Rejent * rok 16 * nr 5(181)
maj 2006 r.

*Jacek Przetocki*

# Wykorzystanie środków przekazu elektronicznego, między innymi e-podpisu w praktyce notarialnej

## I. Wprowadzenie

Komputer stał się powszechnym i podstawowym narzędziem pracy każdego z nas. W połączeniu z Internetem uzyskujemy niemal nieograniczone możliwości komunikowania się i przekazywania drogą elektroniczną informacji na odległość w stosunkowo krótkim czasie w dowolne miejsce na Ziemi. Rozwój technik kryptograficznych (kryptografia – nauka o metodach przesyłania informacji w zakamuflowanej postaci) pozwala na przekazywanie tych informacji w sposób bezpieczny, czyli taki, który zapewnia im integralność (możliwość sprawdzenia, czy przesłane informacje nie zostały zmodyfikowane podczas transmisji), uwierzytelnianie (możliwość sprawdzenia, czy nadawca informacji jest tym, za kogo się podaje) i niezaprzeczalność (zabezpieczenie przed możliwością wyparcia się przez nadawcę faktu wysłania informacji). Wprowadzenie do porządku prawnego w większości państw rozwiniętych, w tym również Polski, instytucji podpisu elektronicznego pozwala na nadanie praktycznym informacjom rangi dokumentu elektronicznego, mającego indywidualne cechy pochodzące od autora, możliwe do weryfikacji przez odbiorcę tego dokumentu, który ze względu na sposób powstania i sposób jego podpisania nazywamy dokumentem elektronicznym. Nic więc dziwnego, że technologia ta stwarza nowe możliwości dla notariuszy i notariatu jako całości. Od tego, jak szybko notariat podąży za nowymi technikami

tworzenia, przesyłania i gromadzenia dokumentów zależy jego pozycja i wiarygodność w nadchodzącej elektronicznej przyszłości.

Podpis elektroniczny staje się częścią naszej rzeczywistości, a dokumenty elektroniczne w coraz większym stopniu zastępują dokumenty tradycyjne. Przesyłanie drogą elektroniczną dokumentów przy zastosowaniu podpisu elektronicznego coraz częściej staje się wymogiem ustawowym, a nie tylko możliwością ułatwiającą pracę. Powszechność tej drogi przysyłania informacji wydaje się przesądzona (deklaracje ZUS, zeznania podatkowe, inne). Notariusze zostali zobligowani do przysyłania informacji Głównemu Inspektorowi Informacji Finansowej (GIIF) drogą elektroniczną, z zastosowaniem e-podpisu. Należy się spodziewać, że w taki sposób będą w niedługim czasie przesyłać większość informacji, do przekazania których są zobowiązani. Obowiązek przesyłania informacji do GIIF przyczynił się do upowszechnienia e-podpisu. Jako notariusze mamy więc za sobą pierwsze kroki w dziedzinie przekazywania w sposób bezpieczny informacji drogą elektroniczną, czyli potrafimy się posługiwać e-podpisem. Zakres jego zastosowania w notariacie będzie stale zwiększał się, natomiast od nas samych zależy, jakie dziedziny notarialnej działalności zostaną opanowane przez elektroniczną rzeczywistość.

## II. Podpis elektroniczny

Podpis elektroniczny jest to sposób podpisania dokumentu w postaci elektronicznej, ściślej – każdy sposób zastąpienia własnoręcznego podpisu podpisem w nośniku elektronicznym. Według Dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej Nr 1999/93/WE z dnia 13 grudnia 1999 r. podpisy elektroniczne to „informacje w postaci elektronicznej, dołączone, lub w logiczny sposób związane z innymi informacjami w postaci elektronicznej i które służą do ich poświadczenia" (*data in electronic form which are attached to or logically associated with other electronic data and which serve as a metod of authentication)*. W tym sensie podpisem elektronicznym jest na przykład obraz podpisu własnoręcznego otrzymany przy pomocy skanera, podpis sporządzony elektronicznym piórem, kod PIN karty elektronicznej użyty do podjęcia pieniędzy z bankomatu czy też imię lub nazwisko umieszczone w zakończeniu wiadomości wysłanej pocztą elektroniczną lub przy użyciu facsimilie (ogólniej w każdej postaci, w której dokument powstał lub został przetworzony na strumień

logicznie powiązanych bitów informacji, przechowywanych i przesyłanych jako impulsy elektryczne, pola magnetyczne, strumień fotonów itp.). Jest to pewna szczególna forma podpisu elektronicznego.

