ROCZNIKI EKONOMII I ZARZĄDZANIA
Tom 6(42), numer 2 – 2014

JUDYTA PRZYŁUSKA-SCHMITT

PODPIS ELEKTRONICZNY W BIZNESIE

WSTĘP

Każdy, kto prowadzi działalność gospodarczą lub kontaktuje się z urzędami administracji publicznej, wie, ile „musi się nachodzić", ile czasu zajmuje załatwianie poszczególnych spraw, jakie napotyka problemy z dostarczaniem, wysyłaniem i odbieraniem przeróżnych dokumentów. Tradycyjna wymiana dokumentów opiera się na przesyłaniu dokumentów papierowych, opatrzonych stemplami i podpisami. W celu potwierdzenia tożsamości posługujemy się dowodem osobistym lub paszportem, a ważne dokumenty dodatkowo poświadczamy notarialnie. Rozwiązaniem tych wielu codziennych czynności stał się system Elektronicznej Wymiany Danych (EDI), będący zarazem wyrazem konieczności sprostania wymogom rynku w zapewnieniu szybkiej wymiany informacji i sprawnego dokonywania transakcji[1]. Internet oraz inne technologie mobilne dają podstawy nowoczesnym kanałom dystrybucji informacji i w coraz szybszym tempie stają się integralną częścią życia ludzkiego. Nowoczesna technologia wymaga nowych sposobów działań w wielu dziedzinach, które stanowią ważny wyznacznik zachodzących zmian na wielu płaszczyznach życia codziennego[2]. System ten łączy w sobie wiele zalet:

– umożliwia przekazywanie dokumentów w sposób zautomatyzowany bez konieczności ich wielokrotnego przepisywania,

Dr JUDYTA PRZYŁUSKA-SCHMITT – adiunkt Katedry Instytucji i Rynków Finansowych, Instytut Ekonomii i Zarządzania, Wydział Nauk Społecznych na Katolickim Uniwersytecie Lubelskim Jana Pawła II; adres do korespondencji: Al. Racławickie 14, 20-950 Lublin; e-mail: judytaprzyluska@wp.pl

[1] J. PRZYŁUSKA, *Świadczenie usług finansowych drogą elektroniczną,* w: *Innowacje na polskim rynku finansowym*, red. K. Ciejpa-Znamirowski, KUL, Lublin 2004, s. 203.

[2] A. KOŚCIÓŁEK, *Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym,* Wolters Kluwer Polska, Warszawa 2012, s. 18.

– przyspiesza reakcję drugiej strony na przekazaną informację,
– redukuje koszty emisji i obsługi tradycyjnych dokumentów,
– usprawnia marketing,
– pozwala na zastosowanie nowych metod organizacji produkcji,
– zwiększa konkurencyjność firm i wpływa na charakter więzi gospodarczych.

Jednocześnie transakcje jakiejkolwiek wymiany w sieci wymagają zapewnienia bezpieczeństwa, a wymogiem postępującej globalizacji współczesnego świata jest przyspieszenie i ułatwienie wymiany informacji i dokumentów. Temu celowi podporządkowuje się nowoczesne, elektroniczne środki przekazu, które wymagają zastosowania nowych, efektywnych metod bezpieczeństwa, gwarantujących w końcowym efekcie przynajmniej taki sam poziom pewności, jak metody tradycyjne. W tym celu, dla ochrony obrotu dokumentów w transakcjach handlowych stworzono ideę podpisu elektronicznego i cyfrowych certyfikatów weryfikujących tożsamość kontrahentów[3]. Wszystko to ma nie tylko usprawnić i przyspieszyć pracę oraz zapewnić jej jasny i przejrzysty obrót. Celem artykułu jest przybliżenie infrastruktury organizacji i funkcjonowania e-podpisu oraz obszarów jego wykorzystania.

1. KRÓTKA HISTORIA PODPISU ELEKTRONICZNEGO W POLSCE

Problematyka podpisu elektronicznego nie jest w Polsce zupełnie nowa. Uregulowana została w ustawie o podpisie elektronicznym z dnia 18 września 2001 r. (Dz. U. 2001, Nr 130, poz. 1450 z późn. zm.), która – wraz z pakietem aktów wykonawczych – weszła w życie 16 sierpnia 2002 r.[4], tworząc podwaliny do budowy kwalifikowanej infrastruktury klucza publicznego i zgodnie z zamysłem Ministerstwa Gospodarki przybliżając perspektywę udrożnienia obiegu elektronicznych dokumentów w obrocie administracyjno-prawnym oraz handlowym.

Bezpieczny podpis elektroniczny posiada niewątpliwie wiele zalet, gdyż: ułatwia i przyspiesza obrót handlowy, umożliwia zawieranie umów na odległość, gwarantuje otrzymanie dokumentu od konkretnie określonej osoby, stanowi dowód nadania i otrzymania dokumentu, stwarza możliwość składania wniosków, podań i odwołań w formie elektronicznej. Poza tym Ministerstwo Gospodarki wskazuje, że bezpieczny podpis elektroniczny może być obecnie stosowany do: podpisywania pism i decyzji administracyjnych przez urzędy, podpisywania faktur elektronicznych, zarejestrowania działalności gospodarczej (przy czym zakup

[3] K. LANGE-SADZIŃSKA, M. ZIEMECKA, *Przewodnik po EDI,* Uniwersytet Łódzki, Łódź 2000, s. 38.
[4] http://www.mg.gov.pl/ Akty prawne [dostep: 06.10.2014].

podpisu elektronicznego na potrzeby działalności gospodarczej może być zakwalifikowany jako koszt uzyskania przychodu w ramach prowadzonej działalności gospodarczej), składania deklaracji celnych i podatkowych oraz zgłoszeń ubezpieczenia społecznego (system PUE ZUS), podpisywania wniosków do Krajowego Rejestru Sądowego, podpisywania raportów dla Generalnego Inspektora Informacji Finansowej, korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych, podpisywania dokumentacji medycznej[5].

