Ministerstwo Gospodarki

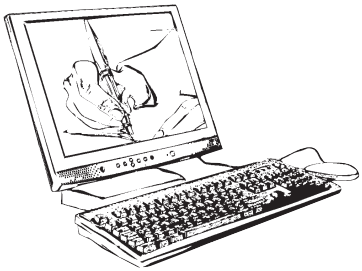
Podpis elektroniczny

Sposób działania, zastosowanie i korzyści

Warszawa 2005

Podpis elektroniczny

– sposób działania, zastosowanie i korzyści



Ministerstwo Gospodarki

Warszawa 2005

Nadzór merytoryczny:
Departament Przedsiębiorczości
Ministerstwa Gospodarki

Autorzy:
Artur Kruk – Unizeto Technologies SA
Piotr Matusiewicz – Unizeto Technologies SA
Jerzy Pejaś – Politechnika Szczecińska, Wydział Informatyki
Andrzej Ruciński – Unizeto Technologies SA
Wojciech Ślusarczyk – Unizeto Technologies SA

Konsultacja prawna:
Marek Aniszewski

Opracowanie graficzne:
Beata Świetlik

ISBN: 83-914536-5-0

Broszura dostępna jest na stronie internetowej Ministerstwa Gospodarki

Wydawca:
Ministerstwo Gospodarki
Departament Przedsiębiorczości
ul. Plac Trzech Krzyży 3/5, Warszawa 00-507
Tel. +22/ 628-09-81, Fax: +22/ 693-40-30, E-mail: sekretariatdwo@mg.gov.pl

Spis treści:

1. Wprowadzenie 5

2. Podpis elektroniczny 7
2.1 Elementy niezbędne do składania podpisu elektronicznego 7
2.2 Bezpieczne urządzenie do składania podpisu 12
2.3 Oprogramowanie 13
2.4 Technologia podpisu elektronicznego 14
2.5 Podpisywanie dokumentów elektronicznych 14
2.6 Weryfikacja podpisu 16
2.7 Szyfrowanie informacji 17
2.8 Znakowanie czasem 19
2.9 Podpis elektroniczny w praktyce
Konfiguracja przykładowych programów 21
2.10 Infrastruktura klucza publicznego
Zaufana Strona Trzecia
(rola, zaufanie w elektronicznej wymianie danych) 22
2.11 Bezpieczeństwo, jako czynnik dostarczany przez PKI 24
2.12 Elementy składowe PKI 25
2.13 Subskrybenci i strona ufająca: prawa i obowiązki 26
2.14 Zadania realizowane przez urzędy certyfikacji
Podstawowe funkcje PKI 27

3. Ramy prawne wykorzystywania podpisu elektronicznego 29
3.1 Podstawowe definicje i uregulowania 29
3.2 Skutki prawne bezpiecznego podpisu elektronicznego 30
3.3 Obowiązki podmiotów świadczących usługi certyfikacyjne 31
3.4 Zasady świadczenia usług certyfikacyjnych 32
3.5 Ważność certyfikatów 34
3.6 Przepisy karne 35
3.7 Podpis elektroniczny w prawie prywatnym 36
3.8 Prawne aspekty stosowania podpisu elektronicznego
w bankach i biurach maklerskich 38
3.9 Podpis elektroniczny w prawie publicznym 39

4. Obszary stosowania podpisu elektronicznego i usług znakowania czasem dokumentów elektronicznych 43
4.1 W biznesie 43
4.2 Banki 45
4.3 Ubezpieczenia 46

4.4 Inne sektory 46
4.5 W administracji publicznej 46
4.6 Dla obywatela 58

5. Korzyści płynące ze stosowania podpisu elektronicznego 51
5.1 Bezpieczeństwo 51
5.2 Usprawnienie działalności 51
5.3 Przyspieszenie realizacji zadań i obiegu informacji 52
5.4 Aspekt ekonomiczny - obniżenie kosztów funkcjonowania 53
5.5 Wypadkowa zastosowań podpisu elektronicznego 53

6. Bibliografia 55

1. Wprowadzenie

Możliwość przesyłania informacji drogą elektroniczną stanowi istotne ułatwienie funkcjonowania ludzi, przedsiębiorstw i urzędów. Internet pozwala prezentować w sieci katalogi produktów, przesyłać umowy, podania, wnioski o ich wzory. Dostęp do Internetu stał się powszechnym narzędziem wykorzystywanym w przedsiębiorstwach oraz gminach a jego dostępność wśród osób prywatnych ulega z roku na rok stałemu powiększeniu. Jaka jest zatem rola podpisu elektronicznego przy zawieraniu tą drogą umów, składaniu oświadczeń woli lub wysyłaniu podań?

