CBKE
e-BIULETYN

Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny

Prof. Mirosław Kutyłowski

Politechnika Wrocławska

Bezpieczeństwo systemów teleinformatycznych stosowanych w sektorze finansowym może być zapewnione jedynie poprzez jednoczesne zastosowanie środków na płaszczyźnie technologicznej, organizacyjnej, kontrolnej i zbudowanie odpowiednich reguł prawnych. Zbudowanie takiego systemu okazuje się w praktyce zadaniem niezwykle trudnym. Wpływają na to następujące czynniki:

Tempo zmian w technologii: tempo zmian w zakresie stosowanych technologii bezpieczeństwa jest bardzo duże. Inaczej niż w przypadku szeregu innych dziedzin technicznych, zmiany są gwałtowne, a ich kierunek jest trudny do przewidzenia. Zdarza się, że bardzo obiecujące techniki okazują się chybione lub zostają zastąpione przez inne, efektywniejsze metody.

Jako przykład posłużyć może postęp w zakresie łamania RSA – najważniejszego bodaj algorytmu podpisu elektronicznego. Początkowo wydawało się, że możliwe jest oszacowanie bezpiecznych parametrów kluczy służących do składania i do weryfikacji podpisu RSA. Okazało się jednak, że prognozy dotyczące bezpiecznej wielkości klucza bywały niedoszacowane – postęp algorytmów faktoryzacji był dużo szybszy od oczekiwań. Czynnikami postępu były zarówno postępy w zakresie budowy algorytmów (NFS), jak i postęp w zakresie budowy specjalistycznego sprzętu kryptograficznego (TWINKLE, TWIRL).

Innym przykładem tego typu są nieoczekiwane postępy w zakresie ataku na algorytm SHA-1, które miały miejsce w 2004 roku. Okazało się, że znalezienie kolizji dla tego algorytmu (stosowanego między innymi do tworzenia podpisu elektronicznego na podstawie Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 w sprawie określenia warunków technicznych

o 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. nr 128, poz. 1094 – dalej: rozporządzenie z 7.08.2002) może stać się niedługo faktem. Kolizje dla funkcji SHA-0 (pierwowzoru SHA-1) zostały znalezione przez Eli Bihama oraz Rafi Chena. Również na konferencji CRYPTO 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai i Hongbo Yu zaprezentowali spektakularny atak na MD5.

Stopień skomplikowania: ścisłe zrozumienie niektórych technik stosowanych w inżynierii bezpieczeństwa wymaga zaawansowanej wiedzy. Dla przykładu, wyrażenie własności funkcji takich jak MD5, SHA-1, RIPEMD-160, stosowanych jako „cyfrowe odciski palców" w wielu popularnych algorytmach (RSA, DSA) i protokołach (SSL), jest trudne pod względem matematycznym. Wyrażenie postulowanej własności *jednostronności* napotyka na trudności nawet na gruncie teorii złożoności obliczeniowej. Częste sformułowania typu: *„dla zadanej wartości y nie jest możliwe znalezienie wartości x takiej że SHA-1(x)=y"* nie są poprawne w sensie matematycznym. Ścisła definicja jest z kolei na tyle zawikłana matematycznie, że jej zrozumienie wymaga odpowiedniego specjalistycznego przygotowania i dokładnej specyfikacji zadania obliczeniowego. Podobnie, pojęcie „bezkonfliktowości" bywa nieprawidłowo interpretowane. Przykładowo, następujące sformułowania nie są prawdziwe: „*dwa dokumenty nie posiadają tego samego cyfrowego odcisku palców"*, *„nie można znaleźć dwóch dokumentów o tym samym cyfrowym odcisku palców".* Pierwsze sformułowanie przeczy zasadzie szufladkowej Dirichleta, w drugim brakuje odniesienia do mocy obliczeniowych – w sensie teorio-informacyjnym jest ono błędne.

