

Jarosław Zajac*

ZASTOSOWANIE PODPISU ELEKTRONICZNEGO W SYSTEMACH BANKOWYCH

Artykuł przedstawia sfery zastosowania infrastruktury klucza publicznego i podpisu elektronicznego w systemach bankowych oraz wpływ jaki wywarło na systemy bankowe wprowadzenie Ustawy o podpisie elektronicznym. W artykule zawarte są podstawowe informacje o strukturach systemów bankowych oraz o tendencji ich rozwoju. Na tym tle przedstawiono możliwości i korzyści zastosowania podpisu elektronicznego.

This article presents areas of possible implementations of the PKI (Public Key Infrastructure) and an electronic signature in banking systems. An impact of the law stated in that field in banking systems is discussed. The article includes basic information about the structure of banking systems and trend in their development. On that background possibilities and advantages of the electronic signature implementation are presented.

Wstęp

Wzrost konkurencyjności w sferze bankowości wymaga od banków oferowania klientom coraz bardziej urozmaiconych produktów bankowych, spełniających ich indywidualne potrzeby. Klienci aby móc w pełni skorzystać z oferty banków muszą mieć umożliwiony dostęp do swych rachunków w każdej chwili i w każdym miejscu. Aby sprostać temu zadaniu systemy bankowe muszą spełniać przynajmniej dwa założenia:

- należy umożliwić klientom dostęp do rachunków poprzez internet i/lub z wykorzystaniem telefonów przenośnych (mobile banking);
- rachunki muszą być odmiejscowione, najlepiej poprzez pełną centralizację.

Łatwy dostęp do rachunków oraz ich odmiejscowienie i centralizacja systemów bankowych wymaga stosowania odpowiednich narzędzi służących do

* Zakład Informatyki Ekonomicznej, Uniwersytet Łódzki

ochrony rachunków przez niepowołanym dostępem oraz uwierzytelniania transakcji dokonywanych przez klientów i operacji realizowanych przez operatorów systemów bankowych.

W artykule przedstawiam możliwości zastosowania narzędzi kryptograficznych oraz podpisu elektronicznego w celu sprostania wymienionym wyżej zadaniom stawianym przed systemami bankowymi..

PKI i podpis elektroniczny

Od 16 sierpnia 2002 roku obowiązuje w Polsce Ustawa o podpisie elektronicznym, sankcjonująca podpis elektroniczny na równi z podpisem ręcznym. Ustawa ta wraz z aktami wykonawczymi określa:

- warunki stosowania podpisu elektronicznego,
- skutki prawne jego stosowania,
- zasady świadczenia usług certyfikacyjnych,
- zasady nadzoru nad podmiotami świadczącymi te usługi,
- szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych,
- podstawowe wymagania dotyczące polityki certyfikacji dla kwalifikowanych certyfikatów,
- szczegółowe warunki techniczne i organizacyjne, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne.

Przedstawione wyżej regulacje określają zasady stosowania infrastruktury klucza publicznego – PKI (ang. *Public Key Infrastructure*)

Infrastruktura klucza publicznego jest to zbiór sprzętu, oprogramowania, reguł oraz procedur niezbędnych do tworzenia, zarządzania, przechowywania i dystrybucji certyfikatów opartych na kryptografii z kluczem publicznym.

PKI składa się zazwyczaj z pięciu podstawowych komponentów:

- CA (*Certification Authorities* – wydawcy certyfikatów), przydzielających i odbierających certyfikaty;
- ORA (*Organizational Registration Authorities* - ciała organizacyjnego rejestracji) poręczającego za powiązania pomiędzy kluczami publicznymi, tożsamością posiadaczy certyfikatów oraz innymi atrybutami;
- Posiadaczy certyfikatów, którym wydawane są certyfikaty i którzy mogą podpisywać dokumenty cyfrowe;

- Klientów, którzy zatwierdzają cyfrowe podpisy oraz ich ścieżki certyfikowania prowadzące od znanych publicznych kluczy zaufanych CA;
- Katalogów przechowujących i udostępniających certyfikaty oraz listy certyfikatów unieważnionych (CRL – *Certificate Revocation List*).

