinna również zawierać wskazanie, że podpis elektroniczny weryfikowany przy pomocy tego certyfikatu nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu. Podmiot świadczący usługi certyfikacyjne jest obowiązany uzyskać pisemne potwierdzenie zapoznania się z tą informacją przed zawarciem umowy.

Podmiot świadczący usługi certyfikacyjne może korzystać z notarialnego potwierdzenia tożsamości odbiorców usług certyfikacyjnych, jeżeli przewiduje to określona polityka certyfikacji.

Kwalifikowany certyfikat zawiera co najmniej następujące dane: numer certyfikatu, wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji, określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę, oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, imię

[15] Dz.U. Nr 64, poz. 565 z późn. zm.

i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone, dane służące do weryfikacji podpisu elektronicznego, oznaczenie początku i końca okresu ważności certyfikatu, poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat, ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji, ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa.

Podmiot świadczący usługi certyfikacyjne, wydając kwalifikowany certyfikat, jest obowiązany zawrzeć w tym certyfikacie inne dane niż wymienione powyżej na wniosek osoby składającej podpis elektroniczny, a w szczególności wskazanie, czy osoba ta działa: we własnym imieniu albo jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo w charakterze członka organu lub organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo jako organ władzy publicznej.

Podmiot świadczący usługi certyfikacyjne, wydając kwalifikowany certyfikat, potwierdza prawdziwość danych i powiadamia podmioty o treści certyfikatu oraz poucza o możliwości unieważnienia certyfikatu na ich wniosek. Certyfikat jest ważny w okresie w nim wskazanym. W przypadkach określonych w ustawie o podpisie elektronicznym podmiot świadczący usługi certyfikacyjne unieważnia certyfikat kwalifikowany przed upływem okresu jego ważności. Unieważnienie certyfikatu nie wyłącza odpowiedzialności podmiotu świadczącego usługi certyfikacyjne za szkodę względem osoby składającej podpis elektroniczny.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, podmiot świadczący usługi certyfikacyjne jest obowiązany niezwłocznie zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości. Zawieszenie kwalifikowanego certyfikatu nie może trwać dłużej niż 7 dni. Po ich upływie, w przypadku niemożności wyjaśnienia wątpliwości, podmiot świadczący usługi certyfikacyjne niezwłocznie unieważnia kwalifikowany certyfikat. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub jego zawieszenie może zostać uchylone. Certyfikat, który został unieważniony, nie może być następnie uznany za ważny. O unieważnieniu lub zawieszeniu certyfikatu podmiot świadczący usługi certyfikacyjne zawiadamia niezwłocznie osobę składającą podpis elektroniczny weryfikowany na jego podstawie. Zawieszenie lub unieważnienie certyfikatu nie może następować z mocą wsteczną.

Podmiot świadczący usługi certyfikacyjne publikuje listę zawieszonych i unieważnionych certyfikatów. Informacje o zawieszeniu lub unieważnieniu certyfikatu umieszcza się na każdej liście zawieszonych i unieważnionych certyfikatów publikowanej

przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu. Lista zawieszonych i unieważnionych kwalifikowanych certyfikatów powinna zawierać w szczególności: 1) numer kolejny listy i wskazanie, że lista została opublikowana zgodnie z określoną polityką certyfikacji i dotyczy certyfikatów wydanych zgodnie z tą polityką, 2) datę i czas opublikowania listy z dokładnością określoną w polityce certyfikacji, 3) datę przewidywanego opublikowania kolejnej listy, 4) określenie podmiotu świadczącego usługi certyfikacyjne wydającego listę i państwa, w którym ma on siedzibę, oraz numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, 5) numer każdego zawieszonego lub unieważnionego certyfikatu oraz wskazanie, czy został on unieważniony, czy zawieszony, 6) datę i czas, z dokładnością określoną w polityce certyfikacji, zawieszenia lub unieważnienia każdego certyfikatu, 7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, publikującego listę.

Podmiot świadczący usługi certyfikacyjne publikuje informacje o zawieszeniu i unieważnieniu certyfikatu na liście zgodnie z odpowiednią polityką certyfikacji, jednak nie później niż w ciągu 1 godziny od unieważnienia lub zawieszenia certyfikatu. Zawieszenie i unieważnienie certyfikatu wywołuje skutki prawne od momentu, o którym mowa w ust. 3 pkt 6, który nie może być wcześniejszy niż data i czas publikacji poprzedniej listy zawieszonych i unieważnionych certyfikatów.

10.5. Skutki prawne podpisu elektronicznego

Jak wykazano na początku niniejszego rozdziału, podpis elektroniczny ma zastępować podpis własnoręczny w transakcjach zawieranych na odległość, muszą mu więc być przydane skutki prawne. Zgodnie z ustawą o podpisie elektronicznym bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu (art. 5 ust. 1 zd. 1). Z brzmienia tego przepisu wynika, że skutki prawne bezpiecznego podpisu elektronicznego utrzymują się również po utracie ważności przez kwalifikowany certyfikat służący do jego weryfikacji (wskutek upływu czasu, na jaki został wydany bądź jego unieważnienia). Jednakże przepis art. 5 ust. 2 przeczy temu założeniu, stanowi bowiem, że 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 (art. 5 ust. 2). Przyjęte rozwiązanie wymaga, by podpis elektroniczny każdorazowo był weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu. Certyfikaty mają prawnie ograniczony okres ważności, który wynosi maksymalnie 2 lata. Przepis ten ma ogromne znaczenie

dla długoterminowego przechowywania dokumentów elektronicznych, w tym opatrzonych podpisami elektronicznymi weryfikowanymi za pomocą kwalifikowanych certyfikatów.

Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu zapewnia integralność danych opatrzonych tym podpisem i jednoznaczne wskazanie kwalifikowanego certyfikatu w ten sposób, że rozpoznawalne są wszelkie zmiany tych danych oraz zmiany wskazania kwalifikowanego certyfikatu wykorzystywanego do weryfikacji tego podpisu, dokonane po złożeniu podpisu.

Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny. Przepis ten nie odnosi się do certyfikatu po upływie terminu jego ważności lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem.

Nie można powoływać się na fakt, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

Bezpieczny podpis elektroniczny złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia (art. 5 ust. 1 zd. 2). Przepis ten jest krytykowany, bowiem skutki prawne podpisu elektronicznego powinny być przywracane od momentu zawieszenia certyfikatu.

Podpis elektroniczny może być znakowany czasem. Polega 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. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego[16]. Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę.

---

[16] Zob. art. 81 k.c.

Po szeregu przepisów określających skutki prawne bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu ustawodawca umieścił jeden, stanowiący o tzw. zwykłym podpisie elektronicznym. Zgodnie z art. 8 ustawy o podpisie elektronicznym 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.

Tymczasem brak szczególnych przepisów proceduralnych, chociażby w Kodeksie postępowania cywilnego, które uznawałyby np. pliki opatrzone bezpiecznym podpisem elektronicznym za pomocą ważnego kwalifikowanego certyfikatu lub niepodpisane e- maile za dokumenty (prywatne lub urzędowe).