Interdyscyplinarność: budowa bezpiecznego systemu teleinformatycznego wymaga zarówno ścisłej specyfikacji, jak i formalnej weryfikacji założonych własności. W sytuacji, gdy jednym z elementów tworzonego systemu jest zgodność z regulacjami prawnymi, konieczna jest weryfikacja pod tym względem. Czynności te wymagają głębokiej wiedzy i doświadczenia z dwóch dziedzin: prawa i informatyki.

Aspekty socjologiczne

Zasadniczym błędem w konstruowaniu systemów bezpieczeństwa okazywało się częste ignorowanie aspektów socjologicznych. Dla przykładu, postulowana dawniej częsta zmiana haseł

dostępowych przez użytkowników (niekiedy wymuszana przez system) powodowała w istocie wybieranie przez użytkowników łatwych do zapamiętania (i do zgadnięcia) haseł Podobnie, wymuszanie „losowych haseł" prowadziło co prawda do utrudnień w stosowaniu ataków słownikowych, ale często powoduje też zjawisko zapisywania haseł przez użytkowników.

Doświadczenia te wskazują, że regulacje dotyczące zachowania użytkowników systemów bezpieczeństwa muszą być skorelowane z możliwościami dostosowania się użytkowników do tych zaleceń. Fundamentalną zasadą budowy skutecznego systemu bezpieczeństwa jest wykorzystanie analogii z innych dziedzin życia: nie można zakładać, że użytkownik takiego systemu będzie przestrzegał założonych reguł, o ile reguły te nie będą jasne, zrozumiałe i oparte na analogiach z życia codziennego. Drugą fundamentalną zasadą jest takie konstruowanie systemu bezpieczeństwa, aby brał on pod uwagę możliwość dokonywania błędów przez użytkownika.

W odniesieniu do regulacji dotyczących bezpieczeństwa należy również zastosować zasadę, by były one sformułowane tak, aby ich znaczenie w sensie prawnym odpowiadało znaczeniu potocznemu. Potrzebę takiego konstruowania regulacji dotyczących użytkownika uwzględniono w dyrektywie Wspólnoty Europejskiej dotyczącej podpisu elektronicznego (1999/93/WE z 13 grudnia 1999) - jednym z obowiązków stojących przed podmiotem świadczącym usługi certyfikacyjne jest informowanie odbiorów usług w „zrozumiałym języku". Zasada ta została pogwałcona w Polsce przez ustawę o podpisie elektronicznym z dnia 18 września 2001. Wprowadzone tam pojęcia „bezpieczny podpis elektroniczny" i „podpis elektroniczny" różnią się dość znacznie zarówno w sensie definicji, jak i w sensie funkcjonalnym. Różnice te nie polegają jednak na obiektywnym poziomie bezpieczeństwa – tym samym terminologia wpływa na błędne zakwalifikowanie przez użytkownika „zwykłego" podpisu elektronicznego. Tak samo ustawowa nazwa może wpłynąć na powstanie nadmiernego zaufania wobec „bezpiecznego podpisu elektronicznego".

Neutralność technologiczna

Jedną z zasadniczych cech systemu prawnego powinna być stabilność regulacji. Z drugiej strony dynamika zmian w zakresie technologii bezpieczeństwa może powodować nacisk na szybkie i częste dostosowywanie prawa do zmieniającej się sytuacji. Szczególnie krytyczne konsekwencje może mieć złamanie mechanizmów zabezpieczeń. Na przykład gdyby w Polsce rozwinął się obrót prawny oparty o podpis elektroniczny, i gdyby złamaniu uległy algorytmy SHA-1 i RIPEMD-160, to w związku z brzmieniem rozporządzenia z 7.08.2002 sparaliżowaniu uległby obrót dokumentów elektronicznych (nie jest dozwolone korzystanie z innych funkcji!). Istniejące procedury

uaktualniania prawa na poziomie ustaw nie pozwalają na odpowiednio szybkie zmiany regulacji. W przypadku aktów prawnych niższej rangi również zmiany dostosowawcze mogą okazać się dużo za wolne – wskazuje na to praktyka stanowienia prawa.