Podstawowe elementy i funkcje PKI są następujące.

- Serwer certyfikatów – platforma do generowania, obsługi i zarządzania certyfikatami i łączenia ich z odpowiednimi kluczami publicznymi – zarówno dla podpisów, jak i szyfrowania danych. Wykonuje on także – na żądanie lub w regularnych odstępach czasu – odnawianie certyfikatów.
- Katalog – repozytorium wszystkich informacji publicznych dotyczących PKI, w tym certyfikatów kluczy publicznych, CRL, ARL, certyfikaty wydawców certyfikatów (CA) itp.
- System odwołań – możliwość odwoływania klucza w celu uniemożliwienia dostępu do szyfrowania i funkcji podpisu użytkownikom pozbawionym tego prawa (np. z powodu zmiany funkcji w organizacji lub zmiany miejsca pracy).
- Oprogramowanie po stronie klienta – jeżeli wszystkie powyższe funkcje są w pełni implementowane przez PKI, to do ich wykorzystania niezbędny jest interfejs po stronie klienta - na PC. Oprogramowanie to może mieć formę specjalnego klienta PKI, dostarczanego przez dostawcę usług PKI lub różnego rodzaju aplikacje obsługujących PKI, takich jak przeglądarki czy klient poczty elektronicznej.

Funkcje rozwiniętych systemów PKI są następujące.

- Generowanie kluczy;
- Rejestracja – proces, za pomocą którego dana jednostka przedstawia się CA – bezpośrednio lub za pośrednictwem Urzędu Rejestracji (*Registration Authority* – RA), zanim CA wyda jej certyfikat lub certyfikaty;
- Uaktualnienie kluczy;
- Historia kluczy;
- Składowanie i odtwarzanie kluczy;
- Obsługa cechy niezaprzeczalności;
- Certyfikowanie przechodnie (*cross-certification*).

Stan prac legislacyjnych nad podpisem elektronicznym i PKI w Polsce

Najważniejszym aktem prawnym regulującym możliwość i warunki stosowania podpisu elektronicznego jest Ustawa o podpisie elektronicznym, która ukazała się w Dz. U. Z 2001 r., Nr 130, poz. 1450.

Oprócz w/w ustawy ukazało się również kilka aktów wykonawczych, precyzujących zapisy ustawowe. Do najważniejszych należą następujące:

Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 roku w sprawie określania warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego, Dz. U. z 2002 roku Nr 128, poz. 1094.

Rozporządzenie Ministra Gospodarki w sprawie określania szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym.

Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 roku w sprawie określania zasad wynagradzania za przeprowadzanie kontroli podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.

Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 roku w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.

Rozporządzenie Ministra Finansów z 8 sierpnia 2002 roku w sprawie sposobu i szczegółowych warunków spełniania obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot.

Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 roku w sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru.

Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 roku w sprawie wysokości opłat za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.

Systemy informatyczne w bankowości

Podstawowym kryterium stawianym przed systemami informatycznymi stosowanymi w sferze bankowości jest ułatwienie klientom dostępu do rachunków. Systemy bankowe powinny być „zorientowane na klienta” oznacza to, że klienta należy obsłużyć w jak najkrótszym czasie oraz że, powinien on mieć możliwość dostępu do rachunku w dowolnym oddziale banku. Ponadto powinna być zapewniona klientowi możliwość wykonywania operacji bankowych bez konieczności udawania się do banku – poprzez wdrożenie systemu bankowości elektronicznej.

