O podpisie elektronicznym i certyfikatach z nim związanych

„Logistyka" rozmawia z Dariuszem Gaconiem, Prezesem Zarządu E-Telbanku Sp. z o. o. – firmą wystawiającą oraz zarządzającą certyfikatami kluczy publicznych służących weryfikacji podpisu elektronicznego.

Iwo Nowak – *Od jesieni 2001 r. dużo się mówiło i pisało o podpisie elektronicznym w Polsce, ale tak naprawdę chyba jeszcze stosunkowo niewiele osób wie, że można już go bezpiecznie stosować w praktyce...*

Dariusz Gacoń – Zgadza się. 11 października ub.r. Prezydent RP Aleksander podpisał ustawę o podpisie elektronicznym. Dokument ten* stwarza podstawy prawne do rozwoju elektronicznej gospodarki w naszym kraju oraz określa zasady działania dostawców usług certyfikacyjnych. Czekamy wprawdzie na wejście w życie przepisów wykonawczych do tej ustawy, ale już teraz mogę powiedzieć, że wprowadziliśmy na polskim rynku pełną komercyjną ofertę usług certyfikacyjnych, pozwalającą klientom bezpiecznie korzystać z poczty elektronicznej tak służbowo, jak i prywatnie. Za pomocą naszych produktów i usług można zabezpieczyć także poufność transakcji w handlu i bankowości elektronicznej, a użycie podpisu elektronicznego uwiarygodnia ostatecznie strony tych transakcji, choćby, np. przy dokonywaniu zakupów w sklepach internetowych.

11.10.2001 r. - Prezydent A. Kwaśniewski składa pierwszy w Polsce podpis elektroniczny

I. N. – *Ustawa, która wejdzie w życie 16 sierpnia br., opiera się na odpowiednim dokumencie Unii Europejskiej.*

D. G. – Ogólnoeuropejskie ramy prawne dla podpisu elektronicznego określono w Dyrektywie 99/93/EC. Jest to fundamentalny dokument dla rozwoju ustawodawstwa w zakresie podpisu elektronicznego w Europie i na świecie, bowiem – co warto podkreślić – jest to jeden z rzadkich przypadków, by europejscy prawodawcy znaleźli naśladowców w Ameryce Północnej. Dyrektywa 99/93/EC otwiera możliwości rozwoju komunikacji elektronicznej nie tylko w gospodarce, ale i w sferze społecznej, a także w polityce. Nasza ustawa o podpisie elektronicznym opiera się właśnie na tym unijnym dokumencie.

I. N. – *Czym w rozumieniu prawa jest zatem podpis elektroniczny?*

D. G. – Podpis elektroniczny oznacza dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Tyle definicja. Jednak w naszej ustawie w obawie o możliwość pojawiania się prób sfałszowania tego podpisu wprowadzono dodatkowo pojęcie „Bezpiecznego podpisu elektronicznego", który:

a) jest przyporządkowany wyłącznie do osoby składającej ten podpis
b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego
c) jest powiązany z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Niestety – wydaje się – że nasz ustawodawca trochę się tu zagalopował, ponieważ tak zdefiniowany podpis jest bezpieczny jedynie po stronie jego tworzenia. A to nie jest wystarczający warunek choćby do prawnego zrównania podpisu elektronicznego z własnoręcznym. Warunki takiego zrównania zdefiniowano w ustawie w art. 5 mówiącym, iż dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym

* Ustawę o podpisie elektronicznym opublikowano 15 listopada 2001 r. (Dz. U 130 poz. 1450). Z mocy art. 59 ust. 1 ustawa ta wchodzi w życie 9 miesięcy po opublikowaniu, a więc 16.08.2002 r. W tym dniu, dzięki zmianie przepisu art. 60 kc, podpis elektroniczny zaistnieje w sposób pełny jako środek wyrażania oświadczenia woli, gdyż zgodnie z nowym brzmieniem art. 78 ust. 2 „Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej". Art. 60 kc nie ograniczał nigdy formy złożenia oświadczenia woli, a szczególne przepisy prawa dopuszczały stosowanie oświadczenia woli w formie elektronicznej. Np. Prawo bankowe w art. 7 ust. 1 stanowiło, iż „oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażone za pomocą elektronicznych nośników informacji". Uzupełnienie art. 60 o zapis dotyczący formy elektronicznej podkreśla równoprawność tej formy z formami tradycyjnymi.

podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej.