Odpowiedź na to pytanie jest dosyć prosta. Internet jest medium anonimowym: założenie skrzynki poczty elektronicznej trwa kilka minut, a każdy edytor tekstu lub arkusz kalkulacyjny tworzą dokument bez wskazania na to, kto go przygotowuje. Z kopii dokumentu elektronicznego, a nawet na podstawie jego źródłowej wersji z reguły nie jesteśmy w stanie stwierdzić, kto jest autorem lub nadawcą dokumentu.

Do tych niedogodności dochodzą zagrożenia podczas „wędrówki" przesyłki przez Internet. Dokument elektroniczny przechwycony przez osobę nieuprawnioną traci poufność: informacje w nim zawarte przestają być wyłączną własnością nadawcy i adresata. Mogą one następnie zostać wykorzystane w sposób nieuczciwy w celu osiągnięcia korzyści, np. poprzez przejęcie kontraktu i zaoferowaniu niższej ceny.

Internet

Dzięki zastosowaniu podpisu elektronicznego możliwe jest poszerzenie obszarów wykorzystania Internetu

Przechwycona informacja elektroniczna może również zostać zmodyfikowana w sposób trudno zauważalny dla stron korespondencji. Pozornie niewinna zmiana treści – będąca w założeniu nawet tylko żartem - spowodować może wymierne straty finansowe dla dostawcy i odbiorcy oraz zakłócić dalszą współpracę między partnerami. Zagrożenie to stanowi jedno z największych ograniczeń w wykorzystaniu potencjalnych możliwości Internetu. Światowa sieć, dzięki swej dostępności, umożliwia bowiem kontakty nie tylko między podmiotami mającymi historię wzajemnych kontaktów gospodarczych, ale także pozwala na nawiązanie nowych relacji biznesowych. Trudno jest jednak podejmować ryzyko gospodarcze, nie wiedząc czy rozmowy prowadzi się z poważnym partnerem, reprezentującym wskazane przedsiębiorstwo, czy też ze zdolnym, acz „dowcipnym" nastolatkiem.

Ilustracja zagrożenia integralności danych

Ilustracja zagrożenia integralności danych: Firma A składa w Firmie B zamówienie na dostawę 100 elementów prefabrykowanych niezbędnych do zbudowania hali produkcyjnej. Termin dostawy elementów, zgodnie z harmonogramem prac, nie może być dłuższy niż dwa tygodnie. Zamówienie ma charakter typowy, Firma B wielokrotnie realizowała zlecenia o podobnych parametrach. W wyniku przechwycenia informacji przez osobę nieuprawnioną, Firma B otrzymuje zmienione zamówienie opiewające na 50 elementów z czasem dostawy trzy tygodnie.

Dla wielu informacji o charakterze biznesowym lub urzędowym, istotny jest czas ich opracowania bądź przesłania. Podpisanie umowy, przesłanie przelewu w warunkach zmiany kursów lub cen są typowymi przykładami „czułych" na termin sytuacji. Możliwość manipulacji czasem, poprzez zmianę ustawień w komputerze, otwiera drogę do ewentualnych nadużyć, których finał może mieć miejsce w sądzie. Zastosowanie podpisu elektronicznego z towarzyszącą mu usługą znakowania czasem pozwala uniknąć opisanych zagrożeń. Dzięki podpisowi elektronicznemu możliwe jest poszerzenie obszarów wykorzystania Internetu o kolejne zastosowania, zarezerwowane dotąd dla dokumentów papierowych.

Przykładowa sytuacja sporna

Przykładowa sytuacja sporna: Klient biura maklerskiego otrzymując informacje o spadku kursu posiadanych akcji wystawia zlecenie na ich sprzedaż po aktualnej cenie. Aby uniknąć strat finansowych, zmienia czas wystawienia zlecenia na taki, w którym kurs akcji był jeszcze dość wysoki. Makler, realizując otrzymane zlecenie w momencie jego otrzymania nie analizuje następstw czasowych. Po dokonaniu transakcji Klient domaga się pokrycia różnicy w cenie sprzedaży walorów. Makler nie dysponuje wiążącym dla sądu dowodem potwierdzającym czas wystawienia zlecenia.