Mając powyższe na uwadze można dokonać następującego podziału bankowych systemów informatycznych:

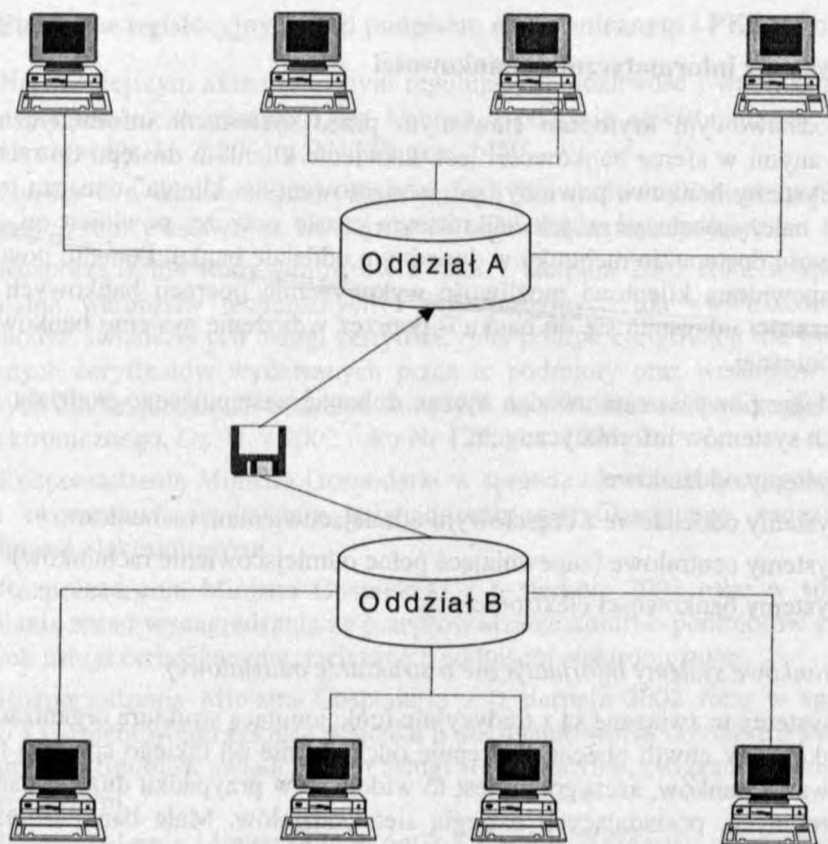
- systemy oddziałowe,
- systemy oddziałowe z częściowym odmiejszczeniem rachunków
- systemy centralowe (zapewniające pełne odmiejszczenie rachunków)
- systemy bankowości elektronicznej.

Bankowe systemy informatyczne o strukturze oddziałowej

Systemy te związane są z tradycyjnie funkcjonującą strukturą organizacyjną w bankach. W chwili obecnej następuje odchodzenie od takiego sposobu funkcjonowania banków, szczególnie jest to widoczne w przypadku dużych banków komercyjnych, posiadających rozległą sieć oddziałów. Małe banki o zasięgu regionalnym, np. banki spółdzielcze jeszcze rzadko decydują się na centralizację, co związane jest m.in. ze stosunkowo dużym kosztem takiej operacji oraz specyfiką ich funkcjonowania (klienci tych banków z reguły nie mają potrzeby dokonywania operacji bankowych poza miejscem zamieszkania).

W systemach bankowych o strukturze oddziałowej rachunki bankowe zgromadzone są w oddziałach i nie ma do nich bezpośredniego dostępu z innych oddziałów banku. W tego typu systemach bazy danych z rachunkami podzielone są na oddziały i umiejscowione w oddziałach. Każdy oddział prowadzi własną księgę główną. Okresowo następuje konsolidacja księgi głównej lub konsolidacja na poziomie sprawozdań. Wymiana danych między oddziałami odbywa się poprzez Rozliczenia Międzyoddziałowe, często za pośrednictwem centrali banku.

Poniższy schemat przedstawia przykładową budowę systemu oddziałowego.