Infrastruktura klucza publicznego stanowi dobre zabezpieczenie, pozwalające na jednoznaczną identyfikację i uwierzytelnienie partnerów. Narzędzia służące cyfrowemu podpisywaniu dokumentów są wbudowane w dostępne i wykorzystywane w codziennej pracy systemy i oprogramowania komputerowe, takie jak: Microsoft Windows, Office czy Outlook.

Podpis elektroniczny wykorzystują nie tylko banki (system Eliksir) i ZUS (system płatnik) – co pozwala błyskawicznie dokonać przelewów i innych operacji finansowych – ale także gminy i przedsiębiorcy – w rozliczeniach między sobą i administracją publiczną. Warto zwrócić uwagę, że w ciągu 20-lecia działalności Krajowej Izby Rozliczeniowej, która jest jednym z kilku kwalifikowanych podmiotów świadczących usługi certyfikacyjne, jak dotychczas, nie odnotowała żadnego przypadku naruszenia bezpieczeństwa elektronicznej przesyłki.

Praktyczne formy podpisów cyfrowych stały się możliwe dzięki rozwojowi kryptografii i stanowią dodatkową informację dołączoną do wiadomości weryfikującej źródło jej powstania.

2. CECHY ELEKTRONICZNEGO PODPISU

Odbiorca informacji musi mieć p e w n o ś ć, że dokument wysłany drogą elektroniczną i podpisany e-podpisem pochodzi od tego właśnie nadawcy i wiadomość przez niego wysłana nie uległa najmniejszej zmianie, co gwarantuje jej i n t e g r a l n o ś ć. E-podpis jest techniką potwierdzenia autentyczności dokumentu i tożsamości jego nadawcy w sposób trudny do podrobienia, możliwy do weryfikacji osoby składającej e-podpis i trwale połączony z dokumentem. Oznacza to, że tylko jedna osoba może posługiwać się takim podpisem, co zapewnia autentyczność nadawcy, czyli jej u w i e r z y t e l n i e n i e. Z kolei p o u f n o ś ć polega na takim zaszyfrowania dokumentu, że dane w nim zawarte odczyta tylko osoba, do której wiadomość została wysłana. Dodatkową cechą w tworzeniu

[5] http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Dzialalnosc+gospodarcza+i+eprzedsiebiorczos/Podpis+elektroniczny

e-kumentów jest ich s t e m p l o w a n i e z n a k i e m c z a s u. Podpis elektroniczny daje możliwość przypisywania dokumentom dokładnego czasu ich powstania, co uniemożliwia dokonywanie jakichkolwiek nadużyć, np. antydatowania utworzonego dokumentu.

A zatem, zgodnie z powołaną ustawą, bezpieczny podpis elektroniczny może być uznany za równoważny podpisowi własnoręcznemu, jeśli jest przyporządkowany wyłącznie do osoby składającej e-podpis; sporządzany za pomocą bezpiecznych urządzeń będących pod kontrolą tej osoby; powiązany z danymi, do których został dołączony.

Złożenie oświadczenia woli opatrzonego bezpiecznym e-podpisem, weryfikowanym za pomocą ważnego, kwalifikowanego certyfikatu, rodzi te same skutki prawne, co własnoręczne podpisanie oświadczenia woli. W takich sytuacjach certyfikat jest niezbędny do posługiwania się podpisem elektronicznym. Dodatkowo, certyfikat kwalifikowany, który został wystawiony jego właścicielowi z zastosowaniem odpowiednich procedur weryfikacji tożsamości oraz klucz prywatny (służący do składania podpisów), musi być przechowywany w sposób bezpieczny (np. na karcie elektronicznej).

3. CERTYFIKATY CYFROWE I ICH RODZAJE

Certyfikat cyfrowy jest elektronicznym zaświadczeniem, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowywane do określonej osoby i potwierdzają jej tożsamość. Fizycznie jest to ciąg danych, zapisanych na odpowiednim nośniku (np. na karcie mikroprocesorowej – smartcard), składający się z pól zawierających: wersję, nazwę lub identyfikator organu wydającego certyfikaty, identyfikator subskrybenta, dla którego wydano certyfikat, jego klucz publiczny, okres ważności i numer seryjny certyfikatu oraz podpis organu wydającego. Autentyczność tego podpisu można sprawdzić tylko wtedy, gdy znany jest klucz publiczny organu certyfikującego. Klucz ten znajduje się na certyfikacie wystawionym dla organu certyfikującego przez organ wyższej instancji (Narodowe Centrum Certyfikacji). Weryfikacja certyfikatu polega na prześledzeniu łańcucha zaufania, zakończonego przez organ nadrzędny, cieszący się powszechnym zaufaniem, który sam dla siebie wystawia certyfikat. A zatem kryptografia klucza publicznego wymaga pewnej infrastruktury (Infrastruktury Klucza Publicznego – PKI) do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów.

Podpisanym dokumentem elektronicznym jest dokument pierwotny zdołączonym do niego zaszyfrowanym skrótem. W skład podpisu może wchodzić także certyfikat osoby podpisującej, który zawiera jej klucz publiczny, oraz informacja o tym, czy certyfikat był ważny w momencie podpisywania danego dokumentu[6].