Oczywiście taki podpis, łatwy do podrobienia, nie posiadając żadnych (poza samą treścią) szczególnych cech pozwalających w sposób niebudzący wątpliwości przypisać go określonej osobie czy dokumentowi, jest w wielu sytuacjach niezadowalający. Znacznie bardziej użyteczna jest inna forma podpisu elektronicznego, często określana mianem zaawansowanego podpisu elektronicznego czy podpisu cyfrowego (*advanced electronic signature, digital signature*). Wówczas przy użyciu technik kryptograficznych (czasami także i innych środków technicznych wykorzystujących szczególną wiedzę, posiadane urządzenie lub specyficzne biologiczne cechy osobnicze osoby składającej podpis) z oryginalnego dokumentu elektronicznego i innych informacji dostarczonych przez osobę składająca podpis (w formie hasła, tajnego klucza, informacji pochodzących z udostępnionego do złożenia podpisu urządzenia, udostępnionych cech biometrycznych) utworzony jest specjalny zbiór informacji – podpis cyfrowy (zwykle jest to po prostu bardzo duża liczba), który w sposób unikalny i jednoznaczny wiąże treść podpisanego dokumentu elektronicznego z informacjami pochodzącymi od osoby podpisującej. Przyjmuje się, że przy obecnym stanie wiedzy nie jest możliwe (nawet przy użyciu zaawansowanych środków technicznych i potężnych mocy obliczeniowych) wytworzenie takiego podpisu bez znajomości oryginalnego dokumentu oraz bez szczególnej wiedzy czy też szczególnych cech osoby składającej podpis. Zwykle weryfikacja takiego podpisu, czyli ustalenie autora oraz stwierdzenie, że dokument nie został zmieniony po podpisaniu, jest możliwa już bez udziału osoby podpisującej. Jedna z najpowszechniej dotychczas używanych technik podpisu cyfrowego oparta jest na kryptografii asymetrycznej. Algorytm podpisu elektronicznego przy jej użyciu przedstawiony jest w pamięci komputera w postaci bardzo dużej liczby (ciągu zer i jedynek). Należy dodać, że można tak przedstawić każdy dokument w postaci elektronicznej, np. dokument tekstowy, utwór muzyczny, wizerunek, film, dane telemetryczne, obraz telewizyjny itp. Liczbie tej zostaje przy pomocy powszechnie znanego algorytmu, nazywanego funkcją skrótu, przyporządkowana inna, na ogół znacznie krótsza liczba (zwykle 40-50 cyfrowa), tzw. etykietka oryginalnego dokumentu. Szczególne

własności kryptograficznej funkcji skrótu zapewniają, że dokumenty różniące się nawet tylko jednym bitem informacji będą miały różne etykietki oraz że nie jest możliwe znalezienie dwóch dokumentów o takiej samej etykietce. Nie jest także możliwe skonstruowanie dokumentu o zadanej etykietce. W tym sensie funkcja skrótu umożliwia „ponumerowanie" lub nadanie znormalizowanych unikalnych etykietek wszystkim możliwym dokumentom elektronicznym. Drugim, obok funkcji skrótu, elementem algorytmu podpisu cyfrowego (w tej konkretnej postaci) jest algorytm szyfru asymetrycznego. Osoba podpisująca wytwarza (przy użyciu komputera lub innych środków technicznych) za pomocą określonej procedury dwie liczby powiązane ze sobą szczególnymi własnościami matematycznymi. Jedna z nich pozostaje tajemnicą właściciela, druga zostaje upowszechniona. Ta pierwsza to klucz prywatny właściciela podpisu elektronicznego, który służy do podpisywania dokumentów elektronicznych, ta druga to klucz publiczny, który służy (wraz z innymi jawnymi informacjami o użytym algorytmie) do weryfikacji podpisu. Następnie podpisujący przy użyciu powszechnie znanego algorytmu szyfru asymetrycznego (szyfr jest asymetryczny, bowiem różne klucze służą do szyfrowania i do odszyfrowania, w odróżnieniu od szyfrów symetrycznych, gdzie ten sam klucz służy do obu operacji) szyfruje etykietkę swojego dokumentu, obliczoną uprzednio przy pomocy funkcji skrótu, używając swego tajnego klucza. Jak zawsze, wszystkie te operacje wykonuje komputer – na biurku, w karcie elektronicznej, w telefonie komórkowym. Zależnie od praktycznej realizacji takiego podpisu, klucz prywatny może być przechowywany w pamięci komputera (nie jest to bezpieczne rozwiązanie), zakodowany w karcie elektronicznej, na dyskietce, płycie CD czy wpisywany z klawiatury. Wynik procesu szyfrowania – zaszyfrowana etykietka (jest to znów liczba o długości kilkudziesięciu, kilkuset cyfr), to podpis cyfrowy dokumentu. Podpis taki jest dołączany następnie do dokumentu oryginalnego i całość wysyłana do adresata (oczywiście podpis może być też przesłany czy przechowany oddzielnie, bowiem podpis cyfrowy dla każdego dokumentu jest inny). Weryfikacja autentyczności podpisu i integralności dokumentu przebiega następująco: odbiorca po otrzymaniu dokumentu oddziela podpis i dla samego dokumentu oblicza znów przy użyciu tej samej, ogólnie znanej funkcji skrótu etykietkę dokumentu. Następnie, używając powszechnie dostępnego klucza jaw-

