

## **Podpis bez pióra i papieru**

Autor tekstu: **Olga Łyjak, Marcin Matuzik**

**Z**a kilka lat prezydenta RP wybierzemy być może bez użycia długopisów i kart do głosowania, za to przy pomocy urządzeń przypominających dzisiejsze bankomaty. Zeznanie podatkowe wyślemy do urzędu przez Internet a w ten sam sposób z ZUS-em rozliczy się nasz pracodawca. Już dziś dzięki powstającym bankom wirtualnym pieniędzmi możemy zarządzać przy pomocy osobistego komputera. Wizja społeczeństwa informacyjnego, w którym papierowe dokumenty zostaną zastąpione przez komputerowe procedury stała się jeszcze bliższa dzięki podpisowi elektronicznemu.

W Polsce ustawa o podpisie elektronicznym obowiązuje od sierpnia 2002 r. W USA podobne prawo obowiązuje już od roku 2000 – Federalna ustawa USA z 24.01.2000 r. o podpisie elektronicznym (*Electronic Signature in Global and National Commerce Act*). Państwa Unii Europejskiej miały wprowadzić odpowiednie regulacje do końca 2001 roku, zgodnie z dyrektywą 1999/93 z 13.12.1999 o wspólnotowych podstawach regulacji podpisu elektronicznego. W tym samym czasie analogiczne prawodawstwo powstało w Czechach, na Słowacji i w Słowenii.

Ustanowienie ram prawnych dla podpisu elektronicznego stało się niezbędne w związku z rozwojem nowych technologii oraz globalnym charakterem Internetu. Aby zapewnić swobodny przepływ informacji wyrażonej w sposób elektroniczny, ułatwić rozwój handlu elektronicznego oraz umożliwić rozwój usług społeczeństwa informatycznego, informacje przekazywane drogą elektroniczną wymagają potwierdzenia ich autentyczności. Koncepcja podpisu elektronicznego musi również odpowiadać wymogom bezpieczeństwa obrotu prawnego i gospodarczego.

Polska ustawa o podpisie elektronicznym opiera się na dyrektywie unijnej nr 1999/93 i tym samym jest istotnym krokiem na drodze dostosowania polskiego prawa do wymogów społeczeństwa informacyjnego. Podpis elektroniczny ma pełnić w obrocie elektronicznym te same funkcje, jakie pełni podpis własnoręczny. Oznacza to, że dane zapisane w postaci elektronicznej opatrzone takim podpisem są równoważne pod względem skutków prawnych dokumentom podpisanym własnoręcznie, czyli spełniają wymogi zwykłej formy pisemnej. Podpis elektroniczny umożliwia zatem wiarygodne i pewne zawieranie umów na odległość.

Podpis elektroniczny nie ma żadnej formy graficznej ani nie jest elektronicznym zapisem znaku graficznego. Nie może również zostać złożony w oderwaniu od podpisywanych danych. Bardzo istotne jest to, że podpis elektroniczny jest ważny tylko wtedy, jeśli został złożony w okresie ważności certyfikatu wykorzystywanego do jego weryfikacji. Te wszystkie regulacje mają na celu zrównanie podpisu elektronicznego z podpisem własnoręcznym oraz umożliwienie wiarygodnej identyfikacji osoby, która złożyła e-podpis. Przy podpisie własnoręcznym identyfikacja osoby możliwa jest dzięki niepowtarzalności tego podpisu, a jego wiarygodność mogą sprawdzić grafolodzy. W przypadku podpisu elektronicznego taką weryfikację umożliwia odpowiedni certyfikat.

**Podpis elektroniczny** to sposób elektronicznego przekształcania danych (np. przy użyciu technik kryptograficznych – będzie to wtedy podpis cyfrowy), z zastosowaniem klucza prywatnego osoby podpisującej, umożliwiającą identyfikację tej osoby. Klucz prywatny zawarty jest w karcie chipowej, umożliwiającej składanie podpisu. Ustawa posługuje się pojęciem bezpieczny podpis elektroniczny weryfikowany na podstawie kwalifikowanego certyfikatu. Oznacza to, że podpis ten pochodzi od osoby, określonej w tym certyfikacie, jest przyporządkowany wyłącznie do osoby składającej ten podpis i został złożony za pomocą urządzenia służącego do składania tego podpisu (karty chipowej). Tylko taki podpis wywołuje takie same skutki prawne, co podpis własnoręczny.

**Certyfikat** to elektroniczne zaświadczenie, które umożliwia identyfikację osoby składającej e-podpis. Wydaje go centrum certyfikacyjne i przypisuje do konkretnej osoby. Certyfikatem kwalifikowanym (umożliwiającym składanie bezpiecznego podpisu) jest certyfikat wydany przez podmiot wpisany do rejestru podmiotów świadczących usługi certyfikacyjne (takie jak wystawianie certyfikatu, oznaczanie okresu jego ważności, zakresu stosowania certyfikatu do wszystkich bądź tylko określonego rodzaju transakcji), nad którym pieczęć ma minister gospodarki.