Kolejnym problemem związanym z szybkim tempem rozwoju technologii może być krępowanie wprowadzania najnowocześniejszych rozwiązań przez takie regulacje, które zbyt szczegółowo odnoszą się do konkretnej technologii. Początkowy okres kształtowania prawa dotyczącego bezpieczeństwa systemów teleinformatycznych charakteryzował się właśnie takim podejściem. Do nich należała pierwsza legislacja w zakresie podpisu elektronicznego - w stanie Utah - użyte sformułowania odnosiły się de facto do podpisów RSA („szyfrowanie" podczas składania podpisu). Równolegle rozwijające się techniki oparte o problem dyskretnego logarytmu nie wykorzystują szyfrowania w trakcie składania podpisu i tym samym były wykluczone ze stosowania w stanie Utah.

Te i wiele innych przykładów pokazuje, że konstruowanie przepisów prawa pod kątem narzucenia reżimów bezpieczeństwa w ramach określonego systemu teleinformatycznego jest błędem. Szybkie zmiany w zakresie technologii powodują, iż przepisy takie bardzo szybko stają się hamulcem rozwoju i wymuszają stosowanie przestarzałych rozwiązań o nierzadko niższym poziomie bezpieczeństwa.

Idea neutralności technologicznej jest odpowiedzią na te zagrożenia. Regulacje prawne mają przestać opisywać, w jaki sposób bezpieczeństwo jest osiągane, mają jedynie opisywać niezbędne, minimalne cechy określonych systemów. W żaden sposób nie mają zaś określać w jaki sposób owe cele są osiągane. Takie podejście zgodne jest zresztą z metodologią budowy systemów teleinformatycznych – faza modelowania i projektowania poprzedzona jest specyfikacją celów, jaki ów system ma osiągnąć.

Strona odpowiedzialna za bezpieczeństwo

Jedną z zasadniczych koncepcji budowy systemu prawnego dla instytucji finansowych w Unii Europejskiej jest wskazanie instytucji finansowej jako strony odpowiedzialnej za poziom bezpieczeństwa stosowanych rozwiązań technologicznych. Koncepcja ta jest odpowiedzią na wykorzystywanie silnej pozycji przez instytucje finansowe i narzucanie klientom niekorzystnych umów obarczających ich skutkami stosowania mało wiarygodnych mechanizmów zabezpieczeń.

Dobrym przykładem w tym zakresie były regulaminy stosowania kart bankomatowych w Polsce. Do niedawna praktycznie cała odpowiedzialność w tym zakresie spoczywała na klientach

banków – wypłata za pomocą prawidłowej karty i prawidłowego PINu obarczała klienta. Jednocześnie banki w Polsce stosują karty z paskiem magnetycznym – co umożliwia klonowanie kart. Praktyka umieszczania kamer nad terminalami w supermarketach, gdzie klienci dokonują wpisania PIN-u dopełnia obrazu systemu o bardzo niskim poziomie bezpieczeństwa. System ten funkcjonuje mimo możliwości wprowadzenia kart, w których elektronicznym nośnikiem informacji byłaby karta mikroprocesorowa – niebywale trudna do sklonowania i mogąca implementować mechanizmy kryptograficzne.

Ograniczenie odpowiedzialności użytkownika elektronicznych instrumentów płatniczych do kwoty 150 Euro przez Ustawę o elektronicznych instrumentach płatniczych z dnia 12 września 2002 jest wyrazem koncepcji przyjętej przez Unię Europejską. Przyjęto bowiem, że efektywnym sposobem zmuszenia instytucji finansowych do działania w celu ulepszeniu systemów bezpieczeństwa jest obarczenie tych instytucji odpowiedzialnością za luki bezpieczeństwa na drodze ustawowej.

Wbrew pozorom rozwiązania tego typu nie są niekorzystne dla banków. Ustanawiają bowiem reguły działania, przy których budowanie solidnych systemów teleinformatycznych zaczyna posiadać uzasadnienie ekonomiczne. Zwiększają również szanse w walce konkurencyjnej tych instytucji finansowych, które poważnie podchodzą do zagadnień bezpieczeństwa obrotu.