nego autora dokumentu, przy użyciu ogólnie znanego algorytmu deszyfrującego deszyfruje podpis. Jeżeli etykietka dokumentu obliczona przez odbiorcę jest identyczna z etykietką otrzymaną po odszyfrowaniu przez niego podpisu cyfrowego, to odbiorca może z prawdopodobieństwem graniczącym z pewnością przyjąć, że dokument, który otrzymał, został podpisany kluczem prywatnym, tworzącym unikalną parę z użytym przez niego do weryfikacji podpisu kluczem publicznym oraz że dokument ten jest identyczny z dokumentem, który został podpisany. Ponadto, dysponując dokumentem, kluczem publicznym i podpisem cyfrowym może tę weryfikację powtórzyć dowolną ilość razy (na przykład na potrzeby postępowania dowodowego). Weryfikacja podpisu kończy algorytm podpisu cyfrowego przy użyciu kryptografii asymetrycznej. Istnieją liczne odmiany podpisy cyfrowego, np. zwykły – jak powyżej, ślepy – osoba podpisująca nie musi znać treści podpisanego dokumentu, niezaprzeczalny – weryfikacja podpisu wymaga współpracy osoby podpisanej oraz szereg innych. Należy zauważyć, że samo określenie zastosowania asymetrycznej kryptografii do celów uwierzytelnienia i potwierdzenia integralności elektronicznego dokumentu mianem podpisu jest dość niefortunne, bowiem z matematycznego punktu widzenia poprawna weryfikacja podpisu elektronicznego przy założeniu, że klucze prywatny i publiczny zostały wytworzone z zachowaniem pewnych – dość łatwych do sprawdzenia – warunków, pozwala jedynie stwierdzić, że pewien proces (komputer realizujący algorytm podpisu) miał w pewnym momencie dostęp zarówno do oryginalnego dokumentu, jak i do tajnego klucza (komplementarnego) użytego do weryfikacji klucza publicznego. Algorytm taki nie pozwala jeszcze stwierdzić, czy z tym procesem wiąże się jakakolwiek forma wyrażenia woli oraz związek kluczy (prywatnego i publicznego) z konkretną osoba fizyczną. Nie jest to więc podpis w prawnym znaczeniu tego słowa. Aby go osiągnąć, potrzebne jest przyjęcie szeregu dodatkowych założeń, między innymi ustalenie związku pomiędzy intencjami podpisującego a faktem użycia odpowiedniej techniki kryptograficznej oraz stworzenie mechanizmu jednoznacznego przypisania kluczy (lub innych szczególnie określonych unikalnych cech czy informacji) do konkretnej osoby fizycznej. Innymi słowy, potrzebne jest zbudowanie odpowiedniej infrastruktury zaufania i bezpieczeństwa. Jedną z jej możliwych form jest

tzw. Infrastruktura Klucza Publicznego (PKI), nazywana także siecią Urzędów Certyfikatów, Zaufaną Trzecią Stroną lub podobnie.

Infrastruktura Klucza Publicznego (*Public Key Infrastructure)* służy do jednoznacznego przypisania klucza publicznego używanego do weryfikacji podpisu elektronicznego (pozostając przy realizacji podpisu elektronicznego przy użyciu kryptografii asymetrycznej) konkretnej osobie fizycznej. W tym celu posługuje się ich certyfikatami. Certyfikat to dokument elektroniczny zawierający dany klucz publiczny, informacje o tożsamości jego właściciela oraz informacje dodatkowe (o okresie ważności certyfikatu, identyfikujące instytucję, która certyfikat wystawiła, ewentualne ograniczenia jego stosowania itp.), podpisany elektronicznie podpisem cyfrowym przez instytucję lub osobę zaufania publicznego. Przyjmuje się, że klucz publiczny wystawcy certyfikatów, umożliwiający sprawdzenie ważności certyfikatu, jest powszechnie dostępny, co umożliwia każdemu i zawsze sprawdzenie, czy konkretny klucz publiczny jest zaopatrzony w ważny certyfikat, a zatem czy podpis elektroniczny opatrzony ważnym certyfikatem rzeczywiście jest przypisany do autora dokumentu elektronicznego. Sposób wystawiania certyfikatów – „polityka certyfikacji", wiarygodność i rzetelność procedury przypisania konkretnych kluczy do konkretnych osób fizycznych oraz bezpieczeństwo używanych technik identyfikacji i kryptograficznych decydują o zaufaniu do instytucji podpisu elektronicznego, dlatego też we wszystkich regulacjach prawnych wprowadzających podpis elektroniczny wiele uwagi poświęca się zasadom funkcjonowania oraz odpowiedzialności Urzędów Certyfikatów za wystawione certyfikaty podpisów cyfrowych.