Liczne rozporządzenia wykonawcze do ustawy regulują m.in. korzystanie z Infrastruktury Klucza Publicznego, technologii pozwalającej na bezpieczne używanie w obrocie prawnym i gospodarczym podpisu elektronicznego oraz na poufność przesyłanych drogą elektroniczną danych.

## Jak to działa

By podpis elektroniczny był wiarygodny osoba chcąca się nim posługiwać powinna kupić certyfikat umożliwiający składanie bezpiecznych e-podpisów w jednym z punktów ich sprzedaży, czyli centrów certyfikacyjnych. Certyfikat to karta, na której znajdują się dwa klucze: publiczny i prywatny. Za pomocą klucza prywatnego szyfrowany jest podpis oraz dane przesyłane np. do kontrahentów. Właściciel karty otrzymuje również kod PIN potrzebny do używania karty. Centra certyfikacyjne oferujące podpisy elektroniczne zajmują się również uwierzytelnianiem podpisów i zbieraniem danych o podmiotach chcących się nim posługiwać. Potwierdzają także autentyczność podpisu i tożsamość obydwu stron podczas dokonywania transakcji handlowej lub podpisywania dokumentów urzędowych. Np. jeśli kupimy towar w wirtualnym sklepie to złożony przez nasz podpis wygenerowany przy pomocy klucza prywatnego zostanie potwierdzony sprzedawcy. My również, dzięki certyfikatowi sprzedawcy, otrzymamy z centrum potwierdzenie czy sprzedawca jest zarejestrowany jako użytkownik podpisu. Aby jednak połączyć się z centrum certyfikacyjnym drogą Internetu wymagane jest zainstalowanie odpowiedniego oprogramowania. Centra weryfikują także serwery, z których zawierane są transakcje, by uniknąć oszustów wykorzystujących niezarejestrowane komputery. Dzięki temu możemy również ustalić, czy nasz kontrahent nie jest oszustem. Deszyfrowanie podpisanego dokumentu oraz identyfikacja drugiej strony jest możliwa dzięki powszechnie dostępnemu kluczowi publicznemu. Sam elektroniczny podpis mieści się np. w karcie przypominającej kredytową a składać go można nawet przy pomocy przystawki podłączonej do komputera w domu.

## Skorzystać mogą wszyscy

Ustawa o podpisie elektronicznym przyczyniła się do informatyzacji polskich urzędów i ułatwiła z nimi kontakt. Zgodnie z nią do końca 2004 roku urzędy muszą być gotowe do komunikacji z obywatelem przez Internet, jeśli ten zażyczy sobie właśnie takiego sposobu. Praktyka ta nie jest jeszcze powszechna. Natomiast od sierpnia 2006 r. urzędy muszą zapewnić petentom, odbiorcom usług certyfikacyjnych, wnoszenie podań i wniosków w formie elektronicznej. Olbrzymim ułatwieniem byłoby np. umożliwienie składania zeznań podatkowych PIT, CIT, czy deklaracji ZUS przy użyciu podpisu elektronicznego. Kolejną korzyść, jaka płynie z wprowadzenia podpisu elektronicznego to ułatwienie świadczenia usług wirtualnym bankom i sklepom elektronicznym. Banki wirtualne nie muszą już wysyłać do swoich klientów dodatkowych papierowych dokumentów. Pewniejszy jest też obieg pieniędzy w e-handlu i płatności kartami kredytowymi podczas wirtualnych transakcji. Ponadto wszystkie banki miały obowiązek dostosowania swojej działalności do wymogów ustawy do końca 2002 roku. Banki mogą również, podobnie jak firmy ubezpieczeniowe, biura maklerskie lub fundusze emerytalne tworzyć własne centra certyfikacyjne, poszerzając w ten sposób profil swojej działalności, co przyczyni się do wzrostu obrotów. Biura certyfikacyjne będą też powstawać jako niezależne firmy.

## Czy to bezpieczne?

Trudności z identyfikacją partnera z którym kontaktujemy się przez Internet to pierwszy problem, który może pojawiać się w praktyce, jednak nie powinien on być powszechny ze względu na działalność centrów certyfikacyjnych. Udane mogą okazać się także próby nielegalnego zdobywania numerów kart kredytowych. W roku 2000 czeskim specjalistom udało się złamać kod podpisu elektronicznego, co początkowo postawiło pod znakiem zapytania plany jego wprowadzania do powszechnego użytku. Jednak nie był to kod taki jaki jest obecnie używany w wypadku podpisów certyfikowanych. Czy tego bardziej skomplikowanego nie uda się złamać pokaże praktyka. Trudności mogą pojawić też w transakcjach międzynarodowych podczas potwierdzania tożsamości. Mogą one być też utrudnione ze względów technicznych.

