Maciej Dominiak

Jak stać się posiadaczem e-podpisu?

KROK PO KROKU PORADNIK

Definicję podpisu elektronicznego zaczerpnijmy z ustawy o podpisie elektronicznym, a zatem: Podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone, lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Ustawa wprowadza ponadto pojęcie – „bezpieczny podpis elektroniczny", który zdefiniowano następująco: bezpieczny podpis elektroniczny to podpis elektroniczny, który:

a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,

b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń oraz danych służących do składania podpisu elektronicznego,

c) jest powiązany z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Mamy zatem dwa pojęcia: „podpis elektroniczny" i „bezpieczny podpis elektroniczny". Należy dodać, że ten drugi, mocą ww. ustawy, powoduje skutki prawne równoważne podpisowi własnoręcznemu, jeśli weryfikowany jest za pomocą kwalifikowanego certyfikatu.

Istnieje więc możliwość zarówno technologiczna jak i prawna, posługiwania się dokumentami elektronicznymi mającymi moc dokumentów tradycyjnych opatrzonych podpisem własnoręcznym. Oznacza to, że osoba posługująca się bezpiecznym podpisem elektronicznym może składać oświadczenie woli – podpisywać różnego rodzaju dokumenty, jak np. zamówienia, decyzje, umowy, a także faktury w dowolnym miejscu i dowolnym czasie. Następnie za pośrednictwem Internetu można przesyłać je do odbiorcy znacznie szybciej niż pocztą tradycyjną. Porównanie kosztów związanych z generowaniem dokumentów oraz ich późniejszym obiegiem i przechowywaniem wskazuje znaczące oszczędności przy zastosowaniu dokumentów w formie elektronicznej. Podsumowując, sankcjonując prawnie podpis elektroniczny, stworzono podstawy do rozwoju szybszej i tańszej gospodarki elektronicznej (e-Biznesu). Ponadto podpis elektroniczny ma wkrótce ułatwić kontakty obywateli i biznesu z szeroko rozumianą administracją.

Aby móc posługiwać się bezpiecznym podpisem elektronicznym należy zaopatrzyć się certyfikat kwalifikowany oraz bezpieczne urządzenie do składania podpisu elektronicznego. Certyfikaty kwalifikowane wystawiane są przez centra certyfikacji, wpisane na mocy decyzji Ministra Gospodarki do rejestru kwalifikowanych podmiotów, świadczących usługi certyfikacyjne związane z podpisem elektronicznym. W Polsce funkcjonują cztery takie centra wymienione wg kolejności wpisu do ww. rejestru: CERTUM – Powszechne Centrum Certyfikacji – prowadzone przez Unizeto Technologies SA, SIGILLUM – należące do Polskiej Wytwórni Papierów Wartościowych, SIGNET – utrzymywane przez TP Internet oraz KIR – Krajowa Izba Rozliczeniowa SA.

Bezpieczne urządzenia, w skład których wchodzi karta kryptograficzna, czytnik kart oraz oprogramowanie podpisujące, także są oferowane przez ww. centra certyfikacji.

Koszt pełnego zestawu, zawierającego certyfikat kwalifikowany oraz dodatkowo certyfikat niekwalifikowany, umożliwiający między innymi podpisywanie i szyfrowanie poczty elektronicznej, kształtuje się w zależności od wystawcy na poziomie 348–399 zł. Jest to koszt jednorazowy pełnego zestawu. Po 12 miesiącach wygaśnie ważność certyfikatu, którego odnowienie kosztuje od 95 do 130 zł.

Na przykładzie CERTUM – Powszechnego Centrum Certyfikacji, przedstawię sposób uzyskania pełnego zestawu do składania bezpiecznego podpisu elektronicznego –

bezpieczne urządzenie oraz certyfikat kwalifikowany.

Ponieważ procedura wystawienia certyfikatu kwalifikowanego wymaga osobistego stawienia się w celu weryfikacji tożsamości, należy wejść na stronę www.certum.pl

i w zakładce *o nas*, a następnie *punkty rejestracji*, odszukać adres najbliższego Punktu Rejestracji (PR).