Rys.1. Schemat użycia e-podpisu

Źródło: http://www.mg.gov.pl Podpis_elektroniczny [dostęp: 06.10.2014]

Od 1 maja 2008 r. wszystkie urzędy administracji publicznej zostały zobowiązane do przyjmowania dokumentów drogą elektroniczną. Infrastruktura PKI ma zastosowanie w: bezpiecznej poczcie, transakcjach typu e-commerce, wirtualnych sieciach prywatnych (Virtual Private Network – VPN), systemach ERP (zintegrowanego zarządzania przedsiębiorstwem), zabezpieczeniach stacji roboczej użytkownika (jego danych), zapewnieniu bezpieczeństwa na witrynach internetowych, urządzeniach i aplikacjach klienta. Zapewnia bezpieczne logowanie się, zastępując w ten sposób używane dotychczas tokeny.

PKI oparta jest na cyfrowych certyfikatach wiążących konkretnego uczestnika transakcji z kluczem kryptograficznym, stosowanym podczas realizowania bezpiecznych transakcji. Certyfikat jest wydawany przez Organ Certyfikacji, który

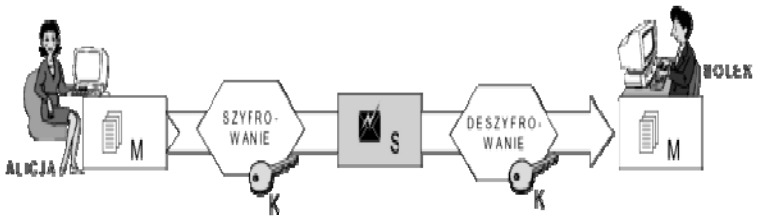
[6] Podpis elektroniczny, sposób działania, zastosowanie i korzyści, Ministerstwo Gospodarki, Warszawa 2005.

w momencie wydania dokumentu potwierdza podpisem cyfrowym związek pomiędzy użytkownikiem a kluczem, którego on używa. Ponieważ tak wystawiony certyfikat ma zawsze pewien okres ważności, należy przewidzieć następujące sytuacje związane z zarządzaniem certyfikatami: rejestracja użytkowników, generowanie certyfikatów, ich dystrybucja, aktualizacja i unieważnianie.

4. ZASADA DZIAŁANIA KLUCZY PUBLICZNYCH

Metody szyfrowania informacji można podzielić na dwie grupy: szyfrowanie z jednym kluczem (kryptografia symetryczna) i szyfrowanie z parą kluczy (kryptografia asymetryczna).

Kryptografia symetryczna odnosi się do metod, w których nadawca i odbiorca wiadomości używają tego samego klucza (hasła). Jest to tradycyjny sposób szyfrowania danych, który polega na tym, że szyfrowanie i deszyfrowanie informacji odbywa się za pomocą tego samego klucza. Przy jego użyciu nadawca szyfruje wiadomość, a następnie przesyła zakodowane informacje do odbiorcy przez niezabezpieczony kanał. Klucz, który utrzymany jest w ścisłej tajemnicy, wysyła kanałem bezpiecznym. Odbiorca, po otrzymaniu klucza i wiadomości, może ją odczytać. Minusem stosowania szyfrowania symetrycznego jest konieczność podjęcia dodatkowych środków w celu przekazania klucza odbiorcy. Należy tego dokonać w taki sposób, aby ktoś niepowołany nie dowiedział się o kluczu i nie posiadł go. W takim przypadku może on zarówno czytać, jak i zmieniać przesyłane informacje. Bezpieczeństwo tego systemu zależy więc od jakości ochrony klucza.

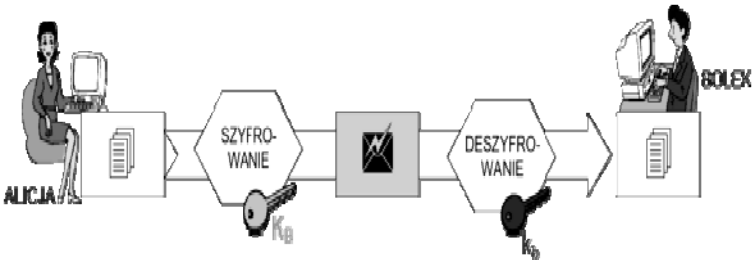


Rys. 2. Metoda symetrycznego szyfrowania informacji

Źródło: http://wazniak.mimuw.edu.pl [dostęp: 06.10.2014].

E-podpisy korzystają z kryptografii asymetrycznej, która polega na utworzeniu pary kluczy: prywatnego i publicznego. Klucz prywatny służy do podpisywania wiadomości, a klucz publiczny do weryfikowania podpisu.

Przy użyciu klucza publicznego – otrzymanego od adresata – nadawca koduje informacje, a następnie przesyła ją do odbiorcy. Odbiorca, dzięki swojemu kluczowi prywatnemu, może odszyfrować i odczytać informację. Do wiadomości może zostać dołączony elektroniczny podpis nadawcy, generowany na podstawie klucza prywatnego nadawcy. Weryfikacja autentyczności podpisu następuje po odszyfrowaniu go za pomocą klucza publicznego nadawcy. Adresat po odczytaniu podpisu może być pewny, że list jest autentyczny, gdyż weryfikacja taka pozwala na jednoznaczne określenie nadawcy.



Rys. 3. Metody asymetrycznego szyfrowania informacji

Źródło: http:// ważniak.mimuw.edu.pl [dostęp: 06.10.2014].

Do zaszyfrowania wiadomości wybierane są dowolne dwie duże liczby „p" i „q" (np. o długości 256 bitów), których iloczyn tworzy liczbę „n" (znaną publicznie). Na podstawie tych trzech liczb wykonywane są operacje matematyczne służące do zaszyfrowania wiadomości. Złamanie algorytmu jest zabiegiem wymagającym dużej mocy obliczeniowej, co wynika z faktu, że jego działanie polega na skomplikowanym matematycznym rozkładzie dużych liczb na czynniki pierwsze[7]. Obecnie najczęściej wykorzystywanym systemem jest RSA, który ma olbrzymie zastosowanie we współczesnej telekomunikacji, zwłaszcza w Internecie. Służy on do wymiany kluczy oraz do podpisu elektronicznego.

