STANISŁAWA PROĆ

Podpis cyfrowy a bezpieczeństwo gospodarki elektronicznej

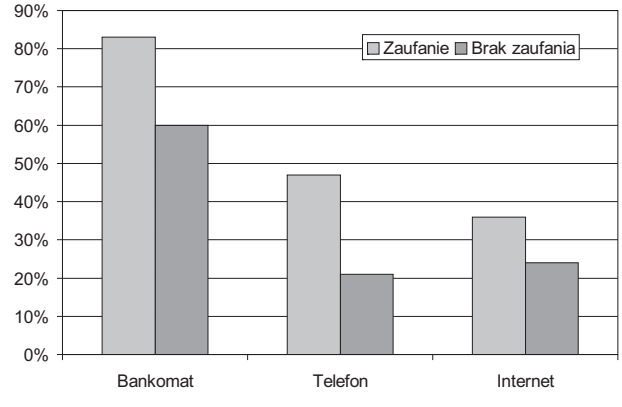
1. Wprowadzenie

Podstawą gospodarki elektronicznej jest wymiana danych poprzez sieci transmisyjne, w szczególności przez Internet. Wymiana ta powinna odbywać się w sposób całkowicie bezpieczny i nie niosący zagrożeń dla uczestników tej wymiany. Bezpieczeństwo leży u podstaw zaufania, jakim klienci obdarzają instytucje oferujące swe usługi w Internecie. Fakt istnienia bariery zaufania należy zaliczyć do najpoważniejszych czynników ograniczających rozwój gospodarki elektronicznej.

Rynek usług finansowych jest jednym z najbardziej zaawansowanych segmentów gospodarki elektronicznej i badania dla tego segmentu mogą odzwierciedlać potencjalne zachowania klientów dla całej gospodarki elektronicznej. W świetle badań prowadzonych w Polsce w roku 2000 przez Fundację Edukacji i Badań Bankowych poziom zaufania do elektronicznych kanałów dystrybucji usług finansowych kształtuje się w zależności od rodzaju medium (wykres 1).

Wykres 1

Poziom zaufania do elektronicznych kanałów dystrybucji usług finansowych



Źródło: Opracowanie własne na podstawie danych FEiBB [4].

Z badań tych wynika, że mniej niż 40% potencjalnych klientów usług finansowych ma pełne zaufanie w stosunku do transakcji wykonywanych przez Internet. Zaufanie to, bądź jego brak, często jest kształtowane przez pojawiające się w mediach informacje o spektakularnych przestępstwach dokonywanych w tym zakresie. W rzeczywistości zagrożenia bezpieczeństwa transakcji wykonywanych w Internecie, choć niebagatelne, nie uzasadniają tak wysokiego braku zaufania, skłaniają jednak do analizy sposobów ochrony danych w Internecie.

Do najistotniejszych zagrożeń, jakie niesie ze sobą transmisja danych przez sieć, należą trzy rodzaje nielegalnej działalności:

— podsłuch — informacje nie zostają zmienione, ale naruszona jest ich poufność,

— manipulacja — informacje zostają zmienione i wysłane do odbiorcy przekazu,

— podstawienie — podszywanie się pod prawowitego nadawcę w celu oszukania odbiorcy.

Zabezpieczenie internetowej transmisji danych powinno zapobiec tego rodzaju działaniom, a więc zapewnić podstawowe warunki bezpieczeństwa:

— poufność — czyli ochronę informacji przed jej poznaniem przez osoby nieuprawnione; poufność informacji może zapewnić jej zaszyfrowanie,

— niezaprzeczalność — czyli uniemożliwienie wyparcia się przez nadawcę faktu wysłania wiadomości,

— integralność — czyli ochronę przed wprowadzeniem zmian do wiadomości przez osoby nieupoważnione; do tego celu używa się podpisów elektronicznych,

— uwierzytelnianie — czyli potwierdzanie tożsamości danego użytkownika; do weryfikacji tożsamości służą certyfikaty nadawane podpisom elektronicznym.

Dwa ostatnie warunki mogą być realizowane za pomocą mechanizmu zwanego podpisem elektronicznym (cyfrowym), wykorzystującym zaawansowane techniki kryptograficzne. Podpis elektroniczny pozwala na zawieranie wszelkiego rodzaju umów i transakcji przez sieć, pod warunkiem wcześniejszego ustanowienia odpowiednich regulacji prawnych.