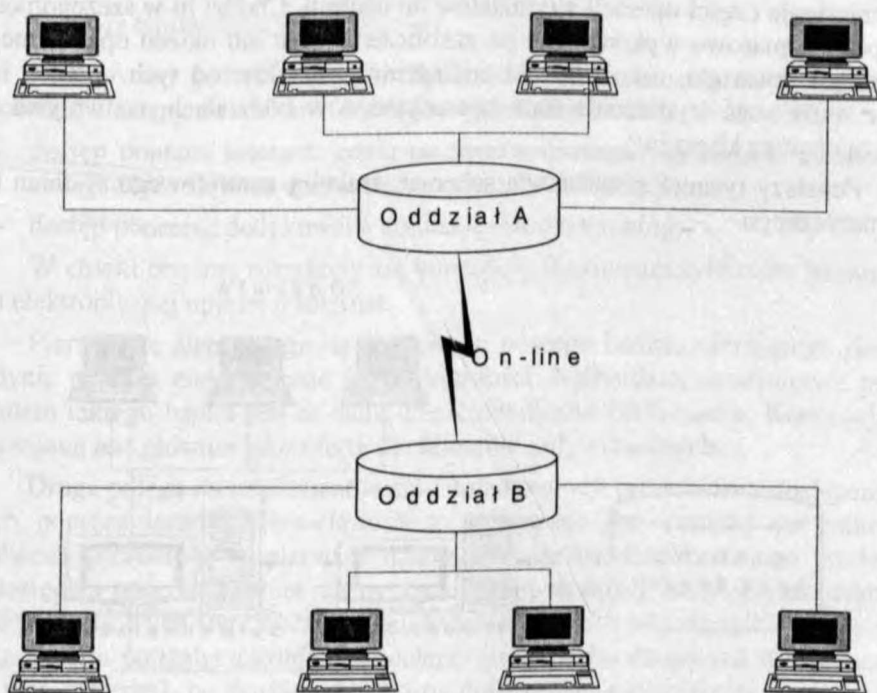
Rys. 1. Struktura systemu oddziałowej,
Źródło: opracowanie własne

Bankowe systemy informatyczne o strukturze oddziałowej z częściowym odmiejszczeniem rachunków

Często w okresie przejściowym między stosowaniem struktury oddziałowej a przejściem na strukturę centralową banki dokonują połączenia on-line między oddziałami. Rozwiązanie takie pozwalana klientom na wykonywanie niektórych operacji na rachunkach niezależnie od oddziału, w jakim znajduje się rachunek. Obarczone ono jest jednak pewnymi ograniczeniami:

- w przypadku braku połączenia z oddziałem, w którym znajduje się rachunek wykonanie operacji na tym rachunku nie będzie możliwe,

- nie wszystkie operacje można zrealizować on-line, np. zlecenia stałe mogą być przyjmowane w dowolnym oddziale, lecz dokumenty muszą być przesłane do oddziału macierzystego i dopiero tam zlecenie zostanie wykonane (często z datą waluty realizacji w oddziale macierzystym).



Rys. 2. Struktura systemu oddziałowego z częściowym odmiejszczeniem rachunków, źródło: opracowanie własne

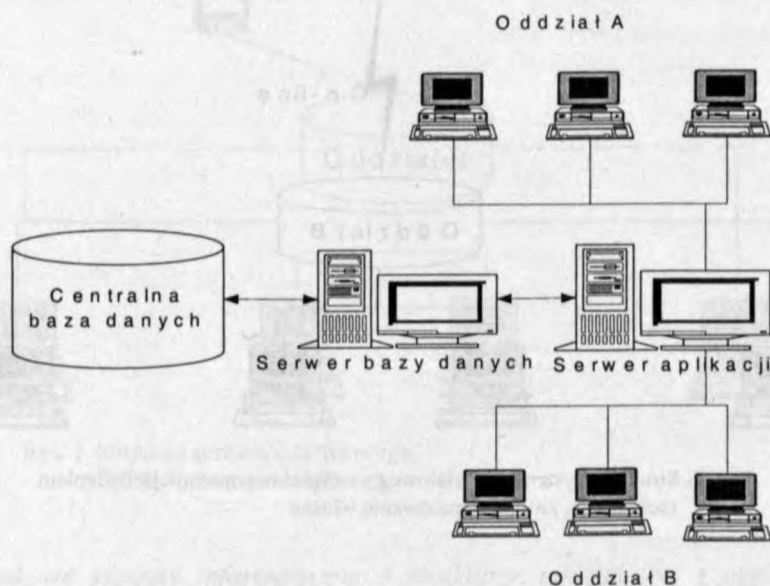
Bankowe systemy informatyczne o strukturze centralowej