2

2. Podpis elektroniczny

Od kilkudziesięciu lat naukowcy poszukiwali sposobu, w jaki dokumentowi elektronicznemu można nadać indywidualne cechy pochodzące od autora i zarazem możliwe do weryfikacji przez odbiorcę dokumentu. Jednocześnie zabiegano o zamodelowanie takiego sposobu weryfikacji, który przy zachowaniu poufności nie wymaga osobistego kontaktu stron i ich wzajemnej znajomości.

W połowie lat 70-tych XX wieku, naukowcy amerykańscy znaleźli metody spełniające powyższe oczekiwania (tzw. schematy podpisu cyfrowego). Stwierdzili m.in., że możliwe jest obliczenie dwóch takich liczb, że po zaszyfrowaniu dowolnego pliku z wykorzystaniem jednej z nich, odszyfrowaną postać pierwotną można uzyskać wyłącznie używając drugiej liczby z pary.

Aby opisane liczby mogły być używane do podpisywania dokumentów, należy wprowadzić dodatkowe zalecenie dla ich posiadacza. Jedna z liczb, nazywana **kluczem publicznym**, może i powinna być udostępniana każdemu zainteresowanemu (gdyż służy do sprawdzenia, kto podpisywał dokument), drugą zaś nazywaną **kluczem prywatnym**, użytkownik winien chronić przed ujawnieniem i pozostawić wyłącznie do własnej dyspozycji.

Celem niniejszego opracowania nie jest przedstawienie skomplikowanych wzorów matematycznych na dowód bezpieczeństwa i poprawności przyjętych schematów podpisu. Dlatego ograniczymy się do stwierdzenia, że podpis elektroniczny realizowany w technologii PKI (ang. Public Key Infrastructure – infrastruktura klucza publicznego) opiera się na przydzieleniu każdemu użytkownikowi pary opisanych wyżej kluczy oraz wirtualnego dokumentu potwierdzającego fakt posiadania konkretnych kluczy przez konkretną osobę. Sam podpis elektroniczny stanowi sposób kodowania danych, umożliwiający **identyfikację osoby**, która go złożyła oraz gwarantuje **integralność dokumentu**. Podpis elektroniczny nie służy do szyfrowania danych.

Zastosowanie dwóch różnych kluczy prywatnych (i związanych z nimi technik kryptograficznych) do podpisywania (klucz do podpisywania) i odczytywania (klucz do odszyfrowania) informacji w postaci elektronicznej znacznie podnosi poziom bezpieczeństwa informacji, uniemożliwiając tym samym osobom niepowołanym zarówno zmodyfikowanie, jak również zapoznanie się z treścią zabezpieczonej informacji.

2.1 Elementy niezbędne do składania podpisu elektronicznego

W rozdziale 3, prezentującym kwestie prawne dotyczące podpisu elektronicznego szczegółowo omówiono dwa rodzaje podpisu elektronicznego: bezpieczny podpis elektroniczny i zwykły podpis elektroniczny. Czynności wykonywane w trakcie składania obydwu rodzajów podpisu są identyczne. Różnice pojawiają się w odniesieniu do wymagań, jakie spełniać muszą urządzenia i oprogramowanie podpisujące w przypadku podpisu bezpiecznego.

Posługiwanie się bezpiecznym podpisem elektronicznym

Posługiwanie się bezpiecznym podpisem elektronicznym wymaga użycia komponentu technicznego (sprzętu) i oprogramowania podpisującego gwarantujących, że podpisywanym dokumentem jest ten, którego prezentację widzi podpisujący. Jednocześnie w trakcie składania podpisu zapewniona musi być należyta ochrona klucza prywatnego, uniemożliwiająca jego skopiowanie lub poznanie przez osoby niepowołane.

Przykładowe urządzenie do składania podpisu elektronicznego

Czytnik i karta

Dokument elektroniczny

Dokument elektroniczny kojarzy się przede wszystkim z komputerem. Warto jednak wiedzieć, że również inne urządzenia mogą służyć do składania oświadczenia woli drogą elektroniczną. Przykładowo jednym z urządzeń, które może służyć do składania podpisu elektronicznego są np. niektóre modele telefonów komórkowych.