## III. Podpis elektroniczny w pracy notariusza

Obecnie nie ma chyba notariusza, który by w swojej pracy zawodowej nie korzystał z jakiejś formy podpisu elektronicznego. Różnice powstałe pomiędzy notariatami poszczególnych krajów, a także pomiędzy samymi notariuszami, dotyczą jedynie zakresu jego stosowania. W pracy każdego notariusza zauważalne są dwie sfery funkcjonowania elektronicznego podpisu.

Pierwsza sfera nie jest ściśle związana z dokonywaniem czynności notarialnych, dotyczy wykorzystywania podpisu elektronicznego przy prowadzeniu różnego rodzaju rejestrów, przesyłaniu informacji, wzajem-

nym komunikowaniu się czy też gromadzeniu danych i tworzeniu baz danych w dziedzinach, którymi notariat jest żywo zainteresowany. W grupie tej elektroniczny podpis niewątpliwie usprawnia pracę, przyśpiesza ją i uatrakcyjnia przez możliwość natychmiastowego zdobywania informacji niezbędnych przy dokonywaniu czynności notarialnych. Nie trzeba tłumaczyć, jakie korzyści przynosi możliwość natychmiastowego wglądu poprzez Internet np. do centralnego rejestru testamentów, rejestru gruntów czy ksiąg wieczystych. Stosunkowo niewielkim nakładem finansowym można stworzyć wiele rejestrów innych, np. rejestr transakcji, rejestr osób ubezwłasnowolnionych itp. Do nich, prowadzonych na zasadzie elektronicznych baz danych, mogliby mieć dostęp tylko osoby uprawnione, a jest to możliwe właśnie dzięki podpisowi elektronicznemu. Coraz częściej zdarza się, że notariusze ustawowo obowiązani są do przesyłania drogą elektroniczną różnych informacji, a wtedy informacje te zaopatrują w kwalifikowany podpis elektroniczny.

Zakres stosowania elektronicznego przekazywania informacji w notariatach w innych krajach jest różny i przedstawia się następująco:

1. AUSTRIA – w formie elektronicznej od 1999 r., centralny rejestr prowadzony jest od roku 2000:

a) wszystkie akty notarialne sporządzone przez notariuszy są skanowane, rejestrowane, podpisywane drogą elektroniczną i gromadzone w centralnym systemie cyberDOC,

b) rolę centralnego organu rejestrującego pełni spółka z.o.o z większościowym udziałem Rady Krajowej Notariatu Austriackiego,

c) poza wspomnianym centralnym rejestrem spółka zarządzająca obsługuje również rejestry upoważnień notarialnych i rejestry handlowe, na prośbę notariuszy zarządza bankiem rejestrów depozytów powierniczych, ma dostęp do elektronicznej bazy danych ksiąg wieczystych, sporządza wyciągi i odpisy z tych ksiąg, a także inne dokumenty związane ze stosunkami publicznymi i organizacją pewnych wydarzeń.

2. BELGIA – system centralnego gromadzenia danych związanych z pracą notariuszy wprowadzono w roku 2000. Obejmuje on:

a) rejestry testamentów,

b) elektroniczne kontakty z fiskusem oraz innymi instytucjami prowadzącymi centralne rejestry.

3. FRANCJA – centralny rejestr informacji dotyczący czynności notarialnych wprowadzono w roku 1997. Rejestr obejmuje i prowadzi:

a) przelewy finansowe między kasami depozytowymi,
b) rejestry hipoteczne,
c) przechowywanie akt notarialnych,
d) wymiany między notarialnymi kasami emerytalnymi,
e) deklaracje o przemieszczeniu się osoby,
f) składki i rejestry katastralne,
g) testamenty,
h) bazy danych nieruchomości,

Osobą zarządzającą centralną bazą danych jest spółka akcyjna jednoosobowa, której jedynym akcjonariuszem jest Rada Krajowa Notariatu Francji.

4. CZECHY – system centralnego gromadzenia danych wprowadzono w 2001 r. System ten prowadzi:

a) Centralny Rejestr Testamentów,
b) rejestr nieruchomości,
c) rejestr osób zatrudnionych w kancelariach notarialnych.

Osobą zarządzającą centralnym rejestrem jest spółka kapitałowa świadcząca usługi na podstawie umowy z notariatem czeskim.

5. ŁOTWA – centralny system gromadzenia danych został wprowadzony w roku 2004. Obejmuje on:

a) centralny rejestr testamentów i innych dokumentów spadkowych,
b) centralny rejestr pełnomocnictw.

Osobą zarządzającą tym rejestrem jest spółka kapitałowa mająca umowę z Krajową Radą Notarialną Łotwy.