Centralizacja systemów informatycznych pozwala na pełne odmiejszczenie rachunków. Przy tego typu strukturze baza danych ze wszystkimi rachunkami znajduje się w centrali banku lub wyznaczonym oddziale. Wszystkie jednostki operacyjne banku połączone są drogą elektroniczną z serwerem centralnej bazy danych, przez co umożliwiony jest stały dostęp do każdego rachunku. Rozwiązanie takie wymaga jednak odpowiedniego zabezpieczenia stałości połączenia między komputerem znajdującym się w oddziale a serwerem bazy danych. Aby zapobiec problemom z połączeniem należy tworzyć zastępcze środki komunikacji (np. łączność radiową) oraz tak projektować sieć połączeń aby

umożliwione było połączenie między oddziałem a centralą za pośrednictwem innego oddziału. Rozwiązanie to wymaga ponadto stworzenia właściwej polityki uprawnień dostępu do elementów systemu.

Zastosowanie centralizacji systemów informatycznych w banku pozwala na przeniesienie części operacji z oddziałów do centrali. Chodzi tu w szczególności o operacje masowo wykonywane na zakończenie dnia lub okresu operacyjnego (miesiąca, kwartału, roku). Dzięki odciążeniu oddziałów od tych operacji istnieje możliwość wydłużenia dnia operacyjnego w oddziałach, co wpływa na lepszą obsługę klientów.

Poniższy rysunek przedstawia schemat struktury centralowego systemu informatycznego.



Rys. 3. Struktura systemu centralowego, źródło: opracowanie własne

W praktyce stosuje się jeszcze inne sposoby centralizacji i/lub odmiejszczenia rachunków. Najpopularniejszym jest replikowanie bazy danych. Oddziały nie są połączone ze sobą bezpośrednio, lecz w centrali znajduje się baza danych stanowiąca skonsolidowaną bazę danych tworzoną poprzez replikacje baz oddziałowych. Rozwiązanie takie pozwala na przechowywanie w jednym miejscu danych ze wszystkich oddziałów, co usprawnia dokonywanie sprawozdawczości dla całego banku. Nie pozwala ono jednak na odmiejszczenie ra-

chunku. Dane w centrali są aktualne na koniec poprzedniego dnia i mogą być wykorzystywane do wykonywania bieżących operacji na rachunkach. Często banki łączą rozwiązanie oddziałowe z częściowym odmiejszczeniem rachunków wraz z replikacją baz danych.

Systemy bankowości elektronicznej

Podstawowy podział systemów bankowości elektronicznej związany jest ze sposobem dostępu do rachunków bankowych, który może być następujący:

- dostęp poprzez internet, gdzie na stronie internetowej istnieje możliwość zalogowania się oraz dokonania operacji na rachunku;
- dostęp poprzez dedykowaną aplikację (Home banking).

W chwili obecnej rozwinęły się koncepcje stosowania systemów bankowości elektronicznej opartej o internet.

Pierwsza z nich polega na stworzeniu nowego banku, oferującego dostęp jedynie poprzez elektroniczne środki łączności. Najbardziej rozwiniętym przykładem takiego banku jest m-bank, część detaliczna BRE banku. Koncepcja ta rozwijana jest głównie jako oferta dla klientów indywidualnych.