Masowe wystawianie dokumentów elektronicznych z bezpiecznym e-podpisem wymaga masowego uwierzytelniania się wobec urządzenia do składania bezpiecznego podpisu elektronicznego. W praktyce dokonywane jest automatyczne i wielokrotne składanie bezpiecznych podpisów elektronicznych, a udział osoby generującej e-podpis ogranicza się do jedynie do zainicjowania masowego procesu podpisywania i jego zakończenia[8].

[7] Szyfry symetryczne i asymetryczne, http://vpn.svera.pl/szyfry.php [06.10.2014].
[8] J. JANOWSKI, *Elektroniczny obrót prawny,* Wolters Kluwer Polska, Warszawa 2008, s. 370.

5. PODPIS ELEKTRONICZY I ZNAKOWANIE CZASEM W OBSZARZE BIZNESU

Podpis elektroniczny w działalności gospodarczej powinien być traktowany jak inwestycja w nowoczesność, choć wdrożenie go wiąże się z podjęciem konkretnych działań organizacyjnych i w określonych nakładach. Decyzje z tym związane powinny wynikać z budowania przewagi konkurencyjnej, podnoszenia efektywnosci i bezpieczeństwa oraz innych korzyści, jakie może osiągnąć przedsiębiorstwo. Planowanie skali i modelu wykorzystywania podpisu elektronicznego wymaga zebrania danych, dotyczących:

– charakteru spodziewanych korzyści (oszczędności czasowe, obniżenie kosztów, zwiększenie efektywności oraz zysków),

– liczby użytkowników, którzy będą korzystali z e-podpisu (wewnętrzny obieg dokumentów, występowanie kontrasygnaty, wymiana informacji z otoczeniem),

– wymagań prawnych dla podpisywanych dokumentów i przesyłek (stosowanie certyfikatów kwalifikowanych lub zwykłych, charakter danych: informacja niejawna, tajemnica handlowa, wymagania archiwizacji),

– zakresu wdrożenia w odniesieniu do organizacji (usługi PKI udostępniane wewnątrz firmy, w centrali, w oddziałach, w firmach partnerskich),

– źródeł i sposobów finansowania przedsięwzięcia (ze środków własnych, współfinansowanie przez partnerów handlowych)[9].

Obszary te dają podstawę do określenia optymalnego modelu korzystania z usług infrastruktury klucza publicznego, które można podzielić na trzy rozwiązania, dotyczące: zakupu usług od dostawcy zewnętrznego, budowy własnej infrastruktury klucza publicznego, zlecenia prowadzenia tej infrastruktury podmiotowi profesjonalnie zajmującemu się świadczeniem tego typu usług. Bez względu na wybór wariantu, niezbędne jest określenie harmonogramu wprowadzania podpisu elektronicznego w organizacji. Taki harmonogram jest podstawą do bieżącej oceny osiągania zamierzonych efektów, przy czym należy pamiętać, iż przed osiągnięciem zamierzonej wydajności systemu może wystąpić okresowy spadek sprawności obiegu dokumentów, spowodowany przystosowaniem się do wprowadzanych zmian.

Przestrzeganie przez podmioty certyfikujące norm dotyczących formatu i zawartości certyfikatów pozwala na sprawną wymianę danych pomiędzy podmiotami funkcjonującymi w różnych lokalizacjach i branżach. Bez względu na to, ja-

[9] *Podpis elektroniczny – sposób działania, zastosowanie i korzyści*, Ministerstwo Gospodarki, Warszawa 2005, s. 54.

kie programy użytkują nadawcy i odbiorcy informacji, mechanizm zabezpieczeń będzie zgodny. Bezpieczny transfer danych w postaci elektronicznej umożliwia prowadzenie interesów z wykorzystaniem Internetu. Transakcje mogą być realizowane między podmiotami, które już wcześniej ze sobą współpracowały w sposób tradycyjny bądź między stronami, które dotychczas nie kontaktowały się ze sobą. W ten sposób traci na znaczeniu odległość, koszty telekomunikacyjne oraz pozostałe, związane z czasem. Korzyści płynące z elektronicznej wymiany danych w biznesie można zaobserwować w usprawnieniu prowadzonej działalności, przyspieszeniu przebiegu procesów, poprawie wskaźników ekonomicznych.

Wypadkową efektu zastosowania elektronicznej wymiany danych jest zmiana stylu pracy organizacji. Wymuszane przez stosowane oprogramowanie uporządkowanie rejestracji i pełniejsza kontrola zachodzących (wewnątrz systemu informacyjnego firmy) zdarzeń, daje znacznie więcej, niż najlepiej skonstruowana procedura organizacyjna obiegu dokumentów tradycyjnych. Wsparcie najsłabszego ogniwa, jakim jest człowiek, ze strony systemów zarządzania obiegiem dokumentów pozwala na poprawę jakości funkcjonowania oraz lepszą ocenę efektywności pracy[10].

Podobne zjawisko występuje w relacjach między różnymi podmiotami gospodarczymi. Współpraca prowadzona na platformie wirtualnej wymaga stosowania się do reguł narzuconych przez użytkowane oprogramowanie. Wszystkie operacje są w automatyczny sposób rejestrowane i służyć mogą do analizy podejmowanych w przeszłości decyzji oraz stanowią dowód zaciągniętych zobowiązań. Przedsiębiorstwa, które odczuwają pozytywne efekty systematyzacji działalności, będą zainteresowane, aby większość ich kontaktów (jak nie wszystkie) była prowadzona w ten sam sposób. To wpływa na motywowanie partnerów w interesach do korzystania z elektronicznej wymiany dokumentów poprzez np. oferowanie współpracującym firmom lepszych warunków handlowych (niższych cen, wydłużonych terminów płatności) przy składaniu zamówień drogą elektroniczną.