Złożenie podpisu elektronicznego wymaga posługiwania się dokumentem w postaci cyfrowej (przesyłka e-mail lub plik np.: z Worda, Acrobata lub Excela). W przypadku, gdy podpisywane będą przesyłki poczty elektronicznej niezbędne jest posiadanie dostępu do Internetu. Jeżeli podpisywanymi obiektami mają być pliki zlokalizowane na konkretnym komputerze, dostęp do sieci może okazać się potrzebny dopiero w trakcie weryfikacji złożonego podpisu.

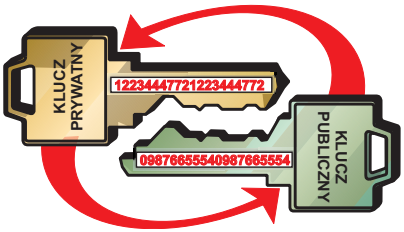
W przypadku serwisów internetowych oprócz funkcji związanych z wymianą dokumentów handlowych i zawarciem transakcji, istotnym elementem jest prezentowanie informacji, mających dostarczyć przesłanek do skorzystania z oferty konkretnych podmiotów. Wówczas kluczowe znaczenie ma certyfikacja serwera, z którego pobierane są informacje. Ustalenie, czy konkretny serwis WWW jest zarządzany przez dany podmiot, dokonywane jest w tej samej technologii, co podpis elektroniczny, z wykorzystaniem kluczy i certyfikatów przypisanych do serwerów. Dalszym rozszerzeniem schematu uwiarygodniania informacji udostępnianej klientom jest wyposażenie osób zainteresowanych uzyskaniem danych w atrybuty autoryzacyjne. Stosowanie certyfikatów przez klientów serwisów WWW tworzy bezpieczny, dwukierunkowy kanał wymiany danych.

Elementy wykorzystywane do składania podpisu są ściśle związane z samą technologią klucza publicznego. Ze względu na przejrzystość opisu i spójność pojęciową zostaną tu opisane:

- klucz prywatny i klucz publiczny,
- certyfikat, czyli dokument elektroniczny potwierdzający przynależność pary kluczy do konkretnego użytkownika, wydawany przez podmiot zwany urzędem certyfikacji,
- nośnik kluczy i certyfikatu.

Czym są klucze?

Klucze są liczbami całkowitymi o określonej, bezpiecznej długości



Klucze są liczbami całkowitymi o określonej, bezpiecznej długości

Klucze to liczby całkowite, o określonej, bezpiecznej długości. Przykładowo dla algorytmu RSA (od nazwisk twórców Rivest, Shamir, Adleman) przyjmuje się, że dla zapewnienia wiarygodności i bezpieczeństwa podpisu mierzonego odpornością klucza na jego „złamanie" metodą prób i błędów, długość liczby zapisanej w systemie dwójkowym (czyli wyłącznie przy zastosowaniu zer i jedynek) nie powinna być krótsza niż 1024 cyfry.

Tworzenie i dystrybucja kluczy, w szczególności klucza prywatnego, musi być dokonana w taki sposób, aby użytkownik miał pewność, że jest jego wyłącznym posiadaczem. Oznacza to, że w żadnym momencie swej ważności klucz prywatny nie może być dostępny lub podatny na ingerencję osób trzecich. Dlatego też najbezpieczniej jest generować klucze bądź na komputerze użytkownika, bądź bezpośrednio na mikroprocesorowej karcie kryptograficznej.

Klucze prywatny i publiczny

Klucze prywatny i publiczny, oprócz sytuacji, w których są generowane przez użytkownika, mogą być tworzone bezpośrednio w urzędzie certyfikacji. W takim przypadku wykorzystane są karty mikroprocesorowe z kryptoprocesorem (klucze generowane są wewnątrz karty i pozostają tam aż do ich zniszczenia) lub tzw. sprzętowe moduły kryptograficzne, czyli specjalne urządzenia, które potrafią przesłać wygenerowane klucze na kartę mikroprocesorową. Konstrukcja modułów uniemożliwia przejęcie przez kogokolwiek innego klucza prywatnego.