6. NIEMCY – centralny system gromadzenia danych został wprowadzony w połowie lat 80-tych na poziomie Krajowej Rady Notarialnej. W roku 2000 do systemu prawnego Niemiec wprowadzony został podpis elektroniczny, umożliwiający notariuszom korzystanie ze specjalistycznych baz danych i narzędzi prawnych w ich codziennej praktyce, brak jest jednak scentralizowanego archiwum elektronicznego. Rolę centrum certyfikacji podpisów elektronicznych notariuszy pełni spółka z ograniczoną odpowiedzialnością Notarnet GmbH, powołana przez Krajowa Radę Notarialną.

7. WŁOCHY – centralny system gromadzenia danych wprowadzony został w roku 1993, od roku 2002 dokument elektroniczny zaczęto stosować przy transakcjach związanych z obrotem nieruchomościami, przy wpisach do ksiąg wieczystych i innych. Centralna baza danych, do której notariusze mają dostęp, obejmuje rejestr nieruchomości, spółek, rejestry hipoteczne, a także współpracuje z administracją skarbową. Osobą zarządzającą centralnym rejestrem jest spółka akcyjna Notartel, której 90% akcji należy do Krajowej Rady Notarialnej, a 10% do Narodowej Kasy Notarialnej.

8. HISZPANIA – centralny system gromadzenia danych wprowadzony został w połowie lat 90-tych. W systemie tym notariusze połączeni są poza siecią Internetu, gdyż na ich potrzeby stworzona została tzw. indywidualna struktura informatyczna, co znacznie zwiększyło bezpieczeństwo przesyłania informacji. Centralny system gromadzenia danych prowadzi rejestry testamentów, pełnomocnictwa, rejestry odwołanych testamentów i odwołanych pełnomocnictw. Jest on zintegrowany z administracją skarbową i innymi rejestrami, co pozwala notariuszom ustalić np. zaległości podatkowe klientów i zdobywać inne niezbędne informacje o funkcjonowaniu notariatu. Osobą zarządzającą centrum gromadzenia danych jest spółka kapitałowa powołana przez Krajową Radę Notarialną, będąca obecnie na własnym rozrachunku. Spółka ta utrzymuje się z opłat wnoszonych przez notariuszy (ok. 150 euro miesięcznie płaci każdy notariusz za to, ze jest objęty centralnym systemem) oraz z wynagrodzeń, jakie otrzymuje tytułem udostępniania bazy danych innym instytucjom (oczywiście na ściśle określonych warunkach).

Powyższe wyliczenie ma charakter przykładowy.

Zakres stosowania podpisu elektronicznego przy tworzeniu centralnych baz danych stale rozszerza się i choćby z tego powodu każdy notariusz powinien być wyposażony w kwalifikowany (bezpieczny) podpis elektroniczny, a jeśli jeszcze nie posługuje się takim podpisem, to z pewnością w najbliższym czasie zostanie do tego zmuszony ustawami. Jeden z problemów, jaki pojawia się przed notariatami krajowymi dotyczy tego, kto ma wydać certyfikat elektronicznego podpisu notariusza. Najwłaściwszym ze względów prestiżowych byłoby rozwiązanie, w którym certyfikat podpisu elektronicznego notariusza wydawałaby Rada Krajowa

Notariatu danego kraju bądź naczelny organ administracji publicznej (np. Minister Sprawiedliwości). Możliwość wydawania certyfikatów przez Radę Krajową Notariatu wiązałaby się ze stworzeniem własnego Centrum Certyfikacji i bardzo dużymi nakładami finansowymi. W Polsce notariusze uzyskują certyfikaty elektronicznego podpisu od komercyjnych firm świadczących tego typy usługi, na takich samych zasadach jak każdy obywatel. Polska ustawa o podpisie elektronicznym, jak większość ustaw krajów europejskich, dopuszcza na zasadzie równości świadczenie usług certyfikacyjnych, a więc i wydawanie certyfikatów elektronicznego podpisu, przez podmioty mające siedzibę w każdym kraju Unii Europejskiej. Możliwa zatem byłaby sytuacja, aby stworzyć jedno centrum certyfikacji dla notariuszy z krajów, w których uznawane są certyfikaty wydane przez podmioty mające siedzibę w innych krajach. Stworzenie takiego Międzynarodowego Centrum Certyfikacji dla notariuszy np. państw należących do Międzynarodowej Unii Notariatu należałoby poważnie rozważyć.

Drugą sferą wykorzystania elektronicznego podpisu przez notariusza, jakże trudną i kontrowersyjną, są elektroniczne czynności notarialne. W tej dziedzinie wyróżniamy dwie grupy czynności:

1) uczestniczenie w procesie wydawania certyfikatów podpisu elektronicznego bądź wydawanie certyfikatów elektronicznego podpisu,

2) dotychczasowe czynności notarialne, ale dokonywane przy użyciu podpisu elektronicznego:

a) elektroniczny akt notarialny,

b) elektroniczne dokumenty poświadczone przez notariusza.