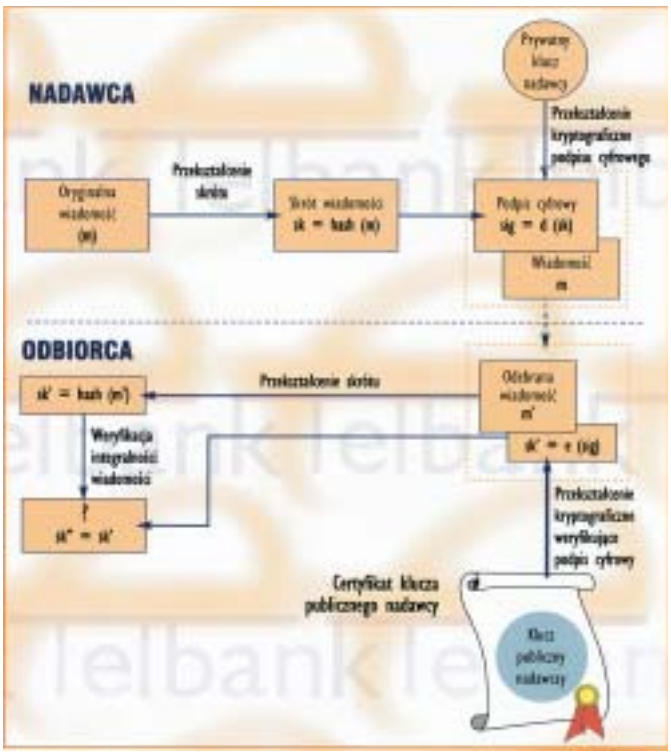
I. N. – *A zatem podpis elektroniczny, nawet bezpieczny, powinien być odpowiednio zweryfikowany, by spełniał warunki uznania go za równoważny „zwykłemu" podpisowi, którego – co za paradoks – w żaden sposób za zupełnie bezpieczny uznać nie można?*

D. G. – Analiza wymagania weryfikacji podpisu elektronicznego wskazuje jednoznacznie na potrzebę istnienia dostawców wiarygodnych danych weryfikujących ten podpis, oferujących coś w rodzaju elektronicznego dowodu tożsamości, czyli właśnie certyfikatu. Ustawa z 15 listopada 2001 r. określa go jako elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej taki e-podpis i które umożliwiają identyfikację tej osoby. W swych zapisach ustawa określa ogólne zasady świadczenia usług certyfikacyjnych, nie nakładając żadnych ograniczeń na ich dostawców. Jeśli jednak dążymy do zrównania podpisu elektronicznego z własnoręcznym, logicznym wydaje się wprowadzenie podziału na dostawców certyfikatów niekwalifikowanych i kwalifikowanych. W stosunku do dostawców tej ostatniej kategorii ustawa definiuje instytucję nadzoru (Minister Gospodarki) oraz warunki techniczno – administracyjne sprawowania nad nimi kontroli. Środkiem realizacji nadzoru jest rejestr dostawców certyfikatów kwalifikowanych oraz zaświadczenia certyfikacyjne świadczące o kwalifikowanym statusie danego dostawcy. Ustawa upoważniła też Narodowy Bank Polski do powierzenia wytwarzania i wydawanie zaświadczeń certyfikacyjnych dla dostawców certyfikatów kwalifikowanych, podmiotowi świadczącemu usługi certyfikacyjne zależnemu od NBP (nie mogą to być jednak usługi certyfikacyjne polegające na wydawaniu certyfikatów).

Hierarchia certyfikacji PolCert

I. N. – *Kto obecnie w Polsce może już wydawać odpowiednie certyfikaty dla użytkowników podpisu elektronicznego?*

D. G. – Powiem może nieskromnie, ale na razie tylko my świadczymy na naszym rynku usługi na poziomie odpowiadającym zastosowaniom komercyjnym. Działające od niespełna 10 lat Bankowe Przedsiębiorstwo Telekomunikacyjne „TELBANK" S.A. założyło w lutym 2001 r. firmę E-Telbank Sp. z o. o. dla prowadzenia działalności gospodarczej w zakresie udostępniania kanałów dla elektronicznego obrotu finansowego, w tym m. in. dla płatności elektronicznych. Z kolei E-Telbank Sp. z o. o. uruchomił 20 lipca ubr. Ośrodek Certyfikacji PolCert TM, funkcjonujący jako tzw. Zaufana Trzecia Strona, zapewniająca swym klientom praktyczną realizację czterech podstawowych usług bezpieczeństwa: uwierzytelnienia, integralności, niezaprzeczalności i poufności.



