

*Daniel Guga**

**BEZPIECZEŃSTWO TRANSAKCJI ELEKTRONICZNYCH
WYKORZYSTUJĄCYCH INFRASTRUKTURĘ
KLUCZA PUBLICZNEGO**

1. WPROWADZENIE

Rozwój technologii informatycznych w ostatnich latach zmienił nie tylko zakres stosowania komputerów związany ze wzrostem mocy obliczeniowej tych ostatnich, ale również wpłynął na sposób wykorzystania komputerów przez gospodarstwa domowe, wynikający z rozpowszechniania się sieci Internet. Początkowo komputery były wykorzystywane w instytucjach naukowych, w drugiej kolejności trafiły do przedsiębiorstw, a obecnie coraz powszechniej są wykorzystywane w domach. W roku 2005 40% gospodarstw domowych w Polsce posiadało komputer stacjonarny bądź przenośny (wzrost o 4 pp w stosunku do roku 2004), jednocześnie 30% gospodarstw domowych dysponowało komputerem z dostępem do sieci Internet (wzrost o 4 pp w stosunku do roku 2004)¹.

Osoby posiadające dostęp do sieci Internet wykorzystują tę sieć najczęściej do komunikowania się (30% osób z przedziału wiekowego 16–74 lat). Drugim pod względem popularności celem korzystania z Internetu było wyszukiwanie informacji o towarach i usługach, w następnej kolejności sieć wykorzystywano do przeglądania elektronicznych wersji czasopism, rozrywki (pobieranie gier i granie w gry w wersji *on-line*), korzystanie z serwisów poświęconych turystyce (6%), słuchanie radia, oglądanie telewizji *on-line* (6%), korzystanie z usług bankowych (6%), szukanie pracy, wysyłanie ofert (5%), kupowanie, zamawianie towarów lub usług (5%). Powoli wolumen transakcji związanych z kupowaniem towarów i usług w Polsce za pośrednictwem sieci Internet

* Mgr, asystent w Zakładzie Informatyki Ekonomicznej Uniwersytetu Łódzkiego.

¹ Wykorzystanie technologii informacyjno-telekomunikacyjnych w 2005 r., <http://www.stat.gov.pl>, 2.02.2006 r.

zaczyna przybierać realne rozmiary, wartość towarów i usług zamówionych lub kupionych przez Internet w 2005 r. przekroczyła miliard złotych.

2. KLASYFIKACJA DANYCH

Komputery są wykorzystywane przez gospodarstwa domowe, małe i średnie przedsiębiorstwa, duże organizacje i instytucje. Gospodarstwa domowe mogą wykorzystywać komputery w celach czysto rozrywkowych bądź też komputery mogą wspomagać zarządzanie budżetem domowym, mogą też służyć do komunikacji lub innych celów. W przedsiębiorstwach komputery przetwarzają i przechowują dane, wspomagają funkcjonowanie firmy. Dane przetwarzane przez komputer mogą należeć do jednego pracownika (dane przechowywane na stacji roboczej dostępnej dla jednej osoby), do wielu pracowników (dane przechowywane na jednej stacji roboczej, z której korzysta wielu pracowników) lub też wielu pracowników może mieć dostęp do tych samych danych (dane przechowywane na serwerach plików lub w sieciowych bazach danych). Dane przechowywane przez komputer mogą być dostępne nie tylko dla pracowników firmy, ale też dla kontrahentów, klientów lub dowolnych osób spoza organizacji (dane udostępniane poprzez serwery obsługujące serwisy internetowe). Miejsce przechowywania danych, liczba osób, którym są one udostępniane oraz to, czego dotyczą mają istotne znaczenie dla sposobu zabezpieczenia owych danych.

Dane, które są przechowywane, przetwarzane bądź udostępniane przez komputery można podzielić na cztery kategorie².