Specyfika rozwiązań bankowych – horyzont czasowy

Techniki bezpieczeństwa stosowane w bankach muszą odpowiadać podstawowym założeniom co do funkcjonowania systemu bankowego. Bardzo ważną cechą jest tu ograniczony horyzont czasowy dla dokonywania czynności i ważności szeregu dokumentów. Powoduje to, że mechanizmy bezpieczeństwa stosowane do czynności o przewidywalnym horyzoncie czasowym i powiązane z całym systemem operacji muszą gwarantować określony poziom bezpieczeństwa jedynie we wskazanym okresie. Zaprojektowanie odpowiedniego systemu jest przez to dużo łatwiejsze. Uwidoczniło się to na przykład w problemach z koncepcjami prawnego modelu ważności podpisów elektronicznych: o ile w kontekście problematyki ważności podpisu elektronicznego i zachowania formy pisemnej w oświadczeniach woli spowodowało to szereg kontrowersji (i przyjęcie odmiennych koncepcji np. przez Austrię i Niemcy), to problem ten dla sektora bankowego ma jedynie charakter poboczny i wiąże się głównie z umowami z klientami zawieranymi w postaci elektronicznej. Tym samym główny system elektronicznego obiegu informacji w sektorze bankowym nie jest dotknięty tymi problemami, które wiążą się z ważnością podpisu pod oświadczeniami woli w postaci elektronicznej.

Nienadążanie za technologią

Przykładem nietrafionego podejścia do zagadnienia elektronizacji obiegu dokumentów jest Rozporządzenie Ministra Finansów z dnia 11 sierpnia 2003 r. zmieniające rozporządzenie w sprawie sposobu pobierania, zapłaty i zwrotu opłaty skarbowej oraz sposobu prowadzenia rejestrów tej opłaty (Dz.U. nr 143, poz. 1392).

Paradoksalnie, jedną z trudności we wnoszeniu podań drogą elektroniczną jest uiszczanie opłaty za pomocą znaczka skarbowego. Prosty system znaczków skarbowych, który ułatwiał dokonywanie niewielkich płatności, okazał się czynnikiem hamującym elektronizację wnoszenia podań. W epoce bankowości elektronicznej tańsze i efektywniejsze może być przekazywanie opłat drogą przelewów elektronicznych lub za pomocą rozmaitych technik umożliwiających mikropłatności. W rozporządzeniu wybrano jednak inne rozwiązanie: o ile sama płatność może być dokonana na drodze przelewu bankowego, to jej dokonanie musi być potwierdzone dowodem wpłaty opatrzonym bezpiecznym podpisem elektronicznym wystawionym przez pracownika banku. Przypomnijmy, że wystawienie podpisu elektronicznego nie może być dokonane automatycznie przez odpowiedni serwer – czynność tę można wykonać wyłącznie osoba fizyczna z zachowaniem odpowiednich (czasochłonnych) czynności. Powoduje to, iż wystawienie elektronicznego potwierdzenia przelewu staje się operacją stosunkowo kosztowną dla banku, a potwierdzenie nie może być wystawione równocześnie ze zleceniem przelewu.

Rozporządzenie nie podejmuje również w poważny sposób problematyki archiwizacji podań wnoszonych drogą elektroniczną. Przyjęte rozwiązanie mówi, iż podanie wniesione drogą elektroniczną, a także dowód wpłaty wraz z podpisem elektronicznym muszą zostać wydrukowane, a na wydruku umieszczony znaczek opłaty skarbowej. Stanowi to krok w dokładnie przeciwnym kierunku niż postępujący proces elektronizacji archiwów bankowych. W istocie przyjęte rozwiązanie ze względów praktycznych wyklucza wnoszenie podań drogą elektroniczną.