Podpisy cyfrowe funkcjonują już dziś, bez uregulowań prawnych. Honorowanie ich jest jednak efektem dwustronnych porozumień. Po przyjęciu stosownych przepisów każdy dokument elektroniczny, uzupełniony podpisem cyfrowym, będzie miał taką samą moc prawną jak dokument papierowy.

Brak w Polsce regulacji prawnej dla podpisu elektronicznego oznacza dziś rezygnację z wyścigu o zyski e-biznesu, a to w dobie globalizacji może się okazać barierą rozwoju całej gospodarki.

2. Podpis własnoręczny a podpis elektroniczny

Podpis własnoręczny jest podstawową formą nadawania dokumentom wiarygodności. Umożliwia on identyfikację podpisującego — zawiera bowiem jego

imię i nazwisko. Potwierdza, że podpisujący zapoznał się z dokumentem, oraz uniemożliwia wyparcie się podpisu przez autora. Możliwa jest także weryfikacja podpisu przez osobę niezależną.

Podpis elektroniczny jest mechanizmem, który nadaje wiarygodność dokumentom w formie elektronicznej, a tym samym umożliwia realizację idei, aby sieci teletransmisyjne można było traktować jako legalny instrument zawierania umów i transakcji. Musi spełniać te same warunki co podpis własnoręczny, tzn. musi umożliwiać stwierdzenie, że dokument pochodzi od określonej osoby oraz że nie został sfałszowany.

Na podpis elektroniczny składa się ciąg bitów przygotowany odpowiednią metodą i dodawany do dokumentu elektronicznego. Podpis ten zależy od treści dokumentu i tożsamości podpisującego.

Podpis elektroniczny posiada przewagę nad jego wersją odręczną przejawiającą się w tym, że w podpisy elektroniczne mogą być zaopatrywane, oprócz osób prywatnych — organizacje, komórki organizacyjne, ale też systemy informatyczne, które wymieniają ze sobą informacje w sposób półautomatyczny w rozwiązaniach *business to business*. Kolejną zaletą jest łatwość weryfikacji podpisu elektronicznego. W przypadku podpisu odręcznego ostateczna weryfikacja może zostać przeprowadzona przez biegłego specjalistę. Weryfikacji podpisu elektronicznego może dokonać każdy za pomocą względnie prostego oprogramowania, które oddziela dokumenty elektroniczne fałszywe od prawdziwych i alarmuje jedynie o próbach nadużyć.

Podpis elektroniczny nie ma jeszcze w Polsce obowiązującej mocy prawnej. Przewiduje się, że dopiero w lipcu 2001 r. wejdzie w życie ustawa o podpisie elektronicznym. Od tego momentu podpis elektroniczny będzie miał taką samą moc prawną jak jego odręczny odpowiednik.

3. Podpis cyfrowy i jego atrybuty

Przygotowywany obecnie w Polsce projekt ustawy o podpisie elektronicznym ma za zadanie prawne usankcjonowanie podpisu elektronicznego oraz dokumentu elektronicznego.

Potrzebę stworzenia ram prawnych dla dokonywania obrotu gospodarczego poprzez sieci teleinformatyczne dostrzeżono już wcześniej w wielu rozwiniętych gospodarczo krajach. Poszczególne państwa europejskie wprowadziły już instytucję podpisu elektronicznego do swoich systemów prawnych. Najwcześniej zrobiły to Niemcy — już 22 lipca 1997 r., ale również Austria, Wielka Brytania, Czechy, Estonia, Szwajcaria, Belgia i Holandia. W odpowiedzi na te wewnętrzne procesy Unia Europejska wydała dyrektywę Rady i Parlamentu Europejskiego z 13 grudnia 1999 r. (nr 1999/93/EC). Celem dyrektywy jest standaryzacja rozwiązań stosowanych przez poszczególne państwa członkowskie Unii. Polski projekt ustawy

o podpisie elektronicznym oparty jest na rozwiązaniach zastosowanych w tej dyrektywie.