Druga polega na implementowaniu pojedynczych produktów z dostępem do nich poprzez internet. Rozwiązanie to stosowane jest częściej co najmniej z dwóch powodów: po pierwsze tańsze jest wprowadzanie nowego produktu z dostępem poprzez internet niż tworzenie całej struktury bankowej dla oddziałów internetowych (wprawdzie oddziały takiego banku istnieją tylko wirtualnie, lecz istnieje potrzeba zatrudnienia całego sztabu ludzi dbających o utrzymanie takiego systemu), po drugie pozwala na dołączenie „e-produktów bankowych” do pełnej oferty banku.

Podpis elektroniczny i kryptografia klucza publicznego w bankowości

Obecnie stosowane sposoby ochrony rachunków i procesów bankowych

Przed wprowadzeniem Ustawy o podpisie elektronicznym instytucje finansowe udostępniały klientom dostęp do rachunków drogą elektroniczną, stosując różnego rodzaju zabezpieczenia rachunków bankowych przed niepowołanym dostępem. Do najpopularniejszych rozwiązań należą: hasła jednorazowe, tokeny.

Tokeny

Są to urządzenia zabezpieczone PINem, które potrafią generować jednorazowe hasło i podpisy elektroniczne. Oparte są zwykle na algorytmie DES

i 3DES. Użytkownik nie musi martwić się o hasło - jest ono generowane automatycznie i w dodatku w sposób nie pozwalający na jego złamanie.

Pierwszym zabezpieczeniem jest PIN, który uruchamia token. Nawet jeżeli ktoś ukradnie nam urządzenie i tak nie będzie mógł go użyć. Po trzech nieudanych próbach podania PINu token przestaje reagować i przechodzi w stan zablokowania. Urządzenie można odblokować zdalnie, wystarczy zadzwonić lub udać się do operatora i na podstawie identyfikacji użytkownika, dostarczany jest numer do odblokowania (dla każdego urządzenia i w każdej chwili czasu inny). Następnie użytkownik może wprowadzić nowy PIN - zna go tylko właściciel tokena.

Po podaniu PIN'u urządzenie jest gotowe do pracy. Na podstawie wielu zmiennych (czas, klucz DES, dodatkowy klucz) generuje kod, który po wpisaniu do formularza sprawdzany jest po stronie serwera w bazie danych. Na serwerze również według tej samej procedury następuje wygenerowanie hasła dla konkretnego loginu (identyfikatora) i hasła są porównywane. Jeżeli hasła są takie same, następuje udostępnienie zasobów dla użytkownika, jeżeli są inne - dostęp nie jest możliwy. Hasło jest jednorazowe, nie można podać po raz kolejny tego samego hasła. Zmienia się ono w czasie i nawet jeżeli ktoś podejrzy jakie informacje wpisujemy, nie będzie miał z tego żadnego pożytku.

Używanie tokena może być limitowane w czasie i w ilości użyć. Można zaprogramować do trzech kluczy DES. Zadanie do wygenerowania hasła może być odczytane z ekranu komputera bez konieczności wprowadzania go z klawiatury (16 znaków). Odpowiedź może być wyświetlana w postaci dziesiętnej lub szesnastkowej. Token ma również możliwość użycia pytania i odpowiedzi (challenge/response). Może również służyć do generowania elektronicznych podpisów.

Sfery stosowania podpisu elektronicznego i systemów kryptograficznych w bankowości

Możliwości rozwoju usług i produktów bankowych

Stosowanie metod kryptograficznych w połączeniu z podpisem elektronicznym w sposób oczywisty chroni rachunki bankowe przed niepowołanym dostępem, pozwalając bankom na rozwinięcie oferty e-bankingu. Każdy klient deklarujący chęć stosowania podpisu elektronicznego w kontaktach z bankiem musi zostać zaopatrzony w stosowny podpis. Autoryzacja klienta może być realizowana, co najmniej w dwojaki sposób.