To tam należy się zgłosić w celu złożenia wniosku o wydanie kwalifikowanego certyfikatu oraz zawarcia stosownej umowy. Gdy Punkt Rejestracji jest zbyt odległy, należy skorzystać z Punktu Potwierdzania Tożsamości. Przed wybraniem się do PR warto zapoznać się z instrukcją umieszczoną w ww. serwisie pt. „Certyfikat kwalifikowany – krok po kroku", która ułatwi podjęcie decyzji dotyczącej rodzaju certyfikatu oraz z wykazem „niezbędnych dokumentów", które należy mieć ze sobą. Przykładowo osoba fizyczna, która będzie posługiwała się bezpiecznym podpisem we własnym imieniu, zobowiązana jest okazać w PR dowód osobisty lub paszport oraz drugi dokument np. prawo jazdy. Osoba reprezentująca firmę, poza dokumentem stwierdzającym tożsamość, winna przedstawić dokumenty firmy – przykładowo odpis z KRS, oraz pełnomocnictwo podpisane przez osobę uprawnioną do reprezentacji firmy. Inne opcje reprezentacji i wymag-

anych dokumentów są szczegółowo opisane w podanym serwisie www.

Następnym krokiem jest wizyta w Punkcie Rejestracji, tam operator dokona weryfikacji tożsamości osoby ubiegającej się o certyfikat, sprawdzi dostarczone dokumenty, sporządzi wniosek o certyfikat i przygotuje stosowną umowę. Wizytę w PR skróci wypełniony wniosek pobrany z podanej powyżej strony internetowej CERTUM.

Wizyta w Punkcie Rejestracji, podczas której załatwiane są wszelkie formalności, trwa około 25 minut. Następnie Powszechne Centrum Certyfikacji na podstawie otrzymanych dokumentów wystawia certyfikat, zapisując go na karcie kryptograficznej. Karta oraz kody PUK i Sekret są przekazywane w bezpiecznych kopertach w ciągu kilku, maksymalnie 7 dni, osobie wnioskującej o wydanie certyfikatu. Użytkownik po otrzymaniu karty, kopert z kodami oraz zainstalowaniu bezpiecznego urządzenia w komputerze, posiada gotowy do użycia zestaw do składania bezpiecznego podpisu elektronicznego.

W skład zestawu do składania bezpiecznego podpisu elektronicznego wchodzi dodatkowo certyfikat niekwalifikowany. Wynika to z ograniczeń zastosowania certyfikatów kwalifikowanych, które służą tylko i wyłącznie do opatrywania dokumentów elektronicznych bezpiecznym podpisem elektronicznym. Natomiast certyfikat niekwalifikowany może być wykorzystywany do podpisywania oraz szyfrowania dokumentów, poczty elektronicznej a także autoryzacji w Sieci. Wzbogacenie zestawu do składania bezpiecznego podpisu elektronicznego o certyfikat niekwalifikowany umożliwia użytkownikom korzystanie z dodatkowych usług oferowanych w ramach infrastruktury klucza publicznego – PKI (*ang. Public Key Infrastructure*).

Wszystkich zainteresowanych pogłębieniem wiedzy na temat e-podpisu odsyłam do broszury „Podpis Elektroniczny, sposób działania, zastosowanie i korzyści" wyd. przez Ministerstwo Gospodarki; wydanie II 2005, która w wersji elektronicznej jest dostępna w serwisie www.e-fakty.pl. Znajdziecie tam Państwo również oprogramowanie proCertum Combi Lite, służące do podpisywania, szyfrowania, oznaczania czasem dokumentów elektronicznych oraz weryfikowania złożonych podpisów. proCertum Combi Lite jest wolny od opłat licencyjnych w wykorzystaniu niekomercyjnym.

Maciej Dominiak pracuje jako Produkt Manager w firmie Unizeto Technologies SA.

Jakie parametry powinien mieć komputer przeznaczony do składania bezpiecznych podpisów elektronicznych?

Komputer współpracujący z bezpiecznym urządzeniem powinien spełniać niżej wymienione wymagania:
Procesor: minimum Pentium 100Mhz,
pamięć RAM: 64 MB,
porty: USB, RS232 lub PCMCIA, (połączenie z czytnikiem kart kryptograficznym)
system operacyjny: Microsoft Windows 95, 98, ME, NT, 2000, XP,
napęd CD-ROM,
przeglądarka internetowa np. Internet Explorer 5.5x (siła szyfrowania: 128-bit).