– Dane publiczne – udostępniane dowolnym użytkownikom, najczęściej za pośrednictwem firmowych witryn internetowych. Zapewnienie poufności tych danych jest zbędne, istotna jest ich integralność. Zmodyfikowanie firmowej witryny internetowej może być przyczyną spadku wiarygodności przedsiębiorstwa, a co za tym idzie również przychodów i zysków. Dla większości osób fizycznych ta kategoria danych nie ma wielkiego znaczenia. W przypadku posiadania strony internetowej będącej wizytówką danej osoby, konsekwencje zmiany zawartości takiej witryny nie są tak dotkliwe, jak dla przedsiębiorstw. Należy jednak rozróżnić strony internetowe osób fizycznych wykonujących wolne zawody lub też pracujących na własny rachunek. Jeżeli taka strona ma być wizytówką połączoną z pracą zarob-

² Podział danych ze względu na poufność oraz przykłady obszarów danych w przedsiębiorstwach na podstawie: Microsoft Official Curriculum 2150, *Designing a Secure Microsoft Windows 2000 Network*, Microsoft Corporation 2000, rozdz. 1, s. 2.

kową, to integralność danych na niej ma podobne znaczenie, jak dla przedsiębiorstw.

– Dane wewnętrzne, nieudostępniane osobom niezatrudnionym w przedsiębiorstwie, do którego należą takie dane. Mogą one zawierać informacje dotyczące procedur przedsiębiorstwa, wzorów pism, danych marketingowych. Nieuprawniona modyfikacja takich danych może powodować zakłócenia w funkcjonowaniu przedsiębiorstwa. Ujawnienie tego typu danych osobom z zewnątrz firmy może być przyczyną spadku wiarygodności przedsiębiorstwa w oczach klientów oraz kontrahentów. Wśród danych przechowywanych przez osoby fizyczne, do tego typu kategorii danych można zaliczyć wiadomości pocztowe (o ile nie zawierają poufnych informacji, np. haseł dostępowych do witryn internetowych), historie uruchamianych aplikacji, otwieranych i edytowanych dokumentów oraz odwiedzanych witryn internetowych.

Dane poufne – to informacje, do których w przedsiębiorstwie powinna mieć dostęp tylko wybrana grupa użytkowników (np. tylko dział księgowości i kierownictwo firmy ma dostęp do danych finansowo-księgowych). Informacje tego typu mają małą wartość dla osób spoza organizacji, jednak ujawnienie ich może zachwiać zaufaniem kontrahentów oraz pracowników do organizacji. W przypadku spółek publicznych, ujawnienie tego typu danych może wpłynąć na wartość akcji spółki, może być również podstawą do wyciągnięcia konsekwencji natury finansowej i karnej przez instytucje nadzorujące publiczny obrót papierami wartościowymi³. W przypadku osoby fizycznej do tej kategorii danych można zaliczyć wyciągi bankowe, zeznania podatkowe, polisy ubezpieczeniowe.

– Dane tajne – posiadające wartość intelektualną dla przedsiębiorstwa, wzory produkcyjne, patenty, receptury. Utrata bądź nieupoważniony dostęp do tego rodzaju danych może zachwiać istnieniem organizacji. Dla osoby fizycznej do tej kategorii danych można zaliczyć identyfikatory i hasła dostępu do kont bankowych, funduszy inwestycyjnych, serwisów aukcyjnych, kont pocztowych. Utrata tych danych może być przyczyną strat finansowych (kradzież środków finansowych z konta bankowego), czy też problemów

³ Osoby niepowiązane ze spółką, które wykorzystają informację poufną dotyczącą spółki akcyjnej dopuszczonej do publicznego obrotu, mogą być ukarane karą pieniężną w wysokości do 200 000 złotych albo do pięciokrotności uzyskanej korzyści majątkowej, ujawnienie informacji poufnej przez osoby powiązane ze spółką podlega grzywnie do 2 000 000 zł albo karze pozbawienia wolności do lat 3; wykorzystanie informacji poufnej przez osoby związane ze spółką podlega grzywnie do 5 000 000 zł albo karze pozbawienia wolności od 3 miesięcy do lat 5, albo obu tym karom łącznie – *Ustawa z dnia 21 sierpnia 1997 r. Prawo o publicznym obrocie papierami wartościowymi*, tekst jednolity DzU, 2005, nr 111, poz. 937, art. 161c, 161h, 176.

prawnych (kradzież tożsamości – wykorzystywanie danych ofiary do realizacji nielegalnych transakcji w serwisach aukcyjnych lub serwisach rozliczeniowych typu Paypal).