Proces generowania kluczy realizowany jest w ścisłej współpracy z wydawcą certyfikatów. Najczęściej stosowanym wariantem jest składanie wniosku o wydanie certyfikatu za pośrednictwem Internetu. Urząd certyfikacji udostępnia na swoich stronach formularze, przy pomocy których użytkownik podaje swoje dane osobowe i tworzy tzw. żądanie wydania certyfikatu. Następnie żądanie, wraz z kluczem publicznym i dowodem posiadania przez użytkownika odpowiadającego mu klucza prywatnego, przesyłane jest drogą elektroniczną do urzędu certyfikacji.

W kolejnym kroku urząd certyfikacji podejmuje czynności związane ze sprawdzeniem spójności i prawdziwości przesłanych danych. Spójność danych weryfikowana jest z reguły automatycznie. Obejmować ona może m.in. istnienie w sieci adresu poczty elektronicznej podanego w formularzu oraz zgodność numeru PESEL z datą urodzenia. Weryfikacja tożsamości wiąże się z potrzebą dodatkowego uwiarygodnienia podanych w formularzu informacji. Ponieważ dla różnych rodzajów certyfikatów określone są odmienne zasady potwierdzania danych, wymagania urzędu certyfikacji są zróżnicowane, a mianowicie mogą to być:

- przesłanie fotokopii dowodu osobistego listem zwykłym,
- przesłanie notarialnie potwierdzonych kopii dowodu osobistego lub innego dokumentu listem poleconym,
- osobiste stawiennictwo w urzędzie certyfikacji lub punkcie rejestracji (przedstawicielstwo urzędu certyfikacji, którego rola i zadania zostały szerzej zdefiniowane w dalszej części broszury) i okazanie dokumentów przedstawicielowi wydawcy certyfikatu.

W przypadku pozytywnego zakończenia weryfikacji - po uregulowaniu przez subskrybenta opłaty - urząd certyfikacji wydaje mu certyfikat. Certyfikat umieszczany jest jednocześnie na stronach internetowych (dokładniej, w repozytorium) wydawcy tak, aby mógł być pobierany i instalowany przez innych użytkowników, w celu weryfikacji prawidłowości podpisu składanego przez subskrybenta lub kodowania danych dla niego przeznaczonych.

Zasady wydawania oraz wymagania dla certyfikatów i kwalifikowanych certyfikatów określone zostały w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (zwanej dalej ustawą) oraz w rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia 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*. Wynika z nich, że wydanie certyfikatu (nie tylko kwalifikowanego) musi być poprzedzone m.in.:

- stwierdzeniem tożsamości osoby ubiegającej się o certyfikat,
- zawarciem umowy na świadczenie usług certyfikacyjnych z dostawcą tych usług,
- poinformowaniem wnioskodawcy o cechach żądanego certyfikatu, jego stosowaniu i skutkach użycia.

Wydanie kwalifikowanego certyfikatu wymaga osobistego stawienia się w punkcie rejestracji. Są jednak dwa wyjątki. Pierwszy pozwala na posłużenie się notarialnym potwierdzeniem tożsamości. Drugi wyjątek ma zastosowanie wtedy, gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat. Wtedy na podstawie rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 *potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez ten sam podmiot i w ramach tej samej polityki certyfikacji*. Wspominany już kilkukrotnie certyfikat klucza publicznego jest wirtualnym **„dowodem tożsamości" osoby wyposażonej w parę kluczy używanych do składania podpisu elektronicznego.**

Powszechnie stosowanym standardem opisującym zawartość certyfikatu jest norma ISO/IEC 9594-8, nazywana często w skrócie normą X.509.

Podstawowe informacje zapisane w certyfikacie to:

- określenie właściciela (posiadacza certyfikatu) - poprzez podanie, np. imienia i nazwiska, bądź pseudonimu oraz kraju pochodzenia,
- wskazanie wydawcy certyfikatu (urzędu certyfikacji),
- wskazanie - poprzez podanie odpowiedniego identyfikatora - polityki certyfikacji, czyli zbioru reguł określających sposób postępowania wydawcy przy wydawaniu certyfikatu określonego typu,

- wskazanie okresu ważności certyfikatu opisane datami wydania certyfikatu i momentem utraty przez niego ważności.