Bez względu na branże, w jakiej działa przedsiębiorstwo, e-podpis może znaleźć zastosowanie w obiegu informacji wewnątrz firmy, gdyż wszędzie tam, gdzie podejmowane są decyzje, ma miejsce dwukierunkowy przepływ dokumentów. Przełożeni posługują się dokumentem w celu wydania poleceń służbowych, a pracownicy dostarczają w ten sposób żądane analizy, zestawienia, sprawozdania i raporty.

[10] Podpis elektroniczny – sposób działania, zastosowanie i korzyści, Ministerstwo Gospodarki, Warszawa 2005, s. 55.

Przesyłanie poleceń z wykorzystaniem podpisanej poczty elektronicznej lub podpisanych dokumentów otrzymywanych z zewnątrz jest rozwiązaniem bardziej oczywistym, ale stanowiącym malutki fragment możliwych zastosowań.

Jeżeli rozważymy możliwość wdrożenia prostego w obsłudze systemu agregującego wewnętrzne zapotrzebowanie np. na materiały biurowe, otrzymamy w efekcie usprawnienie procesu zamawiania towarów, unikniemy zbędnych zakupów oraz zoptymalizujemy wielkość zapasów. Podpis elektroniczny używany przez pracowników zgłaszających zapotrzebowanie, jak i weryfikujących zapotrzebowanie pod względem merytorycznym, pozwala na posługiwanie się dokumentem wirtualnym jako alternatywą dla druków. Dodatkowo, posługując się na rynku większym zbiorczym zamówieniem, można uzyskać korzyści w postaci lepszej oferty cenowej.

Kolejną zaletą jest możliwość dokonywania zakupów na wirtualnych giełdach towarowych. Elektroniczne platformy transakcyjne, na których spotykają się dostawcy i odbiorcy, również stwarzają możliwość negocjacji cen i innych parametrów handlowych. Jednocześnie pozwalają na wykorzystywanie efektu agregacji zamówień składanych przez różnych kupujących. Najskuteczniejszym mechanizmem autoryzacji dostępu i ochrony poufności transakcji prowadzonych na giełdach internetowych jest technologia klucza publicznego. W tym miejscu należy wspomnieć o możliwości stworzonej przedsiębiorcom przez ustawodawcę w zakresie tworzenia elektronicznych faktur. Faktury takie, opatrywane bezpiecznym podpisem elektronicznym (lub przesyłane za pomocą platformy EDI), mają wpływ – w dłuższym okresie czasu – na obniżenie kosztów obsługi księgowej i przyspieszenie czasu obsługi e-faktury (Dz. U. 05.113.1119).

Innym obszarem, w którym znajduje zastosowanie e-podpis, są zewnętrzne kontakty firmy. Wyposażenie pracowników operujących „w terenie" w certyfikaty pozwalające na autoryzację dostępu do firmowych baz danych, umożliwia bieżącą aktualizację ich zawartości. Przykładowo, jeśli pracownik dostawcy odpowiedzialny za ekspozycję i ilość towarów w sklepie, na bieżąco zgłasza zapotrzebowanie na poszczególne pozycje asortymentowe przez Internet, to wykorzystanie mechanizmów PKI pozwala na rezygnację z dodatkowej autoryzacji zgłoszeń. Posłużenie się prywatnym kluczem przy zdalnym dostępie do firmowej bazy może służyć indywidualizowaniu danych podawanych konkretnemu odbiorcy. Z kolei, zaopatrzeniowiec partnera handlowego posługując się swoim certyfikatem, otrzymuje dostęp do wydzielonego fragmentu serwisu internetowego dostawcy. W serwisie tym składa zamówienia, nie angażując handlowców do obsługi typowego zamówienia, a jednocześnie dostaje wgląd do informacji doty-

czących jego firmy, (takich jak: stan płatności faktur, przyznane limity zamówień czy aktualne warunki handlowe dla poszczególnych grup towarowych).

Podpis elektroniczny w działalności gospodarczej jest tylko jednym z obszarów jego zastosowań, poza którym znajduje on zastosowanie w wielu innych branżach[11]. Wystarczy wymienić: banki, ubezpieczenia, administrację publiczną czy indywidualnych obywateli, z którymi podmioty gospodarcze nawiązują stosunki handlowe i które ze sobą nawzajem mogą wchodzić w interakcje gospodarcze.

Jedno z założeń Dyrektywy 99/93/EC w sprawie wspólnotowej struktury dla e-podpisów wskazuje: (19) Podpisy elektroniczne będą stosowane w sektorze publicznym jako środek komunikowania się jednostek administracji rządowych oraz administracji Wspólnoty ze sobą oraz między tymi jednostkami a obywatelami i przedsiębiorcami, np. przy zamówieniach publicznych, podatkach, ubezpieczeniach społecznych, w systemach ochrony zdrowia i wymiaru sprawiedliwości.

Nowe technologie umożliwiły wprowadzenie sieci teleinformatycznych jako środka komunikacji między urzędem a obywatelem. Wiele dokumentów istniejących w postaci papierowej powinno być już dziś przesyłanych elektronicznie (pierwszą formą realizacji takiej usługi w Polsce był elektroniczny obieg dokumentów między ZUS-em a płatnikami składek ubezpieczeniowych). Inne usługi certyfikacyjne otwierają cały szereg zastosowań, w których dokument musi zachować wartość dowodową przez wiele lat, np. akty urzędu stanu cywilnego, dokumenty ubezpieczeniowe czy choćby (najpowszechniejsze) zeznania podatkowe.