3. ZABEZPIECZANIE DOSTĘPU DO DANYCH

Osoba korzystająca z sieci Internet może realizować za pośrednictwem tej sieci operacje związane tylko z danymi publicznymi bądź też z danymi poufnymi czy tajnymi. Podczas wyboru poziomu zabezpieczenia danych istotnym kryterium decyzyjnym jest to, czy dane, które mają być zabezpieczone, należą do tej osoby i są w jej gestii posiadania, przechowywania i zabezpieczenia, czy też są to dane innych osób lub instytucji, do których ta osoba uzyskuje jedynie dostęp i zabezpieczenie, przechowywanie oraz przetwarzanie tych danych nie należy do tej osoby. W sytuacji zapewnienia dostępu do elektronicznych danych, system przetwarzający i udostępniający owe dane musi zapewnić dwa mechanizmy: autentyfikację – czyli identyfikację osoby uzyskującej dostęp do systemu oraz autoryzację – mechanizmy pozwalające na nadawanie uprawnień i kontroli poziomu dostępu do określonych informacji. Dla dalszych rozważań autor przyjął założenie, że systemy są na tyle bezpieczne, na ile gwarantują to producenci, nie uwzględniając w tym momencie niepoprawnego funkcjonowania systemów wynikającego z luk w oprogramowaniu.

3.1. Autentyfikacja użytkowników

Komunikowanie z wykorzystaniem sieci Internet może być realizowane na kilka sposobów. Klasycznym rozwiązaniem jest wysyłanie wiadomości pocztowych za pośrednictwem serwerów pocztowych z wykorzystaniem klienta pocztowego – programu działającego na stacji roboczej użytkownika (przykładowe programy to Outlook Express, Netscape Communicator, MS Outlook). Komunikacja pomiędzy klientem a serwerem realizowana jest z wykorzystaniem protokołu POP3 (dla odbioru danych z serwera) oraz z wykorzystaniem protokołu SMTP (dla wysyłania danych od klienta do serwera). Protokół SMTP jest również wykorzystywany do komunikowania się serwerów pocztowych ze sobą (przesyłania wiadomości z serwera wykorzystanego przez nadawcę do serwera obsługującego odbiorcę wiadomości). Protokoły POP3 oraz SMTP mogą być zabezpieczone dodatkowo protokołem

SSL. Implementacja protokołu SSL⁴ wymaga zainstalowania wygenerowanego certyfikatu dla serwera pocztowego dla użytkownika korzystającego z tak zabezpieczonego serwera. Konfiguracja oprogramowania klienckiego jest sprawą dość łatwą. Należy jednak zauważyć, że dane są zabezpieczone tylko na drodze pomiędzy klientem a serwerem, użytkownik nie ma pewności, czy jego wiadomość w sposób bezpieczny zostanie przekazana z jego serwera do serwera odbiorcy oraz czy odbiorca pobierze taką wiadomość z wykorzystaniem protokołu POP3/SSL. Problemem jest również sposób autentyfikacji użytkownika podczas podłączania się do serwera protokołem POP3 oraz SMTP bez wsparcia SSL, gdyż hasło użytkownika jest wysyłane w sposób jawny, co umożliwia przechwycenie takiego hasła. Przechwycenie hasła dostępowego przez osobę niepowołaną umożliwia jej dokonanie nieuprawnionego wykorzystania konta pocztowego. Inną możliwością jest dostęp do skrzynki pocztowej poprzez stronę www, z wykorzystaniem protokołu http lub https. Bezpieczny protokół https może być wykorzystywany do autentyfikacji użytkownika bądź też do wymiany informacji pomiędzy serwerem a użytkownikiem. Komunikowanie się użytkowników może być również realizowane za pomocą czatów lub też poprzez przysyłanie wiadomości błyskawicznych (ang. *instant messaging*). Obecnie coraz powszechniejsza staje się też możliwość korzystania z telefonii internetowej. Liczba użytkowników polskiego programu do korespondencji natychmiastowej Gadu-Gadu wynosi 3 mln⁵, Skype ma 40 mln użytkowników na świecie, z czego 3 mln w Polsce⁶.