Wydanie certyfikatu podpisu elektronicznego jest niczym innym jak poświadczeniem, że osoba, która posługuje się kwalifikowanym podpisem elektronicznym, jest tą, za którą się podaje. Certyfikat jest więc swoistym poświadczeniem wydanym przez osobę (Centrum Certyfikacji), do której mamy zaufanie. Czynność taka, dokonana poza obiegiem elektronicznym, byłaby czynnością notarialną w czystym wymiarze. W Polsce, gdy rozpoczęła się dyskusja nad ustawą o podpisie elektronicznym, spora grupa naukowców, kompetentna w dziedzinie podpisu elektronicznego, w notariacie upatrywała tę organizację, która jest najlepiej predysponowana do świadczenia usług związanych z wydawaniem certyfikatów podpisu elektronicznego. Głównym argumentem przemawiającym za tym rozwiązaniem było zaufanie, jakim cieszą się notariusze. Zaufanie to po-

wstawało na przestrzeni wielu lat i wpisane jest w tradycję społeczeństwa polskiego. Wyzwanie takie jednak nie tylko przerosło możliwości polskiego notariatu, ale i zaskoczyło samych notariuszy, którzy do świadczenia tego rodzaju usług byli nieprzygotowani. W efekcie polska ustawa o podpisie elektronicznym wykluczyła możliwość wydawania certyfikatów podpisu elektronicznego przez notarialne centrum certyfikacji i świadczenie przez notariuszy usług certyfikacyjnych. Pozostawiono im natomiast jako czynność notarialną dokonywaną w procesie wydania certyfikatu podpisu elektronicznego możliwość notarialnego poświadczenia podpisu na wniosku o wydanie certyfikatu podpisu elektronicznego, o ile przewiduje to w swej polityce certyfikacji podmiot wydający te dokumenty. Czynność taka polega na tym, że osoba ubiegająca się o wydanie certyfikatu podpisu elektronicznego zwraca się do notariusza o poświadczenie swego podpisu (potwierdzenie tożsamości, jak też prawdziwości danych z rejestrów osób prawnych) na wniosku o wydanie certyfikatu oraz na elektronicznym przesłaniu informacji o dokonanej czynności do wskazanego przez tę osobę Centrum Certyfikacji. Na tą okoliczność sporządza protokół. Centrum Certyfikacji po otrzymaniu od notariusza niezbędnych informacji objętych wnioskiem o wydanie certyfikatu, już bez jego pośrednictwa wyposaża wnioskodawcę w certyfikat jego podpisu elektronicznego. W odbiorze wnioskodawcy to właśnie notariusz jest gwarantem wiarygodności podpisu elektronicznego, chociaż samego certyfikatu nie wydaje. Dokonywanie powyższych czynności przez notariuszy pozwala włączyć notariat do kręgu czynności elektronicznych, zachowując dotychczasową pozycję i prestiż zawodu.

Celem wprowadzenia podpisu elektronicznego do ustawodawstw krajowych jest zrównanie formy elektronicznej czynności z formą tradycyjną. Wydawałoby się więc oczywiste, że podpis elektroniczny staje się jedynie nowym narzędziem w pracy każdego prawnika, w tym w pracy notariusza, i czynności notarialne dokonywane w sposób tradycyjny będą mogły być wykonywane przy pomocy technik elektronicznych. Cechy i funkcja podpisu elektronicznego nie pozwalają jednak na sformułowanie powyższej tezy. Immanentną cechą dokonywanej przez notariusza czynności notarialnej, polegającej na sporządzeniu jakiegokolwiek kontraktu, jest jego osobisty kontakt z klientem. Pozwala to na ustalenie treści, wyjaśnienie wszelkich okoliczności towarzyszących umowie, na przeko-

naniu się, że treść kontraktu odpowiada woli kontrahenta. Wola stron umowy wyrażana jest w różny sposób, najczęściej ustnie w obecności notariusza, który sporządza dokument mający cechy dokumentu notarialnego. Cechą i funkcją podpisu elektronicznego jest właśnie to, że zainteresowany nie musi kontaktować się osobiście z kontrahentem ani notariuszem przy wyrażaniu swej woli. Przy elektronicznej formie zawierania umów notariusz staje się bądź osobą zbędną, bądź jego udział zostaje zminimalizowany. Obecnie w większości ustawodawstw krajowych dokument elektroniczny ma moc prawną przy kontraktach mniejszej rangi i nie zastępuje tradycyjnej formy notarialnej, która ma charakter bardziej doniosły.