Dodatkowo w certyfikacie zapisane być mogą dane związane z pracą wykonywaną przez jego posiadacza:

- nazwa firmy-pracodawcy,
- wskazanie komórki organizacyjnej,
- zajmowane stanowisko,
- uprawnienia do podejmowania zobowiązań finansowych do określonej kwoty.

Certyfikat klucza publicznego podpisany jest kluczem prywatnym urzędu certyfikacji.

Struktura kwalifikowanego certyfikatu nie różni się zbytnio od certyfikatu zwykłego, a nawet może być dokładnie taka sama. Różnicę między oboma podstawowymi typami certyfikatów stanowi ich zawartość. Najważniejsza różnica to ustawowy wymóg wskazania, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji (art. 20 ust.1 ustawy o podpisie elektronicznym). Druga różnica dotyczy wymagań dotyczących identyfikatora wydawcy certyfikatu i subskrybenta. Identyfikator wydawcy musi składać się przynajmniej z: nazwy kraju, nazwy organizacji i numeru seryjnego. Z kolei postać identyfikatora subskrybenta może należeć do jednej z trzech dozwolonych kategorii. Na przykład kategoria trzecia pozwala subskrybentowi na posługiwanie się pseudonimem, w miejsce imienia i nazwiska oraz innych danych osobowych.

Wygenerowane klucze i otrzymany od danego urzędu certyfikacji certyfikat muszą być przechowywane przez subskrybenta w sposób bezpieczny. Decyzja odnośnie wyboru nośnika kluczy należy do użytkownika i jest ściśle związana z przewidywanym zakresem używania certyfikatu. Klucze i certyfikat mogą się znajdować:

bezpośrednio w rejestrach systemu operacyjnego komputera – wariant taki może być zaakceptowany w sytuacji, gdy komputer jest urządzeniem wykorzystywanym jedynie przez właściciela danych służących do składania podpisu elektronicznego. W przeciwnym wypadku podpis elektroniczny dokumentu potwierdza jedynie, że został on złożony na konkretnej stacji roboczej. Brak jest przesłanek wskazujących operatora urządzenia, który zainicjował czynność podpisu. Z punktu widzenia posiadacza certyfikatu występuje dodatkowe zagrożenie podjęcia w jego imieniu prawnie ważnych zobowiązań przez osobę trzecią.

na nośniku wymiennym, np. na dyskietce, płycie optycznej lub nośnikach dla łącza USB - rozwiązanie to pozwala wyeliminować niebezpieczeństwa występujące przy przechowywaniu kluczy w rejestrze komputera. Nie jest jednak wygodne dla użytkownika, gdyż wymaga przenoszenia certyfikatu do stacji roboczej na czas składania podpisu. Podstawową wadą opisywanej metody jest bardzo słaba ochrona klucza prywatnego - może on zostać łatwo skopiowany i wykorzystany przez osoby nieuprawnione.

na karcie mikroprocesorowej z koprocesorem kryptograficznym (tzw. kryptoprocesorem) - rozwiązanie takie zapewnia najwyższy stopień ochrony zapisanych składników. Nie istnieje metoda pobrania z karty klucza prywatnego. Klucz prywatny nie opuszcza karty nawet w trakcie składania

podpisu bądź szyfrowania informacji. Wszystkie czynności realizowane są bowiem bezpośrednio na karcie, a na zewnątrz, do komputera przekazywane są tylko wyniki wykonanych operacji kryptograficznych (np. zaszyfrowany skrót wiadomości).

Wybór sposobu przechowywania kluczy i certyfikatu wiązać się może z koniecznością dodatkowego wyposażenia stacji roboczej, za pomocą której składany jest podpis elektroniczny. O ile dwa pierwsze z opisanych powyżej wariantów obsługiwane są przez typowe komputery, o tyle wybór karty jako nośnika kluczy i certyfikatu wiąże się z instalacją czytnika kart i odpowiednich sterowników.

Obowiązek informacji o zalecanych kartach i czytnikach

Wydawcy certyfikatów zwykłych z reguły informują jakiego rodzaju karty i czytniki są przez nich zalecane do przechowywania oraz obsługi kluczy i certyfikatów. Urzędy certyfikacji zajmujące się wydawaniem kwalifikowanych certyfikatów, służących do składania bezpiecznego podpisu elektronicznego mają obowiązek publikacji pełnego wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych oraz warunków technicznych, jakim urządzenia te powinny odpowiadać.