Według wyżej wspomnianej dyrektywy podpis elektroniczny to:

„dane w formie elektronicznej, dołączone lub logicznie powiązane z danymi zawartymi w dokumencie elektronicznym, które służą do uprawdopodobnienia tożsamości podpisującego" [3].

Jednakże tak zdefiniowany podpis elektroniczny nie jest, w świetle tej dyrektywy, równoprawny z podpisem własnoręcznym. Podpis własnoręczny jest równoważny tylko z tzw. zaawansowanym podpisem elektronicznym. Zaawansowany podpis elektroniczny to podpis elektroniczny, który spełnia następujące wymagania:

— jest niepowtarzalnie powiązany z podpisującym,

— umożliwia identyfikację podpisującego,

— jest powiązany z danymi, do których się odnosi, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest możliwa do wykrycia,

— jest tworzony za pomocą urządzeń i metod pozostających pod wyłączną kontrolą podpisującego.

Inną definicję prezentuje Polska Norma PN-I-02000. Wg tej definicji podpis elektroniczny to:

„przekształcenie kryptograficzne danych umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę".

Z powyższych definicji można wyłonić niezbędne atrybuty podpisu cyfrowego:

— możliwość zidentyfikowania nadawcy przez odbiorcę (uwierzytelnianie, autentyfikacja),

— zapewnienie wykrywalności wszelkich zmian w dokumencie (integralność, spójność),

— uniemożliwienie wyparcia się podpisu przez autora (niezaprzeczalność),

— umożliwienie weryfikacji podpisu przez osobę niezależną.

Atrybuty podpisu cyfrowego stanowią o tym, że zaawansowany podpis elektroniczny zapewnia wiarygodność dokumentów elektronicznych analogicznie, jak podpis odręczny zapewnia wiarygodność dokumentów tradycyjnych.

4. Szyfrowanie danych

Idea podpisu elektronicznego wymaga zastosowania metod opartych na procedurach kryptograficznych, które umożliwiają przesłanie informacji w postaci zaszyfrowanej, nieczytelnej dla osób postronnych. Dzięki najnowszym technologiom informacja może być szyfrowana w chwili wysyłania przez sieć i rozszyfrowywana podczas odbierania, pokonując całą drogę w sieci w postaci niemożliwej do odczytania.

Szyfrowanie jest procesem, w którym wiadomość (tekst jawny) jest prze-

kształcana w inną wiadomość (tekst zaszyfrowany) za pomocą algorytmu szyfrowania (odpowiedniej funkcji matematycznej) oraz hasła szyfrowania (zwanego kluczem).

Wszystkie metody szyfrowania mają wspólne elementy:

— Algorytm szyfrowania

Algorytm szyfrowania stanowi funkcję, najczęściej o silnej podbudowie matematycznej, która wykonuje zadanie szyfrowania i deszyfrowania danych.

— Klucze szyfrowania

Klucze szyfrowania są używane przez algorytm szyfrowania do określenia sposobu szyfrowania lub deszyfrowania danych. Algorytm szyfrujący używa klucza do przekształcenia tekstu jawnego w kryptogram, zaś program deszyfrujący używa klucza do przekształcenia kryptogramu w tekst jawny.

— Długość klucza

Klucze kryptograficzne mają postać ciągu znaków w zapisie binarnym. Ilość tych znaków określa długość klucza. Im dłuższy klucz, tym trudniej złamać szyfr.

Współczesne metody szyfrowania opierają się na zastosowaniu odpowiedniego algorytmu szyfrowania wraz z kluczem szyfrującym. Odbiorca informacji odszyfrowuje tekst do postaci tekstu jawnego, za pomocą klucza deszyfrującego i algorytmu deszyfrującego.

W najnowszej kryptografii możliwość utrzymania informacji w tajemnicy oparta jest nie na algorytmie, który zwykle jest szeroko znany, ale na liczbie zwanej kluczem kryptograficznym, która jest niezbędna zarówno do zaszyfrowania wiadomości, jak i do odkodowania informacji zaszyfrowanej.

Istnieją dwa podstawowe typy metod szyfrowania:

— Szyfrowanie z kluczem tajnym, w którym tego samego klucza używa się do szyfrowania i deszyfrowania. Nazywane jest też szyfrowaniem symetrycznym.