Ustawa o dostępie do informacji publicznej z dnia 6 września 2001 r. zobowiązała podmioty publiczne do uruchomienia internetowego Biuletynu Informacji Publicznej (BIP). Był to pierwszy krok w kierunku wykorzystania nowoczesnych technologii w e-administracji. Kolejnym krokiem sprawnego wdrażania systemu elektronicznego obiegu informacji i dokumentów jest spełnienie wymogów prawnych zawartych w instrukcji kancelaryjnej. Do wymogów elektronicznego obiegu dokumentów, stawianych Jednostkom Samorządu Terytorialnego (JTS), należy zaliczyć:

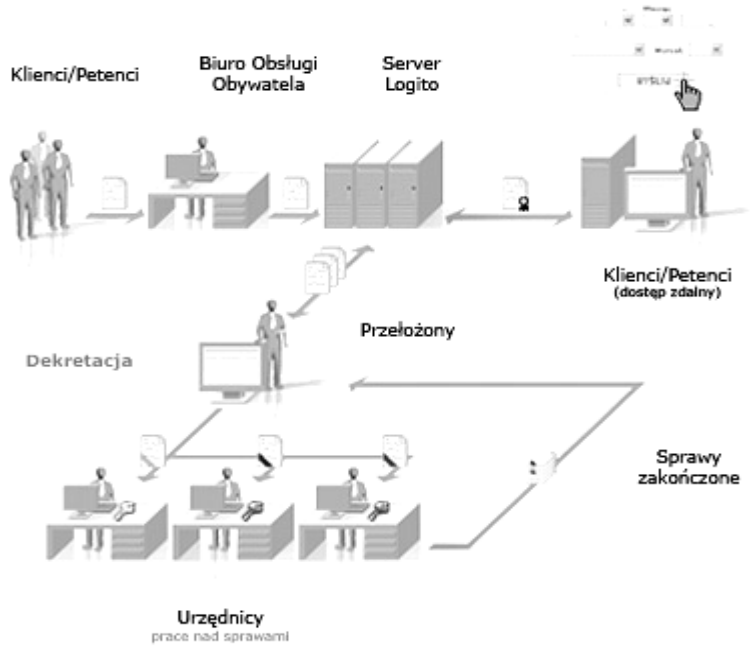
– elektroniczną skrzynkę podawczą,
– elektroniczne doręczanie pism interesantom,
– obsługę i przetwarzanie dokumentów elektronicznych w formacie XML,
– obsługę bezpiecznego podpisu elektronicznego,
– udostępnianie danych z rejestrów publicznych,
– bezpłatny program do prezentacji i weryfikacji dokumentu,
– zgłoszenie systemu do rejestru systemów teleinformatycznych,

[11] Podpis elektroniczny – sposób działania, zastosowanie i korzyści, Ministerstwo Gospodarki, Warszawa 2005, s. 57.

– spełnienie minimalnych wymogów dla systemów teleinformatycznych,
– badanie zgodności z oprogramowaniem interfejsowym,
– archiwa państwowe,
– bezpieczeństwo przetwarzania dokumentów oraz danych elektronicznych,
– format danych zgodny z definicją rejestrów publicznych.

Prawidłowe wdrożenie systemu obiegu informacji i dokumentów w jakiejkolwiek jednostce administracyjnej, skutkuje zwiększeniem się zadowolenia klienta z obsługi. System obiegu informacji pozwala na monitorowanie prowadzonych w urzędzie spraw, przechowywanie gromadzonych zbiorów danych, śledzenie przepływu dokumentów, zbieranie potrzebnych informacji oraz sterowanie tokiem pracy.

Przejście z dokumentów papierowych na formę elektroniczną (rys. 6) jest nieuniknionym elementem rozwoju każdej współczesnej organizacji.



Rys. 6. Elektroniczny obieg dokumentów
Źródło: http://www.cyfrowyurzad.pl [dostęp: 21.03.2012]

Efektywne i sukcesywne wdrożenie systemu obiegu informacji i dokumentów w jednostce administracyjnej, a tym samym przeniesienie usług publicznych na płaszczyznę elektroniczną ma na celu zwiększenie zadowolenia obywatela z obsługi. Wdrażanie systemów informatycznych oraz ich integracja z coraz bardziej

powszechnymi elektronicznymi kanałami komunikacyjnymi pozwala na osiągnięcie rozwoju usług elektronicznych na wyższym poziomie. Wiąże się to zarówno z udostępnieniem dokumentów do pobrania, złożeniem pisma, jak i monitorowaniem przebiegu sprawy urzędowej przez obywatela. Kompleksowa i bezpieczna interakcja obywatela z urzędem jest możliwa dopiero po dostosowaniu działalności w zakresie bezpiecznego podpisu elektronicznego (określonego w ustawie) przez administrację publiczną. Funkcjonalność bowiem takiego elektronicznego urzędu polega na jego powiązaniu z innym wirtualnym urzędem oraz Bazą Informacji Publicznej (BIP), z których mogą korzystać również obywatele.