Usługi bankowości elektronicznej w świetle ustawy o elektronicznych instrumentach płatniczych

Przyjęta 12 września 2002 roku ustawa o elektronicznych środkach płatniczych podejmuje w rozdziale 4 problematykę usług bankowości elektronicznej. Warto zaznaczyć, że włączenie tej tematyki do ustawy o elektronicznych środkach płatniczych było krokiem podjętym z chęci uregulowania pokrewnych zagadnień w jednej ustawie i nie było wymuszone brzmieniem Zalecenia

Komisji Europejskiej nr 97/489/WE z dnia 30 lipca 1997 r. dotyczącej transakcji z użyciem elektronicznych instrumentów płatniczych.

Zasadniczą nowością w ustawie tej jest postanowienie, iż „*bank, świadcząc usługi na podstawie umowy o usługi bankowości elektronicznej, obowiązany jest do: (1) zapewnienia posiadaczowi bezpieczeństwa dokonywania operacji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych*" Regulacja ta stanowi, iż obowiązkiem banku jest zapewnienie bezpieczeństwa dokonywania operacji. Tym samym to bank odpowiada za zastosowanie odpowiednich środków technicznych oraz za odpowiednie poinstruowanie użytkownika. Odpowiedzialność nie jest nieograniczona: konieczne jest jedynie zachowanie należytej staranności i wykorzystanie właściwych rozwiązań technicznych.

W świetle powyższej regulacji warto odnieść się do problemu stosowania kart bankomatowych z paskiem magnetycznym. W sytuacji, gdy nie wymaga większej inwencji skonstruowanie urządzeń do przechwytywania danych zapisanych na karcie i podglądnięcie PINu wpisywanego przez użytkownika na klawiaturze, trudno zakwalifikować owe karty jako „właściwe rozwiązanie techniczne". Istnieje tania alternatywa – karty z mikroprocesorem - zabezpieczające przy odpowiednim skonfigurowaniu przed klonowaniem i nieuprawnionym odczytem. Paradoksalnie, karty magnetyczne wcześniej wycofały firmy telekomunikacyjne, choć kwoty o jakie chodziło w przypadku pojedynczej karty telefonicznej były znikome w porównaniu z kartą bankomatową.

W zarysowanej sytuacji Ustawodawca wykonał racjonalny krok: bez ingerencji w sferę technologiczną i łamania zasady neutralności technologicznej (jakim byłby nakaz stosowania kart mikroprocesorowych) nałożył na banki odpowiedzialność za używanie środków o niewłaściwym poziomie bezpieczeństwa. Sytuacji o podobnym charakterze jest więcej. Stosowane listy haseł jednorazowych są generowane po stronie banku i wyglądają „losowo". Jednak czy istotnie hasła te nie są możliwe do odgadnięcia? Banki odmawiają informacji na temat sposobu generowania haseł jednorazowych. Należy podkreślić, że brak publicznej specyfikacji sposobu generowania haseł jest czynnikiem obniżającym poziom bezpieczeństwa. Na ile jest to problem poważny, można było się przekonać w związku z ujawnionymi słabościami algorytmu generowania PIN-ów do kart EC i zmianą tego algorytmu w 1998 roku po przegranych przez banki procesach sądowych w Zachodniej Europie. Bezpośrednią przyczyną powstania luki bezpieczeństwa i jej istnienia przez wiele lat był brak publicznej weryfikacji algorytmu. Poszkodowany klient banku może obecnie argumentować, że system bezpieczeństwa nie jest oparty o właściwe rozwiązania techniczne – bowiem podstawową zasadą sztuki współczesnej inżynierii bezpieczeństwa jest, że o ile utajnieniu

podlega sposób działania zabezpieczeń i nie podlega on niezależnej weryfikacji, to system taki nie może być uznany za system o wysokim poziomie bezpieczeństwa.

Wspomniana ustawa zawiera jednak postanowienie, które, w niezamierzony zapewne sposób, może się odbić na poziomie bezpieczeństwa banków elektronicznych w Polsce. Chodzi mianowicie o art. 32, który posiada następujące brzemienie:

1. Posiadacz jest obowiązany do nieujawniania informacji o działaniu elektronicznego instrumentu płatniczego udostępnionego w ramach umowy o usługi bankowości elektronicznej, których ujawnienie może spowodować brak skuteczności mechanizmów zapewniających bezpieczeństwo zlecanych operacji.