— Szyfrowanie z kluczem publicznym, które wymaga posiadania pary kluczy: klucza publicznego i klucza prywatnego. Klucza publicznego używa się do zaszyfrowania wiadomości, a klucza prywatnego do jej odszyfrowania. Nazywane jest też szyfrowaniem asymetrycznym. Tylko klucz prywatny musi pozostać tajny. Drugi może być przesyłany bez zachowania środków bezpieczeństwa. Informacja zaszyfrowana jednym kluczem z pary może być odszyfrowana tylko drugim, pasującym kluczem.

Szyfrowanie z kluczem publicznym jest stosowane do tworzenia podpisów elektronicznych.

5. Tworzenie i weryfikacja podpisu cyfrowego

W szyfrowaniu asymetrycznym stosuje się szyfrowanie kluczem publicznym i deszyfrację kluczem prywatnym, ale jest możliwy także proces odwrotny. Dane zaszyfrowane kluczem prywatnym można odszyfrować tylko za pomocą pa-

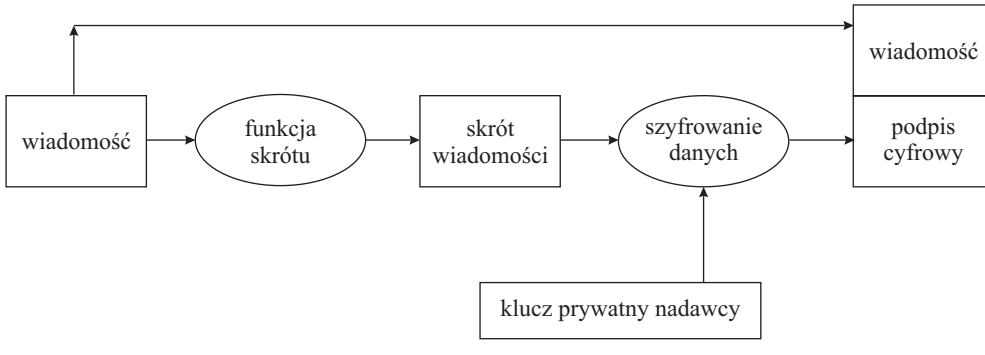
sującego klucza publicznego. Ten drugi sposób jest stosowany do kodowania i dekodowania podpisu cyfrowego

Nadawca informacji musi wygenerować parę kluczy: publiczny i prywatny. Oba klucze: publiczny i prywatny są losowymi ciągami cyfr i należą tylko do jednego właściciela. Klucz prywatny znany jest tylko właścicielowi i jego poufność jest podstawowym warunkiem bezpieczeństwa podpisu. Klucz publiczny przekazywany jest odbiorcy informacji dowolnym kanałem komunikacyjnym. Nadawca informacji koduje ją za pomocą swojego klucza prywatnego. Odbiorca dekoduje wiadomość za pomocą klucza publicznego nadawcy i może mieć pewność, że wiadomość pochodzi od danego autora, gdyż tylko on jest posiadaczem klucza prywatnego z danej pary kluczy. W ten sposób podpis cyfrowy zapewnia identyfikację nadawcy i niezaprzeczalność przesyłanej informacji.

W praktyce za pomocą klucza prywatnego nadawca nie szyfruje całej wiadomości, lecz tylko tzw. skrót wiadomości (kryptograficzna suma kontrolna).

Wykres 2

Generowanie podpisu cyfrowego



Skrót wiadomości tworzony jest z przesyłanej informacji za pomocą przekształcenia matematycznego zwanego jednokierunkową funkcją skrótu. Funkcja ta przypisuje przesyłanej informacji liczbę, zwaną skrótem, o określonej długości i następujących cechach:

— wartość skrótu jest unikalna dla przekształcanych danych,

— na podstawie skrótu nie można odtworzyć zawartości danych przekształcanych.

Dopiero tak utworzony skrót jest szyfrowany za pomocą klucza prywatnego nadawcy i wynik tego szyfrowania stanowi podpis elektroniczny. Procedura tworzenia podpisu cyfrowego sprawia, że podpis ten wygląda za każdym razem inaczej (w zależności od treści wiadomości). Tak utworzony podpis dołączany jest do dokumentu elektronicznego.