Przekształcenie podpisu cyfrowego i jego weryfikacja

I. N. – *OC PolCert został uruchomiony w lipcu 2001 r., a Prezydent RP podpisał ustawę o podpisie elektronicznym dopiero w kilka miesięcy później...*

D. G. – To prawda. Jednak wcześniejsze rozpoczęcie działalności przez OC PolCert było możliwe dzięki podpisaniu strategicznej umowy o współpracy między E-Telbankiem, a belgijską firmą GlobalSign, będącą największym w Europie dostawcą usług certyfikacyjnych i zarazem oficjalnym dostawcą certyfikatów dla Komisji Unii Europejskiej. E-Telbank uzyskując w lipcu 2001 r. akredytację GlobalSign został uprawniony – jako pierwszy i dotąd jedyny w Polsce – do wydawania certyfikatów kluczy publicznych, akceptowanych na całym świecie i odpowiadających standardom europejskim pod względem bezpieczeństwa oraz procedur i przepisów prawnych. Od sierpnia ub. r. OC PolCert TM zaczął udostępniać certyfikaty Osobiste PolCert TM 1, przeznaczone dla zastosowań testowych i prezentacyjnych aby zaznajomić klientów z certyfikatami kluczy publicznych. Ten certyfikat nie jest przeznaczony do zastosowań komercyjnych, choć w wystarczający sposób gwarantuje autentyczność skrzynki pocztowej nadawcy poczty elektronicznej. Natomiast od 15 listopada 2001 r. E-Telbank Sp. z o. o. rozpoczął działalność komercyjną uruchamiając witrynę internetową (www.polcert. pl), udostępniającą certyfikaty Osobiste PolCert TM 1, Osobiste PolCert TM 2 oraz PolCert TM Serwery WWW.

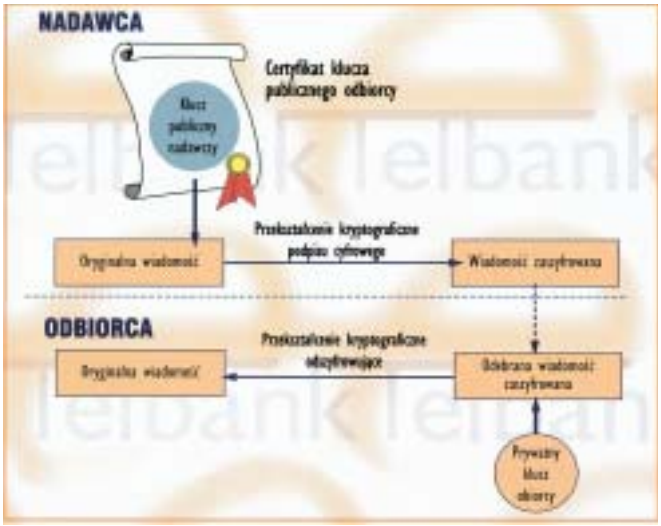
I. N. – *Są jeszcze certyfikaty Osobiste PolCert TM 3, 3 Pro i Obiekty...*

D. G. – Certyfikaty Osobiste PolCert TM 2, 3, 3 Pro umożliwiają przesyłanie dokumentów za pośrednictwem sieci komputerowych z zachowaniem najwyższych stan-

dardów bezpieczeństwa, a także zapewniają możliwość korzystania z prawnie skutecznego podpisu elektronicznego w kraju i za granicą. Certyfikat PolCert TM Serwery WWW wykorzystywany jest do realizacji usługi „bezpieczny serwer", zapewniającej maksimum wiarygodności dla serwisów WWW. W połączeniu z protokołem Secure Sockets Layer (SSL) możliwe jest bezpieczne komunikowanie się między serwerem, a klientem. Głównym obszarem zastosowań usługi „bezpieczny serwer" jest elektroniczna wymiana danych szczególnie w takich dziedzinach, jak handel elektroniczny, informatyczne usługi *on-line* i bankowość elektroniczna. Natomiast certyfikat PolCert TM Obiekty służy bezpiecznemu dystrybuowaniu oprogramowania w Internecie. Odbiorcy takiego oprogramowania mogą być wtedy pewni, że mają do czynienia z oryginalnym produktem i jego autentycznym autorem lub dostawcą. Wszystkie te klasy certyfikatów są już dostępne w naszej ofercie.