- Dostęp poza siedzibą banku: użytkownik musi być zaopatrzony w generator podpisu, np. urządzenie typu token lub generator programowy dostarczany

klientowi wraz z aplikacją wydana przez bank w ramach umowy o stosowanie podpisu elektronicznego. Powinien być zarejestrowany w banku w formie stosownej umowy. W umowie takiej bank zobowiązuje się do umożliwienia klientowi dostępu do rachunku na podstawie podpisu elektronicznego, wydając jednocześnie urządzenie lub program do generowania podpisu. Elementem takiej umowy musi być jednocześnie zobowiązanie się klienta do nieprzekazywania generatora podpisu osobom trzecim.

- Dostęp w siedzibie banku – klient zaopatrzony jest w kartę dostępu (np. chip'ową), generującą podpis elektroniczny. W banku musi znajdować się urządzenie potrafiące odczytać podpis elektroniczny. Uruchomienie systemu powinno być poprzedzone podaniem unikatowego numeru PIN, w celu zabezpieczenia przed korzystaniem z karty przez osoby trzecie, np. w wyniku kradzieży karty. Rozwiązanie to podobne jest do stosowanych powszechnie kart płatniczych (kredytowych), z tą różnicą, że generowany jest podpis elektroniczny.

W jednym i drugim rozwiązaniu aplikacja bankowa musi być połączona z podmiotem uwierzytelniającym podpis elektroniczny. Brak autoryzacji podpisu musi blokować możliwość wykonania operacji

Stosowanie podpisu elektronicznego w celu autoryzacji transakcji wykonanej przez klienta jest najbardziej oczywistym zastosowaniem tego rozwiązania. Podpis elektroniczny daje jednak o wiele więcej możliwości rozwiązania sfery zabezpieczenia rachunków bankowych klientów. Mam tutaj na myśli autoryzację wykonania transakcji przez operatora.

Autoryzowanie dokonania transakcji przez operatora podpisem elektronicznym pozwala na zwiększenie ochrony rachunków bankowych. Lecz niesie za sobą również zagrożenie dla systemów informatycznych banku, związanych głównie z autoryzacją podpisu.

Można mówić o przynajmniej dwóch możliwościach autoryzacji podpisu elektronicznego operatorów.

- Autoryzacja podpisu w trakcie logowania się do systemu. Rozwiązanie to może polegać na tym, że operator chcąc zalogować się do systemu musi włożyć do czytnika kartę z przypisanym mu podpisem elektronicznym oraz podać login i hasło do systemu. Zapisany na karcie podpis elektroniczny musi zostać zweryfikowany przez odpowiednią instytucję autoryzującą podpisy. Po udanej próbie weryfikacji istniałaby dopiero możliwość pracy z systemem. W systemie zapisana byłaby informacja o autoryzacji pracy wskazanego operatora na podanym stanowisku. Przy takim rozwiązaniu

- transakcje były by podpisane podpisem elektronicznym lecz sprawdzanie podpisu nie byłoby realizowane przez oddzielny podmiot ale przez system, dzięki zapisaniu w systemie informacji o autoryzacji podpisu elektronicznego w trakcie logowania do systemu. Aby istniała możliwość dokonania operacji z tego stanowiska przez innego operatora, musiałby on najpierw zalogować się ponownie do systemu, co wymusza autoryzację jego podpisu i zapisanie o tym informacji w systemie. Przedstawione rozwiązanie pozwala na wykorzystanie podpisu elektronicznego do autoryzacji transakcji realizowanych przez operatora lecz nie może być traktowane jako w pełni zgodne z Ustawą o podpisie elektronicznym, w której to zakłada się autoryzację każdej transakcji przez uprawniony do tego podmiot (zgodnie z interpretacją ustawy bank nie może sam sobie autoryzować podpisu).
- Rozwiązaniem alternatywnym do przedstawionego wyżej jest autoryzowanie każdej transakcji operatora przez uprawniony do tego podmiot. Daje to pełna zgodność z Ustawą o podpisie elektronicznym lecz niesie za sobą zagrożenie znacznego spowolnienia pracy systemu. Poprawę sytuacji może przynieść polepszenie infrastruktury sieciowej i telekomunikacyjnej, z której korzysta bank oraz znaczna ilość instytucji mających uprawnienia do autoryzacji podpisu elektronicznego.