3.2. Zagrożenia związane z autentyfikacją użytkowników

Użytkownik korzystający z poczty elektronicznej podczas wyboru usługodawcy powinien zbadać, jaki poziom bezpieczeństwa w zakresie transmisji danych i przysyłania hasła jest zapewniany przez usługodawcę. Jeżeli dostawca usług oferuje kilka kanałów dostępu, nie wszystkie z nich będą bezpieczne dla użytkownika. Osoba korzystająca z takich usług powinna więc wybrać kanał dostępu z odpowiednim poziomem bezpieczeństwa. Istotne jest również to, jakie dane użytkownik przysyła za pomocą konta pocztowego wybranego usługodawcy oraz wybranego kanału dostępu. Jeżeli dane nie mają charakteru poufnego, poziom zabezpieczeń nie ma znaczenia. Użytkownik poczty

⁴ Protokół SSL (ang. *Secure Sockets Layer*) został opracowany przez firmę Netscape. Specyfikacja protokołu SSL w wersji 3.0, <http://wp.netscape.com/eng/ssl3/ssl-toc.html>, 3.02.2006 r.

⁵ Komunikat prasowy Gadu-Gadu Sp. z o.o. z dnia 10.01.2006 r., <http://www.gadu-gadu.pl/biuro-wiadomosci-GGG-3mln.html>, 3.02.2006 r.

⁶ <http://skype.onet.pl/1232757,artykul.html>, 3.02.2006 r.

elektronicznej oraz innych serwisów elektronicznych, do których dostęp jest zabezpieczony poprzez podanie pojedynczego i niezmiennego hasła, musi mieć świadomość, że taka metoda autentyfikacji, niezależnie od sposobu przesyłania hasła (w postaci jawnej bądź zaszyfrowanej), nie gwarantuje bezpieczeństwa tego hasła. Jedną z metod przechwycenia hasła jest zainstalowanie na komputerze ofiary programu typu keylogger⁷ lub też urządzenia typu keylogger. Zainstalowanie urządzenia typu keylogger wymaga bezpośredniego dostępu fizycznego do komputera, zatem można uznać, że tego typu atak nie jest możliwy do zrealizowania na prywatnym komputerze, przechowywanym w miejscu zamieszkania użytkownika. Jednak w przypadku korzystania z komputerów publicznie dostępnych (np. w kawiarenkach internetowych) użytkownik nie ma pewności co do braku ataku tego typu. Programowe przechwycenie wprowadzanego przez użytkownika hasła wymaga, tak jak wcześniej wspomniano, instalacji na komputerze ofiary odpowiedniego oprogramowania. Zainstalowanie takiego oprogramowania nie wymaga dostępu fizycznego do komputera, odpowiedni program może być dostarczony jako załącznik do przesłanej wiadomości pocztowej⁸ lub też jako kod wykonywalny może być umieszczony na stronie internetowej.

3.3. Zabezpieczanie metod autentyfikacji użytkowników

Osoba korzystająca z serwisów internetowych, które identyfikują użytkownika, musi być świadoma poziomu bezpieczeństwa danej metody autentyfikacji. Poziom bezpieczeństwa musi być tym wyższy, im bardziej cenne są dane, do których uzyskujemy dostęp. Autentyfikacja⁹ może być realizowana na różne sposoby: mogą być wykorzystywane hasła (*knowledge-based authentication*) – użytkownik w celu identyfikacji podaje coś co zna, czyli hasło, użytkownik może wykorzystać coś co posiada, token bądź listę haseł

⁷ Keylogger – typ programów komputerowych służących do wykradania haseł. Programy te działają na zasadzie przejęcia kontroli nad procedurami systemu operacyjnego, służącymi do obsługi klawiatury. Każde wciśnięcie klawisza jest odnotowywane w specjalnym pliku. Opcjonalnie informacje o wciśniętych klawiszach poszerzone są o dodatkowe informacje, jak nazwa aktywnego programu lub okna. <http://pl.wikipedia.org/wiki/Keylogger>, 3.02.2006 r.

⁸ Programy typu keylogger zaliczane są do kategorii koni trojańskich. Przykładem takiego programu jest Trojan-Spy.Win32.KeyLogger.db przechwytyjący dane wprowadzane z klawiatury i dokonujący próby wysłania tych danych do zdalnego komputera. Dodatkowe informacje dotyczące przytoczonego programu dostępne na stronach <http://wirusy.antivirenkit.pl/pl/opis/Trojan-Spy.Win32.KeyLogger.db.html>; <http://www.sophos.com/virusinfo/analyses/trojkeylog-gag.html>, 3.02.2006 r.