I. N. – *Sam certyfikat chyba nie wystarczy do zapewnienia całkowitego bezpieczeństwa podpisu elektronicznego np. przed próbami jego podrobienia?*

D. G. – Oczywiście. Dlatego też dla bezpiecznej komunikacji w sieciach teleinformatycznych stosuje się asymetryczne techniki kryptograficzne oparte na dwóch powiązanych ze sobą przekształceniach kryptograficznych: przekształceniu publicznym (definiowanym przez klucz publiczny) i przekształceniu prywatnym (definiowanym przez klucz prywatny). Klucz prywatny jest chroniony przez jego właściciela i nie jest udostępniany żadnym innym osobom, w przeciwieństwie do klucza publicznego – rozpowszechnianego wśród zainteresowanych. Oba klucze charakteryzuje to, że jest obliczeniowo niewykonalne wyznaczenie klucza prywatnego jedynie na podstawie znajomości klucza publicznego. Asymetryczną technikę kryptograficzną można wykorzystać dwojako: 1) w systemie podpisywania, w którym przekształcenie prywatne dotyczy podpisu, a przekształcenie publiczne – jego weryfikacji. Mechanizm podpisu cyfrowego gwarantuje integralność danych, uwierzytelnienie nadawcy podpisanej wiadomości i realizację usługi niezaprzeczalności polegającej na zagwarantowaniu (dzięki odpowiednim mechanizmom i procedurom), że osoba uczestnicząca w komunikowaniu się nie może się wyprzeć tego, iż wysłała lub odebrała daną wiadomość; 2) w systemie szyfrowania, w którym przekształcenie publiczne służy do zaszyfrowania wiadomości, a przekształcenie prywatne do jej odszyfrowania, gwarantując w ten sposób poufność przesłanych treści. Asymetryczne techniki kryptograficzne, w szczególności podpis cyfrowy, mogą być wykorzystywane dla zabezpieczenia poczty elektronicznej (np. S/MIME), szyfrowania połączeń sieciowych (np. SSL), tworzenia wirtualnych sieci prywatnych (VPN) oraz przez mechanizmy kontroli dostępu do baz danych i serwerów WWW.



Mechanizm szyfrowania z wykorzystaniem asymetrycznych technik kryptograficznych

I. N. – Podsumowując: jednym z efektów stosowania podpisu elektronicznego w praktyce może być doprowadzenie do sytuacji dotąd niewyobrażalnej, a więc zaistnienia biura bez papierów?!

D. G. – Biuro bez papierów to już nie jest fikcja. Dotąd dokumenty mające postać elektroniczną musiały i tak być drukowane, aby można było na nich złożyć własnoręczny podpis. W sferze nowej gospodarki elektronicznej staje się on jednak zupełnie bezużyteczny: nie można sygnować nim dokumentów przekazywanych elektronicznie, a poza tym współczesna technika pozwala na jego dowolne kopiowanie i mogące się z tym łączyć ewentualne nadużycia. Dodatkowe korzyści, wynikające ze stosowania podpisu elektronicznego, to błyskawiczne przesyłanie podpisanych oryginałów dokumentów w dowolne miejsce na kuli ziemskiej, likwidacja lub znaczna redukcja kosztów papieru, druku, opłat pocztowych, paliwa oraz pracy osób obsługujących korespondencję. Zastosowanie e-podpisu daje też pewność, że wysłana poczta nie została po drodze (przez rozległe sieci komputerowe) zmieniona, a jej nadawca świadomie podpisał i wysłał e-dokument. Dodatkowe zaszyfrowanie przesyłki uniemożliwia jej odczytanie przez osoby nieuprawnione. W odniesieniu do logistyki trzeba powiedzieć, że obecnie istnieją możliwości wprowadzenia sterowania przepływem towarów za pomocą elektronicznej wymiany dokumentów oraz udziału podmiotów świadczących usługi certyfikacyjne w zapewnieniu bezpieczeństwa tym dokumentom. Przykładowo, usługa oznaczania czasu gwarantuje wiarygodność kontraktów zawierających terminy dostaw lub procedur logistycznych w sytuacjach, gdy zaangażowani są różni przewoźnicy i różne środki transportu. Możemy oczywiście mnożyć dziedziny, w których wprowadzenie podpisu elektronicznego znacznie zmieni dotychczasowy tryb funkcjonowania, np. sektor finansowy,

Ośrodek Certyfikacji PolCert™ udostępnia następujące klasy certyfikatów:

Rodzaj certyfikatu	Okres ważności	Cena PLN	Odpowiedzialność do wysokości	Procedura weryfikacji	Czas oczekiwania na certyfikat
Osobisty PolCert™ 1	30 dni	0	E-Talbank na polską odpowiedzialność	• adres e-mail	1 dzień
Osobisty PolCert™ 2	1 rok	50	2500 Euro	• adres e-mail • wypełniony wniosek	1 dzień od weryfikacji wniosku
Osobisty PolCert™ 3 Osobisty PolCert™ 3 Pro	1 rok	180	37500 Euro	• adres e-mail • wypełniony wniosek • osobiste stawienie się w Punkcie Rejestracji PolCert™	1 dzień od weryfikacji wniosku
PolCert™ Serwery WWW	1 rok	800	37500 Euro	• nazwa domeny internetowej • wypełniony wniosek	1 dzień od weryfikacji wniosku
PolCert™ Obiekty	1 rok	700	37500 Euro	• adres e-mail • wypełniony wniosek	1 dzień od weryfikacji wniosku

Ceny nie uwzględniają podatku od towarów i usług VAT

Ośrodek Certyfikacji PolCert™ udostępnia klasy certyfikatów (Ceny nie uwzględniają podatku VAT)

Pobranie certyfikatu

Najprostszym sposobem pobrania certyfikatu osobistego PolCert 1 jest wejście na witrynę internetową Ośrodka Certyfikacji PolCart (tm). Na stronach www.wabank.pl, po wybraniu opcji PolCert, a nastepnie „wybierz bezpłatny certyfikat klasy 1" znajdziecie państwo na stronie rozpoczynającej procedurę wydawania certyfikatu. Nastepnie należy postępować zgodnie z wyświetlanymi komunikatami.

Trzeba wykonać osiem kroków – wysłać dwie przesyłki pocztą elektroniczną i odebrać dwie informacje od Ośrodka Certyfikacji PolCert (tm).

Pierwszy krok procedury wydawania certyfikatu polega na sprawdzeniu czy certyfikat głównego ośrodka certyfikacji GlobalSign (root) jest zainstalowany w przeglądarce internetowej. Przeważnie jest to formalność, ponieważ wszystkie nowsze wersje przeglądarek mają go wbudowanego na stałe. Jeżeli tak nie jest, to użytkownik uzyska certyfikat GlobalSign (root) już w pierwszym kroku procedury.

Dzięki akredytacji GlobalSign certyfikaty PolCert znajdują się w ścieżce zaufania GlobalSign, oferują tym samym swoim klientom syfrową tożsamość o cechach globalnych, ponieważ certyfikaty PolCert są automatycznie rozpoznawalne w popularnych przeglądarkach. Żaden odbiorca wiadomości z podpisem weryfikowanym przy użyciu certyfikatu PolCert nie zobaczy takiego ekranu:

Następne etapy procedury wydawania certyfikatu obejmują: weryfikację adresu poczty elektrinicznej, wygenerowanie pary kluczy, zaakce [ptowanie Umowy Subskrybencji i przesłanie drogą elektroniczną wniosku o wydanie certyfikatu. W krótkim czasie Ośrodek Certyfikacji PolCert (tm) prześle wiadomość z informacją, skąd można pobrać gotowy certyfikat. Ostatnim krokiem procedury jest instalacja w przeglądarce internetowej. Aby tego dokonać wystarczy w kroku 8 wybrać opcję „zainstaluj". Od tej pory certyfikat klucza publicznego jest zainstalowany w systemie i gotowy do skonfigurowania klienta poczty.

Konfiguracja certyfikatu w programie pocztowym

Aby wysyłać i odbierać podpisane i zaszyfrowane wiadomości pocztą elektroniczną niezbędne jest poprawne skonfigurowanie konta pocztowego. Poszczególne kroki tego procesu są zależne od używanych aplikacji pocztowych takich jak: MS Outlook 98/2000, MS Outlook Express 5, Netscape Messanger 4. x.

Jak pobrać certyfikat Osobisty PolCert 1

organy administracji rządowej i samorządowej, księgi notarialne i wieczyste (pieczęć notariusza może być zastąpiona jego e-podpisem i zaświadczeniem certyfikacyjnym urzędu notarialnego), handel, sądownictwo, usługi pocztowe, rejestry znaków towarowych i patentów oraz publiczna opieka zdrowotna. Jesteśmy na samym początku tej drogi i jak naprawdę potoczy się łańcuch zmian w naszej codziennej działalności wskutek wprowadzenia podpisu elektronicznego – trudno dziś ocenić. Mam jednak nadzieję, że wchodzenie w życie codzienne e-podpisu będzie się odbywało bez jakichkolwiek zahamowań i barier, z pożytkiem dla nas wszystkich.

I. N. – *Dziękuję za rozmowę.*

Rozmawiał Iwo Nowak