2. Posiadacza obciążają operacje dokonane przez osoby, którym udostępnił informacje, o których mowa w ust. 1. Przepisy art. 28 stosuje się odpowiednio.

Intencją tego zapisu było obarczenie posiadacza elektronicznego instrumentu płatniczego odpowiedzialnością za operacje wykonane przez osoby, którym udostępnił hasła, PIN-y itp. informacje. Tym samym zapewniona jest pewna równowaga: bank jest odpowiedzialny za stworzenie odpowiedniego systemu bezpieczeństwa, jednak posiadacz elektronicznego instrumentu płatniczego jest odpowiedzialny za ochronę informacji, które umożliwiają dostęp do tego urządzenia. Tak więc o ile system autoryzacji oparty jest o posiadanie instrumentu i wiedzę posiadacza, to posiadacz jest zobowiązany do utrzymywania tej wiedzy w tajemnicy pod rygorem odpowiedzialności finansowej za dokonywane operacje.

Niebezpieczeństwo kryje się tym razem w zbyt szerokim sformułowaniu. Wraz z postępem technologii mechanizmy zabezpieczeń elektronicznego instrumentu płatniczego mogą okazać się zbyt słabe, by oprzeć się nowym rodzajom ataków. Osoba, która napotka się na tego typu słabości systemu, powinna ze względu na interes publiczny jak najszybciej ujawnić istnienie luki. Doświadczenie w zakresie budowy bezpiecznych systemów teleinformatycznych wskazuje, że raportowanie dostrzeżonych słabości jest jednym z fundamentalnych mechanizmów zapewniania bezpieczeństwa. Publikowanie informacji o słabościach wymusza natychmiastową reakcję administratorów systemów i ich producentów.

Sformułowanie art. 32 skutecznie hamuje jednak ujawnianie tego typu luk. Osoba, która stała się świadoma istnienia luki w mechanizmach bezpieczeństwa elektronicznego instrumentu płatniczego, może co prawda ujawnić informacje o owej luce, ale wobec brzmienia ustępu 2 może zostać obarczona odpowiedzialnością finansową za operacje dokonywane takimi instrumentami w wypadku, gdy bank zaniedba dokonania odpowiedniej modyfikacji systemu bezpieczeństwa. Ryzyko interpretacji art. 32 w kierunku korzystnym dla banku powoduje, że racjonalnie postępująca osoba nie ujawni informacji o istnieniu luk. Z drugiej strony, historia

odkrywania luk w systemach teleinformatycznych pokazuje, że po osiągnięciu pewnego poziomu wiedzy i technologii luki są odkrywane niezależnie przez wiele osób. Tym samym należy założyć, że jedynymi organizacjami, które zostaną wcześniej czy później poinformowane o istnieniu luk, będą organizacje przestępcze.

Instytucja pieniądza elektronicznego

Kilka uwag należy zgłosić również wobec rozdziału ustawy o elektronicznych środkach płatniczych odnoszącego się do rygorów nakładanych na instytucje pieniądza elektronicznego. W związku z kreowaniem pieniądza (choć w bardzo ograniczonym zakresie), instytucje pieniądza elektronicznego powinny być podmiotami wiarygodnymi. Zapewnieniu tego celu służy duża część uregulowań wspomnianej ustawy. Dotyczą one zarówno postanowień odnoszących się do samych podmiotów, jak i nadzoru ze strony Komisji Nadzoru Bankowego (KNB). Niemniej jednak należy zwrócić uwagę na kilka aspektów.

Żadne z postanowień dotyczących instytucji pieniądza elektronicznego nie stanowi, że podmiot ten dysponuje dostępem do odpowiedniej technologii, że posiada personel o odpowiedniej wiedzy i doświadczeniu w zakresie technicznym i organizacyjnym niezbędnym do prowadzenia działalności tego typu. Ponieważ brak jest takich zapisów, nadzór nad instytucją pieniądza elektronicznego nie może kwestionować jej wiarygodności pod tym kątem.