6. KOSZTY POZYSKANIA ELEKTRONICZNEGO PODPISU

W celu posługiwania się bezpiecznym e-podpisem konieczne jest posiadanie zestawu do składania podpisu elektronicznego. Zestaw w postaci standardowej składa się z: czytnika kart kryptograficznych, karty kryptograficznej, oprogramowania, certyfikatu kwalifikowanego, znakowania czasem oraz daty ważności certyfikatu (najczęściej 1 roku lub 2 lata). Koszt takiego zestawu z czytnikiem mogą różnić się pomiędzy podmiotami je oferującymi. Do podmiotów kwalifikowanych świadczących obecnie usługi certyfikacyjne należą: Enigma S.O.I. sp. z o.o., Krajowa Izba Rozliczeniowa S.A., Polska Wytwórnia Papierów Wartościowych S.A., UNIZETO Technologies S.A., EuroCert sp. o.o.
Na stronach internetowych tych podmiotów można znaleźć opłaty za poszczególne zestawy wraz z certyfikatami i okresem ich ważności. Na przykład spółka UNIZETO oferuje (zob. rys. 7).

Zestawy Centrum z certyfikatami	Na zestaw składa się:	Okres ważności 1 rok lub 2 lata
Bez czytnika 	Karta kryptograficzna cryptoCentrum Standard 3.2 bez czytnika (nie zawiera certyfikatu)	123,00 zł brutto/ 100,00 zł netto

Standard 	Klasyczne urządzenie do składania bezpiecznego podpisu elektronicznego	293,97 zł brutto/ 239.00 zł netto
Centrum Mini 	Małe, przenośne i poręczne urządzenie do składania bezpiecznego podpisu elektronicznego	306,27 zł brutto/ 249, 00 zł netto
	Zestaw do podpisu elektronicznego Standard lub Mini z dodatkowym certyfikatem ID do szyfrowania poczty	318,57 zł brutto/ 259, 00 zł netto

Rysunek 7. Zestawy do składania podpisu elektronicznego

Źródło: opracowanie własne na podstawie danych UNIZETO.

Warto wiedzieć, że odnowić można tylko te certyfikaty kwalifikowane, które są jeszcze ważne, a proces odnowienia najlepiej rozpocząć około 14 dni przed jego wygaśnięciem w celu uniknięcia dodatkowych kosztów, związanych z wydaniem nowego certyfikatu kwalifikowanego czy wymiany karty kryptograficznej. Koszt odnowienia również uzależniony jest od czasu ważności. Jeszcze w 2012 r. koszt ten na 1 rok wynosił 99 zł netto (121, 77 brutto), a na 2 lata 139 zł netto (170, 97 brutto). Powszechne Centrum Certyfikacji (PCC) w terminie 30, 14 i 7 dni wcześniej przesyła do Subskrybenta e-mail z informacją o zbliżającej się dacie wygaśnięcia certyfikatu kwalifikowanego.

PODSUMOWANIE

Wiadomo już, że stosowanie e-podpisu daje wiele korzyści w porównaniu z tradycyjnym obiegiem dokumentów: oszczędność zasobów materialnych i czasu personelu, ograniczenie ryzyka zaistnienia pomyłek, brak konieczności weryfikacji danych i wiarygodności nadawcy, a tym samym skrócenie procedur i czasu realizacji zleceń oraz możliwość szybkiego kontaktu z wybranymi korespondentami i dokonywania natychmiastowych, wiążących zmian.

Nie ulega wątpliwości, że podpis elektroniczny jest odpowiedzią na wymogi stawiane uczestnikom rynku w wirtualnej rzeczywistości XXI wieku. Struktura PKI gwarantuje nowoczesne metody zapewnienia poufności, integralności, niezaprzeczalności i uwierzytelnienia przesyłanych danych, co jednak – jak pokazuje rzeczywistość – nie przyczyniło się w ostatnim dziesięcioleciu do szybkiego rozwoju tej formy wymiany handlowej.

Niestety, zainteresowanie e-podpisem na polskim rynku nie przekłada się na ilość nabywanych certyfikatów kwalifikowanych, które jest wciąż małe, choć od momentu wprowadzenia ustawy minęło ponad 12 lat. Zgodnie z danymi statystycznymi Ministerstwa Gospodarki, aktywnych certyfikatów kwalifikowanych na wrzesień 2014 odnotowano w liczbie zaledwie 295 158 wobec liczby certyfikatów 1 008 125 wydanych od początku działalności. Liczby te stanowią zestawienie danych przekazywanych przez podmioty kwalifikowane[12]. Jakie mogą być powody spadku zainteresowania tego typu usługami?

Tak jak przed kilku laty, tak i teraz obserwuje się brak widocznego postępu w elektronicznym obrocie dokumentów, zwłaszcza w kontaktach z urzędami. Bardzo często dzieje się tak, że Zainteresowany pobierze e-formularz ze strony urzędu, wypełni go, złoży e-podpis i ponownie prześle do urzędu, otrzymując potwierdzenie odebrania go przez drugą stronę, ale to byłoby na tyle. Problem powstaje w tzw. *back office*. Sposób załatwienia sprawy zwrotnej wygląda często tak, że urzędnik sprawdzając integralność dokumentu i ważność certyfikatu w następnej kolejności, otrzymany drogą elektroniczną dokument drukuje! i wprowadza go w obieg w sposób tradycyjny. Inną przyczyną mogą być też problemy z internetową infrastrukturą sieciową. Na aspekt ten zwraca uwagę raport Ministerstwa Administracji i Cyfryzacji z 2012 r., pt. „Społeczeństwo informacyjne w liczbach". W raporcie można przeczytać: „zły stan infrastruktury internetowej, objawiający się słabym rozpowszechnieniem łączy szerokopasmowych i niską ich jakością mierzoną przepływnością, jest jednym z głównych czynników ograniczających rozwój społeczeństwa informacyjnego w Polsce"[13].