Generowanie podpisu cyfrowego przebiega następująco:

— wprowadzanie wiadomości w postaci jawnej,

— tworzenie skrótu wiadomości za pomocą jednokierunkowej funkcji skrótu, która ma tę właściwość, że z uzyskanego skrótu nie da się odtworzyć całej wiadomości; w zależności od konkretnie zastosowanego algorytmu otrzymany skrót ma 128 lub160 bitów,

— szyfrowanie skrótu wiadomości za pomocą klucza prywatnego nadawcy wiadomości, co w rezultacie tworzy podpis elektroniczny,

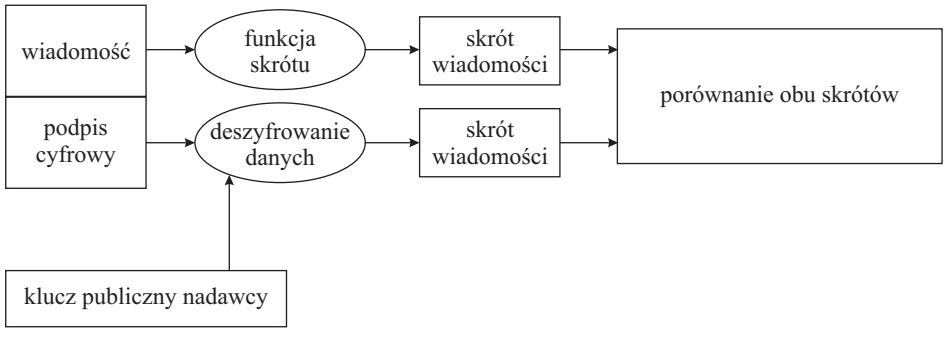
— dołączanie podpisu do wysyłanej wiadomości,

— transmisja wiadomości wraz z podpisem do odbiorcy dokumentu.

Dla sprawdzenia, czy dane nie zostały zmodyfikowane w trakcie transmisji, odbiorca wiadomości dekoduje podpis elektroniczny za pomocą klucza publicznego nadawcy, uzyskując w efekcie skrót odebranej wiadomości. Następnie z odebranej wraz z podpisem wiadomości, za pomocą tej samej jednokierunkowej funkcji skrótu, oblicza skrót otrzymanej wiadomości i porównuje tak uzyskane skróty. Jeżeli skróty są jednakowe, to oznacza, że została zachowana integralność przesłanej wiadomości.

Wykres 3

Weryfikacja podpisu cyfrowego



Weryfikacja podpisu cyfrowego przebiega następująco:

— odbiorca wiadomości deszyfruje podpis elektroniczny za pomocą klucza publicznego nadawcy i otrzymuje skrót wiadomości,

— odbiorca z otrzymanej wiadomości za pomocą tego samego algorytmu co nadawca (jednokierunkowej funkcji skrótu) tworzy skrót wiadomości,

— porównanie obu skrótów,

— jeżeli są jednakowe, to dane nie zostały zmodyfikowane w trakcie transmisji.

6. Certyfikacja kluczy kryptograficznych

Opisany mechanizm realizacji podpisu elektronicznego zapewnia identyfikację i niezaprzeczalność nadawcy oraz integralność danych. Dla zachowania pełnego

bezpieczeństwa konieczne jest jeszcze uwierzytelnienie nadawcy informacji, czyli potwierdzenie tożsamości. Odbiorca musi mieć pewność, że klucz publiczny, z którego korzysta, jest kluczem nadawcy, a nie osoby trzeciej, która rozpowszechniła fałszywy klucz, by w ten sposób wprowadzić do sieci fałszywe dokumenty.

Rozwiązaniem problemu uwierzytelniania nadawcy jest wprowadzenie tzw. zaufanej trzeciej strony, która będzie wydawała elektroniczne certyfikaty potwierdzające autentyczność danego klucza publicznego. Certyfikat ten to:

„elektroniczne potwierdzenie, które łączy dane weryfikujące podpis z osobą i potwierdza tożsamość tej osoby" [3].

Najbardziej znany i akceptowany format certyfikatu zdefiniowany jest przez międzynarodowy standard **X.509** i zawiera:

— klucz publiczny należący do certyfikowanej jednostki,
— nazwę właściciela,
— datę ważności klucza,
— nazwę organu certyfikującego,
— numer seryjny certyfikatu,
— podpis elektroniczny organu certyfikującego.