Należy jednak uważniej przyjrzeć się możliwościom, jakie dla praktyki notarialnej stwarza wprowadzenie do systemów prawnych podpisu elektronicznego, a zwłaszcza skutkom prawnym tego podpisu, zawartego w polskiej (wzorowanej na innych) ustawie o podpisie elektronicznym. Według niej dane w postaci elektronicznej, opatrzone bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, są równoważne pod względem skutków prawnych z dokumentem opatrzonym podpisem własnoręcznym. Analizując powyższą definicję, można uznać możliwość sporządzania aktów notarialnych w postaci elektronicznej, skoro skutki prawne w nim zapisane równoważą podpis elektroniczny z podpisem własnoręcznym. Niektórzy teoretycy prawa głoszą tezę, że opatrywanie aktu notarialnego podpisem elektronicznym jest dopuszczalne. Mówią oni, że akt powinien zawierać podpis elektroniczny notariusza oraz osób obecnych przy jego sporządzaniu, przy czym złożenie podpisu powinno nastąpić w obecności notariusza. Elektroniczny akt notarialny sporządzony w ten sposób może w zasadzie pełnić te same funkcje co akt spisany na papierze, z tą różnicą, że tradycyjne podpisy zostaną zastąpione podpisami elektronicznymi. Czym zatem ma się różnić elektroniczny akt notarialny od aktu tradycyjnego? Czy różnica ma polegać tylko na złożeniu podpisu elektronicznego zamiast własnoręcznego, czy też na tym, że taki elektroniczny akt notarialny miałby być sporządzony za pośrednictwem elektronicznych środków przekazu, bez konieczności obecności udziału notariusza w chwili składania oświadczeń woli stron? Zrezygnowanie z bezpośredniej obecności notariusza przy sporządzaniu aktu notarialnego łamie jeden z atrybutów

prawa w systemie prawa łacińskiego, jakim jest pewność obrotu prawnego. Ponadto wyeliminowanie notariusza z czynności sporządzania elektronicznego aktu notarialnego stawia pod znakiem zapytania samą nazwę akt notarialny. Właściwsze wydaje się twierdzenie, że mamy do czynienia z aktem elektronicznym jako mutacją aktu notarialnego, będącego w istocie rzeczy instrumentem samego prawa elektronicznego, korzystającego z atrybutów szczególnej formy czynności prawnej.

Niewątpliwie elektroniczna forma aktu notarialnego będzie mogła zastąpić formę dotychczasową, ale tylko wtedy, gdy prawo na to wyraźnie zezwoli, a samo zrównanie formy pisemnej z formą elektroniczną, z jakim mamy do czynienia w większości krajowych ustaw o podpisie elektronicznym, nie jest wystarczające do sporządzenia aktów elektronicznych.

Na kongresie Międzynarodowej Unii Notariatu, który odbył się w Meksyku w roku 2004, w części poświęconej wykorzystaniu środków przekazu elektronicznego w praktyce notarialnej w ogóle nie zajmowano się elektronicznym aktem notarialnym ani żadną inną elektroniczną formą czynności notarialnej. Uczestnicy kongresu doszli do wniosku, że notariaty krajowe uwagę swoją powinny skupiać na tworzeniu baz danych, niezbędnych do sprawniejszego funkcjonowania notariatów. Wykorzystywanie nowych elektronicznych technologii powinno czynić notariat bardziej wiarygodny i bardziej atrakcyjny dla klientów.

## IV. Podsumowanie

Nie ulega wątpliwości, że notariusze chcą posługiwać się podpisem elektronicznym w szerokim i pełnym zakresie. Sporządzanie dokumentów przy jego wykorzystaniu jest tak różne od dotychczasowych form składania podpisów własnoręcznych, że z pewnością wymaga odrębnych zasad ujętych w rozstrzygnięciach prawnych dotyczących samego notariatu. Polskie prawo o notariacie nie jest dostosowane do czynności, jakie miałby wykonywać notariusz przy użyciu takiego podpisu. Na rozstrzygnięcia prawne dotyczące tej sfery funkcjonowania notariatu będzie trzeba jeszcze poczekać i dopiero wtedy będziemy zajmować się problemem, w jaki sposób dokonywać elektronicznych czynności prawnych.

Na dzień dzisiejszy zadaniem notariatu jest stworzenie infrastruktury centralnego gromadzenia danych przy zastosowaniu nowych technik elektronicznych.

W polskim systemie prawa notarialnego brak jest zasad organizacji infrastruktury i archiwizacji elektronicznych aktów notarialnych. Notariusze musieliby odpowiadać nie tylko za należyte sporządzenie elektronicznej wersji aktu notarialnego, ale także za to, jak akty te będą przechowywane i przekazywane. Muszą być dostatecznie zabezpieczone, aby osoby postronne nie miały dostępu do archiwum elektronicznego. Za to wszystko odpowiadać będą notariusze jako osoby wykonujące zawód zaufania publicznego. W tej sytuacji istotne jest pytanie, jak zapewnić bezpieczeństwo oraz wiarygodność elektronicznych aktów notarialnych tworzonych, przekazywanych i przechowywanych w postaci elektronicznej.