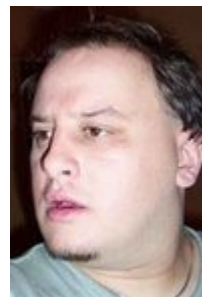
\*

Tekst pochodzi z serwisu [Global](#).

**Olga Łyjak** - dziennikarka, absolwentka prawa na Uniwersytecie Europejskim Viadrina we Frankfurcie nad Odrą oraz Uniwersytecie im. Adama Mickiewicza w Poznaniu. Pracuje w renomowanej kancelarii prawniczej w Warszawie. Interesuje się prawem wspólnotowym a głównie zagadnieniami związanymi ze wspólnym rynkiem. Obecnie jest doktorantką w Instytucie Nauk Prawnych PAN. Pracę doktorską pisze z zakresu prawa wspólnotowego — rynku wewnętrznego w energetyce oraz polskiego prawa energetycznego. Zajmuje się również prawnymi aspektami działalności przedsiębiorstw na wspólnym rynku oraz zarządzaniem strategicznym przedsiębiorstw na rynku UE.

### **Marcin Matuzik**

Absolwent Politologii i Nauk społecznych na Uniwersytecie Jagiellońskim. Dziennikarz zajmujący się głównie tematyką Internetu i Społeczeństwa Informacyjnego oraz nowymi technologiami. Publikował m.in. w Polityce, Dzienniku Polskim, Eurostudencie i Przekroju. Autor publikacji naukowych, zajmuje się m.in. dorobkiem kanadyjskiego medioznawcy i socjologa Marshalla McLuhana i tematyką Globalnej Sieci, jego publikacje ukazały się m.in. w Zeszytach Prasoznawczych i Studiach Medioznawczych. Redaktor Prowadzący działu Technologie serwisu Global.



[Pokaż inne teksty autora](#)

(Publikacja: 17-03-2005)

[Oryginał..](http://www.racjonalista.pl/kk.php/s,4012) (<http://www.racjonalista.pl/kk.php/s,4012>)

Contents Copyright © 2000-2008 Mariusz Agnosiewicz

Programming Copyright © 2001-2008 Michał Przech

Autorem tej witryny jest Michał Przech, zwany niżej Autorem.

Właścicielem witryny są Mariusz Agnosiewicz oraz Autor.

Żadna część niniejszych opracowań nie może być wykorzystywana w celach komercyjnych, bez uprzedniej pisemnej zgody Właściciela, który zastrzega sobie niniejszym wszelkie prawa, przewidziane w przepisach szczególnych, oraz zgodnie z prawem cywilnym i handlowym, w szczególności z tytułu praw autorskich, wynalazczych, znaków towarowych do tej witryny i jakiegokolwiek ich części.

Wszystkie strony tego serwisu, wliczając w to strukturę katalogów, skrypty oraz inne programy komputerowe, zostały wytworzone i są administrowane przez Autora.

Stanowią one wyłączną własność Właściciela. Właściciel zastrzega sobie prawo do okresowych modyfikacji zawartości tej witryny oraz opisu niniejszych Praw Autorskich bez uprzedniego powiadomienia. Jeżeli nie akceptujesz tej polityki możesz nie odwiedzać tej witryny i nie korzystać z jej zasobów.

Informacje zawarte na tej witrynie przeznaczone są do użytku prywatnego osób odwiedzających te strony. Można je pobierać, drukować i przeglądać jedynie w celach informacyjnych, bez czerpania z tego tytułu korzyści finansowych lub pobierania wynagrodzenia w dowolnej formie. Modyfikacja zawartości stron oraz skryptów jest zabroniona. Niniejszym udziela się zgody na swobodne kopiowanie dokumentów serwisu Racjonalista.pl tak w formie elektronicznej, jak i drukowanej, w celach innych niż handlowe, z zachowaniem tej informacji.

Plik PDF, który czytasz, może być rozpowszechniany jedynie w formie oryginalnej, w jakiej występuje na witrynie. **Plik ten nie może być traktowany jako oficjalna**

**lub oryginalna wersja tekstu, jaki zawiera.**

Treść tego zapisu stosuje się do wersji zarówno polsko jak i angielskojęzycznych serwisu pod domenami Racjonalista.pl, TheRationalist.eu.org oraz Neutrum.eu.org.

Wszelkie pytania prosimy kierować do [redakcja@racjonalista.pl](mailto:redakcja@racjonalista.pl)