⁹ A. Bagga, L. O'Gorman, J. Bentley, *Query-directed passwords*, „Computers & Security” No 24, 2005, s. 548.

jednorazowych (*possession-based authentication*) oraz użytkownik może być rozpoznany bezpośrednio przez system z wykorzystaniem metod biometrycznych (ID-based). Istotną z punktu widzenia bezpieczeństwa jest metoda wymiany hasła pomiędzy użytkownikiem a serwerem. Serwer w celu identyfikacji hasła podanego przez użytkownika może dokonywać porównania jawnych wersji hasła (posiadane przez serwer i przesłane przez użytkownika) lub też serwer może porównać swoją niejawną wersję hasła z niejawną wersją hasła przesłaną przez komputer użytkownika. Niejawne wersje hasła są generowane poprzez działanie tego samego algorytmu podczas ustalania i wprowadzania hasła do bazy haseł serwera i podawania hasła przez użytkownika. Bezpieczny kanał transmisyjny zabezpiecza jedynie przed przechwyceniem transmitowanych danych. Połączenie realizowane za pośrednictwem protokołu SSL nie jest odporne na atak typu Pharming¹⁰, a mianowicie przekierowanie szyfrowanej sesji do fałszywego serwera. W sytuacji przekierowania użytkownika do fałszywego serwera możliwe jest wykonanie przez osobę atakującą nieuprawnionych transakcji, nawet w sytuacji wykorzystywania przez użytkownika hasła z listy kodów jednorazowych¹¹, czy też haseł generowanych dynamicznie poprzez urządzenia typu token¹² lub przesyłanych poprzez wiadomości sms¹³.

4. OBSZARY ZASTOSOWAŃ INFRASTRUKTURY KLUCZA PUBLICZNEGO – PKI

Użytkownik serwisu internetowego, korzystając z połączenia zabezpieczonego protokołem SSL, może sprawdzić, czy połączenie zostało nawiązane z prawdziwym serwerem poprzez weryfikację certyfikatu przesłanego przez serwer. Weryfikacja wiarygodności serwera, z którym dokonano połączenia, jest jedną z funkcji możliwych do uzyskania dzięki wykorzystaniu infra-

¹⁰ D. Guga, *Transakcje elektroniczne przeprowadzane w sieci Internet, identyfikacja zagrożeń, czyli „nie bądź rybą w sieci”*, [w:] M. Niedźwiedziński, K. Lange-Sadzińska (red.), *Wybrane problemy elektronicznej gospodarki*, Łódź 2005, s. 78–93.

¹¹ Hasła z listy kodów jednorazowych są zabezpieczeniem stosowanym m. in. przez m-bank http://www.mbank.com.pl/przewodnik/bezpieczenstwo/hasla_jednorazowe.html oraz PKO Bank Polski Konto Inteligo http://www.inteligo.pl/infosite/oferta_dla_ciebie_bezpieczenstwo.htm, 3.02.2006 r.

¹² Zabezpieczenie oparte na urządzeniu RSA SecurID stosuje m. in. Volkswagen Bank Direct <http://www.vwbankdirect.pl/1087.html>, 3.02.2006 r.

¹³ Hasła przesyłane jako wiadomości sms są alternatywną formą potwierdzania transakcji w stosunku do wykorzystania hasła z listy haseł jednorazowych. Rozwiązanie tego typu zostało wprowadzone na początku roku 2006 przez m-bank http://www.mbank.com.pl/przewodnik/bezpieczenstwo/hasla_smsowe.html, 3.02.2006 r.

struktury PKI¹⁴. Infrastruktura ta może być wykorzystana do osiągnięcia następujących celów związanych z danymi¹⁵:

- poufności danych – poprzez szyfrowanie przekazu,
- integralności danych – poprzez podpisanie danych,
- wiarygodności danych – poprzez zaszyfrowanie skrótu danych,
- niezaprzeczalności – poprzez zaszyfrowanie skrótu danych,
- znakowania czasem,
- podpisywania kodu – cyfrowe podpisanie przez jego twórcę oryginalnego oprogramowania, zweryfikowanie integralności danych na podstawie cyfrowego podpisu przez odbiorcę,
- zabezpieczenia komunikacji z serwerami – certyfikat dla protokołu SSL.