Za mniej istotne uznać należy postanowienia z art. 38. Dla przykładu nieskuteczne w sensie praktycznym jest postanowienie ust. 3: *„Przedstawiony przez założycieli plan działalności instytucji pieniądza elektronicznego na okres co najmniej 3 lat powinien wskazywać, że instytucja ta będzie w stanie wywiązywać się ze swoich zobowiązań wobec klientów”*. Nic bowiem nie stoi na przeszkodzie, by instytucja pieniądza elektronicznego po powstaniu zmieniła plan działalności. Tym samym iluzoryczna jest nadzieja, iż istnienie planu działalności wpłynie w istotny sposób na podniesienie poziomu bezpieczeństwa.

Problematyczne okazują się również możliwości kontroli przez KNB. Art. 43 stanowi iż:

3. Czynności kontrolne podejmowane są przez inspektorów nadzoru bankowego ...

4. Czynności, o których mowa w ust. 3, mogą być wykonywane ponadto przez upoważnionych biegłych rewidentów po okazaniu upoważnienia wydanego przez Generalnego Inspektora Nadzoru Bankowego.

W szczególności KNB nie może zlecić wykonania specjalistycznych kontroli laboratoriom i firmom specjalizującym się w wąskich zagadnieniach technologicznych występujących

w problematyce pieniądza elektronicznego. Z drugiej strony, nierealne i nieuzasadnione ekonomicznie jest, aby wspomniane laboratoria powstawały w ramach KNB. Odpowiednimi środkami technicznymi nie będą również dysponowali biegli rewidenci, ze względu na skalę przedsięwzięcia.

Wspomniane problemy stanowią chyba element większej całości – brak jest dotychczas całościowych koncepcji dotyczących sposobu sprawowania kontroli państwowej nad sektorem e-gospodarki. Istniejące regulacje podejmują zazwyczaj kwestie marginalne z punktu widzenia bezpieczeństwa technologicznego.

W ustawie zawartych jest kilka sformułowań, które mimo w zasadzie słusznego kierunku stanowią czynnik blokujący rozwój instytucji pieniądza elektronicznego. Przykładem takiego ograniczenia jest górny limit na zawartość „elektronicznej portmonetki", wynoszący równowartość 150 euro, a wprowadzony ze względów bezpieczeństwa. O ile realizacja tego zapisu w krajach Eurolandu nie powoduje żadnych trudności technicznych, to zapis w polskie ustawie już takie trudności techniczne powoduje. Przypomnijmy bowiem brzmienie art. 58 ust. 1: *Instrument pieniądza elektronicznego udostępniony posiadaczowi powinien posiadać mechanizm uniemożliwiający przechowywanie pieniądza elektronicznego o wartości większej niż równowartość w złotych 150 euro obliczana według średniego kursu ogłaszanego przez NBP obowiązującego w dniu wydania*. Każde rozwiązanie technologiczne elektronicznej portmonetki **uniemożliwiające** przechowywanie kwoty wyższej musi się opierać na komunikacji z NBP i sprawdzaniu bieżącego kursu euro. Tak więc z powodu błahego w istocie problemu zmian kursu euro elektroniczne portmonetki w Polsce nie mogą być urządzeniami pracującymi w trybie off-line.

Elektroniczny dokument bankowy

Kolejnym ważnym aktem prawnym regulującym bezpieczeństwo systemów bankowości w dobie elektronizacji jest Rozporządzenia Rady Ministrów z dnia 25.02.2003 r. w sprawie zasad tworzenia, utrwalania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego, dokumentów bankowych sporządzanych na elektronicznych nośnikach informacji (Dz.U. Nr 51, poz. 442). Rozporządzenie określa zasady tworzenia, utrwalania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego, dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji.