Najbardziej istotnym wydaje się więc stworzenie podstaw prawnych funkcjonowania centralnego rejestru gromadzenia danych dotyczących notariatu. Jedno wydaje się być pewne, rejestr taki wysiłkiem naszego samorządu powinien powstać. Wydaje się, że najbardziej funkcjonalną formą dla jego powstania byłoby powołanie spółki kapitałowej z udziałem notariatu oraz innej osoby mającej potencjał technologiczny i wiedzę zapewniającą właściwe utworzenie i eksploatację tego systemu. Proporcje kapitałowe tak powstałej spółki mogą być przedmiotem dyskusji.

Tworzenie centralnych rejestrów miałoby służyć przede wszystkim notariuszom, ale również mogłoby służyć innym osobom na ściśle określonych warunkach, na zasadach komercyjnych. Centralne rejestry testamentów, pełnomocnictw i inne, którymi zarządzałaby spółka kapitałowo związana z samorządem notarialnym, poza praktycznymi korzyściami, pozwoliłyby na uatrakcyjnienie i uwiarygodnienie notariatu jako instytucji w systemie prawnym. Należy przy tym podkreślić, że centralne rejestry dotyczące czynności notarialnych w różnym zakresie prowadzone są w większości notariatów krajów rozwiniętych.

Kończąc, należy wyciągnąć następujące wnioski:

1. Czynności notarialne z zastosowaniem podpisu elektronicznego bez zmiany obowiązujących przepisów prawa nie mogą być przez notariuszy wykonywane, z wyjątkiem czynności związanych z uczestniczeniem w procesie wydawania certyfikatów e-podpisu, do czego notariusze są już przygotowani i w ograniczonym zakresie wykonują. Należy pamiętać o tym, że prędzej czy później elektroniczna forma czynności prawnej zostanie do naszego porządku prawnego wprowadzona, a zatem nota-

riusze powinni osiągnąć taki stan gotowości, aby nowa elektroniczna rzeczywistość nie była dla naszej korporacji zaskoczeniem.

2. Należy jak najszybciej powołać osobę (spółkę kapitałową bądź inną formę prawną), która zajmie się tworzeniem systemu centralnej bazy danych czynności notarialnych. Osoba taka mogłaby również wydawać jako centrum certyfikacji certyfikaty podpisu elektronicznego notariuszom. Należy wspomnieć, że mogłoby być powołane jedno centrum certyfikacji e-podpisu dla wszystkich notariuszy zrzeszonych w Światowej Unii Notariatu. Mogłoby się ono mieścić w jednym z krajów członkowskich, nie wykluczając Polski.

3. Na początek należy stworzyć centralny rejestr pełnomocnictw i odwołanych pełnomocnictw, a także rejestr testamentów. Dalszym etapem funkcjonowania centralnego notarialnego rejestru bazy danych może być integracja z centralnymi rejestrami innych instytucji, i tak np. rejestru KRS, ksiąg wieczystych, ewidencji gruntów czy też dostępu do bazy PESEL, co umożliwiłoby bezpieczny i szybki przepływ informacji niezbędnych w pracy notariusza, z korzyścią zarówno dla klientów, jak i dla administratorów innych centralnych baz danych.

## BIBLIOGRAFIA

1. Z. Radwański, *Elektroniczna forma czynności prawnej*, Monitor Prawniczy 2001, nr 22.

2. W. Kocot, *Elektroniczna forma oświadczeń woli*, PPH 2001, nr 3.

3. A. Ambroziewicz, *Podpis elektroniczny – pojęcie i funkcje w obrocie*, Przegląd Sądowy 2001, nr 1.

4. *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 r.*, red. J. Jacyszyn, J. Przetocki, A.Wittlin, S. Zakrzewski, Warszawa 2002.

5. D. Szostek, *Podpis elektroniczny – problemy cywilnoprawne*, PPH 2002, nr l; t e n ż e, *Czeska ustawa o podpisie elektronicznym*, Rejent 2003, nr 4.

6. M. Drozdowicz, *(Nie) bezpieczny podpis elektroniczny*, PPH 2003, nr 1.

7. P. Antkiewicz, *Elektroniczne instrumenty płatnicze – potrzeba regulacji obrotu*, PPH 2002, nr 8.

8. J. Jacyszyn, *Podpis elektroniczny w praktyce notarialnej*, Rejent 2003, nr 12.

9. Dyrektywa Parlamentu Europejskiego i Rady Nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 013 z 19.01.2000, str. 0012-0020).

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

11. M. Marucha, *Nowa ustawa o podpisie elektronicznym*, Monitor Prawniczy 2002, nr 2.

12. J. Pejaś, Imed El Fray, *Dokument elektroniczny, podpis elektroniczny i ich aspekty prawne*, II Krajowa Konferencja Naukowa E-Finanse, Szczecin, 8-9 listopada 2001 r., (materiały konferencyjne, niepubl.).

13. Z. Marański, J. Pejaś, W. Ślusarczyk, *Budowa bezpiecznych usług internetowych na bazie certyfikatu klucza publicznego,* IV Krajowa Konferencja Zastosowań Kryptografii ENIGMA'2000, Warszawa 2000 r.