4.1. Autentyfikacja użytkowników oraz podpis elektroniczny z wykorzystaniem infrastruktury PKI

Podniesienie poziomu bezpieczeństwa transakcji elektronicznych może być uzyskane poprzez autentyfikację użytkownika z wykorzystaniem certyfikatu oraz poprzez podpisywanie przez niego przesyłanych danych. Wykorzystanie certyfikatów po obu stronach połączenia, po stronie serwera oraz po stronie klienta, zapewnia wiarygodność obydwu stron transakcji oraz integralność danych. Dane tak przesłane przez sieć nie mogą być zmodyfikowane bez wykrycia. Podpisanie przesyłanych danych jest procesem kilkietapowym. W pierwszej kolejności do przesyłanych danych dołączany jest skrót tych danych poprzez wykonanie działania algorytmu typu *hash*. Z założenia wynik uzyskany poprzez działania tego algorytmu jest niepowtarzalny dla danego ciągu danych. Zmiana pojedynczego bitu w danych poddanych działaniu algorytmu powoduje zmianę ponad połowy cyfr w liczbie będącej wynikiem tej operacji. Jeżeli dane nie ulegną modyfikacji, to wynik działania algorytmu haszującego będzie taki sam. Drugą operacją, jaka jest wykonywana, jest zaszyfrowanie wyniku haszowania z wykorzystaniem klucza prywatnego nadawcy. Wraz z danymi źródłowymi i zaszyfrowanym skrótem wysyłany jest również klucz publiczny nadawcy. Odbiorca tak przygotowanych danych, wykorzystując klucz publiczny nadawcy, odszyfrowuje liczbę będącą wynikiem haszowania przeprowadzonego na komputerze nadawcy. Otrzymane przez

¹⁴ PKI – Public Key Infrastructure – Infrastruktura Klucza Publicznego. Jest to szeroko pojęty kryptosystem, w skład którego wchodzić mają urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów (użytkownicy), oprogramowanie i sprzęt – <http://pl.wikipedia.org/wiki/PKI>, 3.02.2006 r.

¹⁵ Microsoft Official Curriculum 2821, *Designing and Managing a Windows Public Key Infrastructure*, Microsoft Corporation 2003, rozdz. 1, s. 3.

odbiorcę dane są poddawane działaniu tego samego algorytmu, którego użył nadawca i wynik haszowania uzyskany dla danych otrzymanych przez odbiorcę porównywany jest z odszyfrowanym wynikiem haszowania. Jeżeli obie liczby są takie same, to zakładamy, że dane nie zostały zmienione podczas przesyłania oraz że pochodzą od osoby, która jest w posiadaniu klucza prywatnego, skojarzonego z otrzymanym przez odbiorcę kluczem publicznym. Wykorzystanie infrastruktury PKI może zapewnić wiarygodność osoby korzystającej z danego serwisu czy też przesyłającej wiadomość elektroniczną. W polskim prawie¹⁶ wyróżniono podpis elektroniczny i bezpieczny podpis elektroniczny. Podpis elektroniczny służy do identyfikacji osoby składającej podpis, natomiast bezpieczny podpis elektroniczny musi być złożony za pomocą bezpiecznych urządzeń podlegających wyłącznej kontroli osoby składającej podpis. Dokumenty podpisane bezpiecznym podpisem z wykorzystaniem ważnego kwalifikowanego certyfikatu są równoznaczne dokumentom podpisanym własnoręcznie¹⁷.

4.2. Identyfikacja potrzeb w zakresie architektury PKI

Identyfikacja osób wykonujących transakcje elektroniczne w sieci Internet oparta na bezpiecznym podpisie elektronicznym zmniejsza ryzyko wykonania operacji przez osobę niepowołaną. Użytkownik, który chce dokonać operacji podpisania elektronicznie dokumentu bądź też chce dokonać autentyfikacji z wykorzystaniem infrastruktury PKI, musi posiadać wystawioną dla siebie parę kluczy – prywatny oraz publiczny. Oparcie autentyfikacji użytkowników na infrastrukturze PKI wymaga przeanalizowania następujących czynników, mających wpływ na wybór potencjalnego rozwiązania:

- wykorzystanie kluczy generowanych dla użytkowników tylko na potrzeby danej organizacji,
- wykorzystanie kluczy generowanych dla użytkowników na potrzeby danej organizacji oraz określonej liczby organizacji współpracujących,
- wykorzystanie kluczy generowanych dla użytkowników w celu identyfikacji publicznej,
- skutki prawne.