Jednym z centralnych pojęć używanych w rozporządzeniu jest „podpis" składany na danych w postaci elektronicznej. Niestety pojęcie to odbiega od pojęcia podpisu elektronicznego wprowadzonego przez Ustawę o podpisie elektronicznym. Tym samym mamy do czynienia

z kolejnym przykładem chaosu pojęciowego, i mimo poprawności formalnej pogwałcona została zasada takiego konstruowania przepisów prawa, aby były one łatwo i jednoznacznie zrozumiane przez użytkowników systemów teleinformatycznych. Przypomnijmy, że „podpisanie" w sensie tego rozporządzenia polega na:

a) złożeniu bezpiecznego podpisu elektronicznego lub

b) złożeniu podpisu elektronicznego lub dołączeniu danych identyfikujących, zgodnie z umową stron, a w przypadku dokumentów wewnętrznych banku - zgodnie z jego uregulowaniami wewnętrznymi.

Najważniejszym postanowieniem rozporządzenia jest postanowienie, iż każdy elektroniczny dokument bankowy powinien być opatrzony podpisem (w powyższym sensie) i zabezpieczony przed dokonywaniem zmian po jego utworzeniu. W duchu postanowień neutralności technologicznej rozporządzenie unika wskazania konkretnych sposobów, przy pomocy których cel ten ma zostać osiągnięty. Jest to podejście uwzględniające obecny stan technologii i praktyki działalności: z jednej strony coraz bardziej palące pod względem ekonomicznym jest przeniesienie dokumentacji do postaci elektronicznej, a z drugiej strony archiwizacja danych w postaci elektronicznej nie doczekała się dobrze funkcjonujących uniwersalnych standardów, nawet gdy są dostępne atrakcyjne rozwiązania techniczne.

Wiele zapisów rozporządzenia może stanowić godny naśladowania wzór sposobu formułowania regulacji prawnych dotyczących e-gospodarki. Jest jednak bardzo ważny wyjątek: w innym stylu został napisany § 5.2. Przytoczmy jego brzmienie: *W przypadku stosowania podpisu elektronicznego dokument należy utrwalić wraz z całą ścieżką certyfikacji zawierającą certyfikat i zaświadczenia certyfikacyjne oraz ze wszystkimi listami zawieszonych lub unieważnionych certyfikatów użytymi w celu weryfikacji podpisu elektronicznego.* Zapis ten pozornie zapewnia bezpieczeństwo. W istocie jednak praktyczny skutek tego zapisu jest **eliminowanie podpisu elektronicznego** z elektronicznych dokumentów bankowych. Budzi to co najmniej zdziwienie, gdyż w obecnej chwili stosowanie podpisu cyfrowego jest najtańszym, najskuteczniejszym i jedynym (poza zabezpieczeniami na poziomie nośnika fizycznego) sposobem zapewnienia integralności dokumentów cyfrowych i uwierzytelnienia ich pochodzenia.

Przyjrzyjmy się źródłom owych problemów. Po pierwsze należy zwrócić uwagę, że nie ma powodu (ekonomicznego i technologicznego), aby podpis elektroniczny stosowany w systemach bankowych był ograniczony do bezpiecznego podpisu elektronicznego, a tylko do niego odnoszą się pojęcia takie jak „zaświadczenie certyfikacyjne". Po drugie należy przypomnieć, że listy zawieszonych i unieważnionych certyfikatów nie mają ustalonej długości. Tym samym osoba projektująca system informatyczny banku musiałaby zrezygnować z rekordów

stałej długości dla tych dokumentów, które byłyby opatrywane podpisem elektronicznym. Z technicznego punktu widzenia jest to sytuacja trudna do zaakceptowania – regułą konstruowania baz danych jest używanie rekordów o zmiennej długości tylko w wyjątkowych sytuacjach. Nie widać również jakiegokolwiek uzasadnienia merytorycznego dla takiego rozwiązania. Wystarczyłoby przecież archiwizować wspomniane informacje w jakikolwiek sposób umożliwiający późniejszą weryfikację.

Wspomniane niezręczności są być może jednym z poważniejszych powodów niskiego poziomu wprowadzania w życie omawianego rozporządzenia. W dłuższej perspektywie czasu stanowi to o wzroście kosztów funkcjonowania sektora bankowego i obniżenia poziomu bezpieczeństwa.