Rozwój bankowości elektronicznej o nowe typy usług lub produktów

Bankowość elektroniczna stosowana jest w głównej mierze do obsługi produktów bankowych funkcjonujących na rynku narodowym. Chodzi w szczególności o rachunki rozliczeniowe i oszczędnościowe oraz w mniejszym stopniu depozytowe czy kredytowe.

Oprócz tego typu produktów banki oferują również produkty obsługiwane w obrocie zagranicznym. Podzielić je można na takie, których klientami są instytucje niefinansowe lub osoby prywatne oraz podmioty finansowe (np. banki). Druga grupa produktów określana jest mianem back-office. Obsługa produktów funkcjonujących w obrocie zagranicznym częściowo posługuje się elementami bankowości elektronicznej. Wymiana informacji między krajami odbywa się z wykorzystaniem systemu Swift, w postaci odpowiednich komunikatów elektronicznych. Jednak nie wszystkie informacje mogą być przesyłane w postaci komunikatów Swift.

Wśród produktów obsługiwanych w obrocie zagranicznym, przeznaczonym dla klientów niefinansowych są m.in. tzw. operacje dokumentowe: akredytywa dokumentowa i inkaso dokumentowe. Obsługa tego typu produktów wymaga dostarczenia do banku dokumentów związanych z dokonanymi transakcjami biznesowymi, np. faktur, rachunków itp. W chwili obecnej dokumenty te prze-

syłane są w postaci tradycyjnej, tzn. papierowej. Prezentacja dokumentów handlowych jest podstawą do podjęcia decyzji o realizacji akredytywy lub inkasa. Wprowadzenie podpisu elektronicznego jako równoważnego z podpisem tradycyjnym na dokumentach handlowych, pozwala na przesyłanie tych dokumentów drogą elektroniczną, co może znacznie przyspieszyć obsługę klienta.

Rozwiązanie takie obarczone jest oczywiście pewnymi niedogodnościami. Po pierwsze wymusza to stosowanie technik handlu elektronicznego przez instytucje wystawiające te dokumenty. Instytucjami tymi mogą być np. kooperanci handlowi, urzędy spedycyjne, urzędy celne i inne. Po za tym podpis elektroniczny stosowany przez podmiot funkcjonujący w innym kraju musi być autoryzowany przez właściwą instytucję. Z przyczyn technicznych i prawnych nie zawsze istnieje taka możliwość.

Zakończenie

Podpis elektroniczny w bankach pozwala klientom na łatwiejszy dostęp do rachunków. Stosowanie technik kryptograficznych pozwala na bezpieczne wykonywanie tych operacji. Wprowadzenie Ustawy o podpisie elektroniczny może wpłynąć na rozszerzenie oferty banków o wymianę elektroniczną dokumentów nie obsługiwanych przez dotychczas stosowane techniki bankowości elektronicznej, jak: elixir – dla wymiany krajowej czy Swift w przypadku wymiany międzynarodowej.

Źródła

1. J. Muszyński, *Infrastruktura klucza publicznego i podpisy elektroniczne*, „NetWorld”, wydanie specjalne, *Systemy Bezpieczeństwa Sieciowego*, 2001.
2. V. Leyland, *EDI –Elektroniczna Wymiana Dokumentacji*; WNT, Warszawa 1995.
3. J. Muszyński, *Infrastruktura kluczy publicznych*, „NetWorld”, 2000, nr 4.
4. D. Majgier, *Sprzęt: zabezpiecz swoje dane tokenem*, <http://web.reporter.pl/2000/03/w0701.html>