Proponowane rozwiązania implementacji architektury PKI dla przedsiębiorstw prezentowane są w tab. 1.

¹⁶ Ustawa o podpisie elektronicznym z dnia 18 września 2001 r., DzU, 2001, nr 130, poz. 1450, art. 3.

¹⁷ Przepisy odrębne mogą stanowić inaczej. Przykładowo testament musi być sporządzony własnoręcznie i własnoręcznie podpisany, dokument w postaci wydruku czy też maszynopisu podpisany własnoręcznie oraz dokument elektroniczny nie mają mocy prawnej jako testament.

Realizacja infrastruktury PKI na podstawie potrzeb organizacyjnych i prawnych przedsiębiorstw

Wyszczególnienie	Wykorzystanie kluczy generowanych dla użytkowników tylko na potrzeby danej organizacji	Wykorzystanie kluczy generowanych dla użytkowników na potrzeby danej organizacji oraz określonej liczby organizacji współpracujących	Wykorzystanie kluczy generowanych dla użytkowników w sieci Internet
Skutki prawne – identyfikacja osoby	1. Generowanie kluczy przez własny główny bądź zależny urząd certyfikacyjny. 2. Klucze użytkowników przechowywane na dowolnym nośniku.	1A. Generowanie kluczy przez własny główny bądź zależny urząd certyfikacyjny. Konieczność wzajemnego zaufania organizacji do własnych urzędów certyfikacyjnych. 1B. Generowanie kluczy przez jeden główny bądź zależny zaufany urząd certyfikacyjny przez współpracujące organizacje. 2. Klucze przechowywane na dowolnym nośniku.	1. Generowanie kluczy przez zewnętrzny urząd certyfikacyjny zaufany publicznie. 2. Klucze przechowywane na dowolnym nośniku.
Skutki prawne – złożenie podpisu na potrzeby jednej bądź kilku organizacji, bez równoważności z podpisem odręcznym	1. Generowanie kluczy przez własny główny bądź zależny urząd certyfikacyjny. 2. Klucze użytkowników przechowywane na dowolnym nośniku.	1A. Generowanie kluczy przez własny główny bądź zależny urząd certyfikacyjny. Konieczność wzajemnego zaufania organizacji do własnych urzędów certyfikacyjnych. Konieczność podpisania stosownych umów o uznawalności własnych, niekwalifikowanych certyfikatów. 1B. Generowanie kluczy przez jeden główny bądź zależny zaufany urząd certyfikacyjny przez współpracujące organizacje. 2. Klucze przechowywane na dowolnym nośniku.	Brak możliwości.

Tabela 1 (od.)

Skutki prawne – równoważne złożeniu odręcznego podpisu	1. Generowanie kwalifikowanego klucza przez autoryzowany urząd certyfikacyjny. 2. Klucz przechowywany na nośniku podlegającym wyłącznie kontroli właściciela certyfikatu.	1. Generowanie kwalifikowanego klucza przez autoryzowany urząd certyfikacyjny. 2. Klucz przechowywany na nośniku podlegającym wyłącznie kontroli właściciela certyfikatu.	1. Generowanie kwalifikowanego klucza przez autoryzowany urząd certyfikacyjny. 2. Klucz przechowywany na nośniku podlegającym wyłącznie kontroli właściciela certyfikatu.
--	--	--	--

Źródło: oprac. własne.

5. KWALIFIKOWANE CERTYFIKATY

Zgodnie z *Ustawą o podpisie elektronicznym* (DzU, 2001, nr 130, poz. 1450), bezpieczny podpis elektroniczny musi być złożony z wykorzystaniem kwalifikowanego certyfikatu. W Polsce głównym urzędem certyfikacji, certyfikującym pozostałych wystawców certyfikatów jest Narodowe Centrum Certyfikacji <http://www.nccert.pl>. Podmioty wydające certyfikaty kwalifikowane to: UNIZETO TECHNOLOGIES Spółka Akcyjna <http://www.certum.pl>, TP INTERNET Spółka z ograniczoną odpowiedzialnością <http://www.signet.pl>, KRAJOWA IZBA ROZLICZENIOWA Spółka Akcyjna <http://www.kir.pl>, POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH Spółka Akcyjna <http://www.pwpw.pl>.