Informacje o stopniu rozpowszechnienia szybkiego internetu uzyskuje się w wyniku analizy tzw. współczynnika penetracji, wskazującego liczbę łączy szerokopasmowych przypadającą na 100 mieszkańców. Współczynnik ten wskazuje, że pozycja Polski na tle państw członkowskich UE jest bardzo słaba (za nami jest

[12] http://www.mg.gov.pl Podpis elektroniczny [dostęp: 06.10.2014].

[13] Społeczeństwo informacyjne w liczbach, Ministerstwo Administracji i Cyfryzacji, Departament Społeczeństwa Informacyjnego, Warszawa 2012, s. 12.

tylko Rumunia), a do średniej unijnej na poziomie 27% brakuje nam 11 punktów procentowych[14].

A przecież, w celu przejścia na elektroniczny obieg dokumentów, konieczne jest przetwarzanie tradycyjnych dokumentów w sposób zdigitalizowany, który ma za zadanie ułatwić, przyspieszyć i usprawnić taki obieg, a nie go powielać.

Dotychczasowe doświadczenia w obszarze elektronicznego podpisu nie są zadowalające. Pozostaje mieć nadzieję, że edukacja w obszarze elektronicznych narzędzi usprawniających pracę przyczyni się do szerszego ich wykorzystywania.

Tematyka e-podpisu nie wyczerpuje opisanego tu zagadnienia, zarówno pod kątem korzyści, jak i obaw wynikających z zastosowania zaawansowanych technologii. Kwestią otwartą (przynajmniej dla niektórych) pozostają koszty infrastruktury e-podpisu, dostęp do Internetu, szybkość jego łączy, zagrożenia cyberatakami oraz bezpośrednie nawiązanie kontaktu z partnerem czy urzędnikiem, przy czym należy pamiętać, że nie każda osoba w biznesie musi posiadać e-podpis. Co przyniesie przyszłość, to się okaże. Ważne jest, by system sprawdził się w zwykłej ludzkiej codzienności, gdyż sama idea ma przed sobą wielkie perspektywy. W naszym życiu będzie coraz więcej Internetu, a postępująca globalizacja prowadzi świat w kierunku coraz większej współpracy.

BIBLIOGRAFIA

JANOWSKI J., Elektroniczny obrót prawny, Wolters Kluwer Polska, Warszawa 2008.

KOŚCIÓŁEK A., Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym, Wolters Kluwer Polska, Warszawa 2012.

LANGE-SADZIŃSKA K., ZIEMECKA M., *Przewodnik po EDI,* Uniwersytet Łódzki, Łódź 2000.

Podpis elektroniczny – sposób działania, zastosowanie i korzyści, Ministrstwo Gospodarki, Warszawa 2005.

PRZYŁUSKA J., Świadczenie usług finansowych drogą elektroniczną, w: Innowacje na polskim rynku finansowym, red. K. Ciejpa-Znamirowski, KUL, Lublin 2004.

Społeczeństwo informacyjne w liczbach, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

Akty prawne

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

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. Nr 54, poz. 535 z późn. zm. – ostat. zm. Dz. U. 2010, Nr 257, poz. 1726).

Rozporządzenie Ministra Finansów z 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej (Dz. U. Nr 249, poz. 1661).

[14] Tamże, s. 13.

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 29 lipca 2011 r. w sprawie ogłoszenia jednolitego tekstu ustawy o podatku od towarów i usług (Dz. U. 2011, Nr 177, poz. 1054).

Rozporządzenie Ministra Finansów z 28 marca 2011 r. w sprawie zwrotu podatku niektórym podatnikom, wystawiania faktur, sposobu ich przechowywania oraz listy towarów i usług, do których nie mają zastosowania zwolnienia od podatku od towarów i usług (Dz. U. 2011, Nr 68, poz. 360).

PODPIS ELEKTRONICZNY W BIZNESIE

S t r e s z c z e n i e

W dobie globalizacji informacja jest najbardziej pożądanym źródłem wiedzy i bezcennym towarem. Dzięki opracowywaniu coraz to szybszych i skuteczniejszych sposobów przekazywania wiadomości na duże odległości, trudno nam dziś wyobrazić sobie pracę bez użycia komputerów i coraz to lepszego oprogramowania. Zawieranie umów w drodze elektronicznej odbywa się na różne sposoby – poprzez wymianę mailową, wypełnianie formularzy na stronach internetowych, wykorzystywanie baz danych, programów społecznościowych, wreszcie – po elektroniczny podpis i e-dokumentowanie. Wszystko to dzieje się za sprawą nie tylko niemal powszechnego dostępu do Internetu, ale zwłaszcza poprzez ciągłe doskonalenie sposobów szyfrowania informacji, wzrost mocy obliczeniowej procesorów i dostosowanie prawa do wymogów e-rynków.

Celem artykułu jest przybliżenie infrastruktury e-podpisu i obszarów jego zastosowania w biznesie.

Słowa kluczowe: podpis elektroniczny, infrastruktura, certyfikat kwalifikowany, klucz publiczny, klucz prywatny, obieg dokumentów.

ELECTRONIC SIGNATURE IN BUSINESS

S u m m a r y

In the era of globalization, the information is the most desirable source of knowledge and priceless commodity. With the development of ever faster and more efficient ways to communicate messages over long distances difficult for us to imagine working without the use of computers and increasingly better software. Conclusion of contracts by electronic means is carried out in various ways – through the exchange of mail, filling out forms on websites, use of databases, community programs, and finally – after the electronic signature and e-documents. All this happens not only because of nearly universal access to the Internet, but especially through continuous improvement of information encryption methods, the increase in computing power and alignment with the requirements of e-markets.

The purpose of this paper is to present e-signature infrastructure and areas of its application in business.

Key words: electronic signature, infrastructure, qualified certificate, public key, private key, workflow.

Translated by Judyta Przyłuska-Schmitt