Certyfikat łączy dany klucz publiczny z nazwą certyfikowanej jednostki. Certyfikaty mają zapobiec wystawianiu fałszywych kluczy publicznych w celu podszywania się pod kogoś innego. W ten sposób wystawca certyfikatu swoim podpisem elektronicznym potwierdza tożsamość właściciela klucza umieszczonego w certyfikacie. Przed wystawieniem certyfikatu organ certyfikujący weryfikuje dane o certyfikowanej jednostce. Wystawcy certyfikatów powinni być instytucjami zaufania publicznego, dysponującymi odpowiednią infrastrukturą teleinformatyczną.

Unia Europejska w swojej dyrektywie [3] wprowadza pojęcie certyfikatu zwykłego i kwalifikowanego. Certyfikat kwalifikowany jest niezbędny, aby można używać podpisu cyfrowego w kontaktach z organami państwowymi. Certyfikat kwalifikowany może być wydawany tylko przez urzędy certyfikacyjne akredytowane przez odpowiedni organ państwowy. Muszą one oprócz certyfikowanego klucza publicznego zawierać:

— wskazanie, że certyfikat został wydany jako kwalifikowany,
— dane świadczącego usługi certyfikacyjne, w tym również państwo jego siedziby,
— nazwisko lub pseudonim podpisującego,
— załączenie specyficznej cechy podpisującego, jeżeli jest to konieczne w związku z celem, któremu ma służyć certyfikat,
— dane umożliwiające potwierdzenie tożsamości podpisującego (dane weryfikujące podpis),
— wskazanie daty wydania oraz ostatniego dnia ważności certyfikatu,
— indywidualny kod identyfikacyjny certyfikatu,

— zaawansowany podpis urzędu certyfikacyjnego, który wydał ten certyfikat,
— ograniczenia zakresu użycia certyfikatu, jeżeli takie istnieją,
— maksymalną wysokość transakcji, do których certyfikat ma być używany, jeżeli urząd certyfikacyjny takie ograniczenie wprowadzi.

Wystawcy certyfikatów umożliwiają komunikującym się stronom m.in. automatyczne sprawdzenie ważności certyfikatów, a tym samym potwierdzenie autentyczności właściciela certyfikatu.

Organy certyfikacyjne (których może być wiele) wraz z organami nadzorującymi je tworzą uniwersalną, hierarchiczną strukturę instytucji certyfikujących tzw. infrastrukturę klucza publicznego.

7. Uwagi końcowe

Opisany mechanizm tworzenia i weryfikacji podpisu elektronicznego oraz infrastruktura certyfikacji kluczy kryptograficznych to podstawowe czynniki wpływające na poziom bezpieczeństwa internetowej transmisji danych. Podniesienie poziomu bezpieczeństwa tej transmisji przyczyni się do usunięcia jednej z ważniejszych barier rozwoju gospodarki elektronicznej. Dyrektywa Unii Europejskiej dotycząca podpisu elektronicznego ma zostać wprowadzona przez państwa członkowskie do 19 lipca 2001 r. W perspektywie przystąpienia naszego kraju do Unii Europejskiej wydaje się bezwzględnie konieczne stworzenie warunków prawnych i organizacyjnych dla gospodarki elektronicznej, zgodnych ze standardami europejskimi.

Bibliografia

[1] Deptuła T., *Internet z autografem*, Home&market, 9/2000.

[2] Garfinkel S., Spafford G., *Bezpieczeństwo w Unixie i w Internecie*,Wyd. RM, Warszawa 1997.

[3] *Dyrektywa Komisji Europejskiej w sprawie ram wspólnotowych dla podpisu elektronicznego. Komentarz*, Biuletyn Związku Banków Polskich, 4/2000 http://www.zbp/biuletyn.htm

[4] Karpiński P., *Szanse bankowości elektronicznej*, Bank 10/2000.

[5] Kubiak M., *Zastosowanie klucza publicznego PKI w zabezpieczeniu wymiany danych pomiędzy bankami*, Biuletyn Bankowy 6/1999.

[6] Nowakowski M., *Protokół SSL. Zabezpieczenie internetowej transmisji danych — perspektywy rozwoju,* Biuletyn Bankowy 12/1999.