Wydanie certyfikatu niezaufanego i niekwalifikowanego może być przeprowadzone na podstawie infrastruktury sieciowej danego przedsiębiorstwa. Systemy operacyjne Microsoft Windows 2000 i 2003 Server mogą być platformą do budowy centrum certyfikacyjnego (CA), z racji zaimplementowania odpowiednich usług jako integralnych komponentów systemu. Generowanie niekwalifikowanych certyfikatów na potrzeby własne przedsiębiorstwa na podstawie wspomnianych systemów operacyjnych nie wymaga poniesienia żadnych dodatkowych kosztów oprócz nabycia systemu operacyjnego. Jeżeli jednak podpis elektroniczny ma identyfikować użytkownika w sposób zaufany w Internecie, użytkownik musi otrzymać certyfikat z zaufanego urzędu certyfikacyjnego, jeżeli zaś skutki złożenia takiego podpisu mają być równoważne podpisowi odręcznemu, dodatkowo musi być wykorzystany certyfikat kwalifikowany. Przykładowo otrzymanie wydanego przez KIR SA¹⁸ certyfikatu niekwalifikowanego (ważnego 1 rok) zapisanego w pliku kosztuje 90 złotych netto, otrzymanie wydanego przez PWPW¹⁹ certyfikatu kwalifikowanego, zapisanego na karcie w zestawie z czytnikiem kosztuje 529 złotych netto. Z punktu widzenia przedsiębiorstwa wdrażającego infrastrukturę PKI, dokonywanie zakupu kwalifikowanych certyfikatów dla każdego pracownika może być znaczącym obciążeniem. Na potrzeby wewnętrzne organizacji wykorzystującej infrastrukturę PKI wystarczającym rozwiązaniem może być generowanie certyfikatów we własnym zakresie, natomiast zakup zaufanych certyfikatów dla pracowników reprezentujących firmę na zewnątrz jest koniecznym uzupełnieniem własnego rozwiązania.

¹⁸ Na podstawie cennika opublikowanego w Internecie http://www.kir.pl/certyfikacja_kluczy/cennik.html, 4.02.2006 r.

¹⁹ Na podstawie cennika opublikowanego w Internecie <http://www.sigillum.pl/index.php?d=15&aid=8>, przytoczono cenę dla „Zestawu kwalifikowanego PRO”, 4.02.2006 r.

6. PODSUMOWANIE

Wykorzystanie certyfikatów generowanych w ramach infrastruktury klucza publicznego jest dziś nieodzownym elementem zabezpieczającym transakcje elektroniczne. Certyfikaty mogą być generowane dla serwerów, tym samym potwierdzają ich wiarygodność. Użytkownik łącząc się z serwerem mającym certyfikat wydany przez zaufany urząd certyfikacyjny, ma pewność, że połączył się z prawidłowym serwerem. Osoby posiadające certyfikaty mogą być w ten sposób autentyfikowane wewnątrz własnej organizacji, osoby posiadające certyfikaty pochodzące od zaufanych wydawców mogą potwierdzać swoją tożsamość w sieci Internet. Osoby posługujące się kwalifikowanymi certyfikatami mogą składać podpis elektroniczny równoważny prawnie podpisowi odręcznemu. Należy jednak pamiętać, że podpis elektroniczny oparty jest na algorytmach skrótu danych – haszowania. W roku 2004 podano w wątpliwość wiarygodność algorytmu MD5²⁰, w roku 2005 podano w wątpliwość wiarygodność algorytmu kolizja SHA1²¹, co może być podstawą do podważenia wiarygodności danych poświadczonych podpisem elektronicznym.

Daniel Guga

E-COMMERCE SECURITY BASED ON PKI

(Summary)

Security of data is the most important factor in doing e-buissness today. Risk associated with loss of or compromise the data depends on the data type. Defining users' permission for different type of data is the core in network security planning and is based on identity of users. Eliminating potential threats to illegitimate access to resources could elevate security. This article presents risks, advantages and features of PKI in the field of users identity.

²⁰ <http://eprint.iacr.org/2004/199.pdf>, 1.02.2006 r.

²¹ <http://theory.csail.mit.edu/~yiqun/shanote.pdf>, 1.02.2006 r.