Należy pamiętać, że samo istnienie certyfikatu nie informuje o poziomie bezpieczeństwa złożonego podpisu. Przy korzystaniu z podpisanego elektronicznie dokumentu należy zapoznać się z informacjami przechowywanymi wewnątrz podpisu elektronicznego, m.in. z zawartością certyfikatu związanego z podpisem. Pracownicy podmiotów i urzędów będący odbiorcami podpisanych elektronicznie dokumentów powinni zostać przeszkoleni pod kątem weryfikacji podpisu elektronicznego oraz jego treści, jak również sposobu przechowywania klucza publicznego i danych potrzebnych do późniejszej weryfikacji dokumentów.

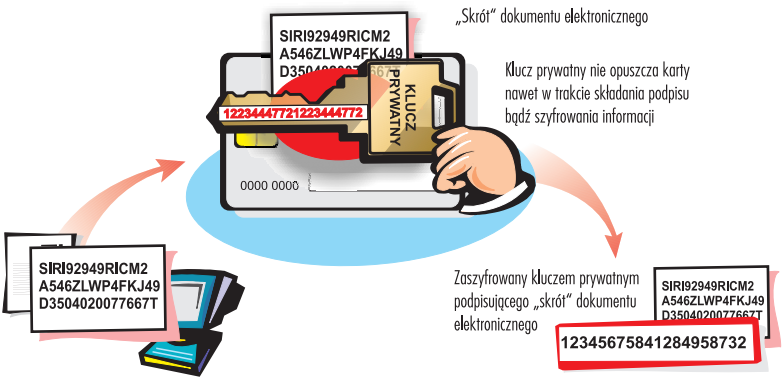
Ustawa o podpisie elektronicznym i wydane na jej podstawie akty wykonawcze określają wymagania jakie spełnić musi komponent techniczny wykorzystywany do składania bezpiecznego podpisu elektronicznego. Ze względu na sposób ochrony klucza oraz miejsce realizacji operacji kryptograficznych jednym z rodzajów komponentu, obecnie najbardziej popularnym, spełniającym wspomniane wymagania, są kryptograficzne karty mikroprocesorowe posiadające stosowne certyfikaty.

2.2 Bezpieczne urządzenie do składania podpisu

Aby podpisać elektronicznie dokument, w sposób autentyczny, niezaprzeczalny i co najważniejsze bezpieczny należy zastosować tzw. bezpieczne urządzenie do składania podpisu elektronicznego. Urządzenie takie składa się z oprogramowania podpisującego oraz współpracującego z nim komponentu technicznego. Komponentem technicznym jest moduł kryptograficzny, w którym następuje proces szyfrowania danych, przy zachowaniu zasady, że klucz kryptograficzny nie opuszcza tego modułu w trakcie wykonywania operacji składania podpisu. Dzięki specjalnej konstrukcji modułu kryptograficznego nie można z niego wydobyć, ani zamienić w jego wnętrzu kluczy. Przykładem takich urządzeń są moduły produkowane m.in. przez firmy nCipher czy CompCrypt. Moduły kryptograficzne stosowane są głównie w urzędach certyfikacji.

Innym rodzajem komponentów technicznych są mikroprocesorowe karty kryptograficzne. Są one najbardziej popularne, ze względu na stosunkowo niską cenę, zdolność do współpracy z popularnymi systemami operacyjnymi (m.in. rodzina MS Windows) oraz rozmiary samego komponentu.

Wszystkie urządzenia mające służyć do składania bezpiecznego podpisu elektronicznego powinny posiadać certyfikaty bezpieczeństwa i deklaracje zgodności z wymienionymi w bibliografii standardami.



Oprogramowanie podpisujące jest ściśle związane z komponentem technicznym i realizuje zadania związane z:

- przygotowaniem danych, które mają być podpisane,
- zapewnieniem takiej komunikacji z komponentem technicznym, aby transmitowane do niego dane odpowiadały danym, które mają być podpisane,
- tworzeniem podpisu elektronicznego w różnych formatach.

Oprogramowanie podpisujące nie wyłącza kontroli systemu operacyjnego nad komputerem i systemem plików, jak również nie blokuje możliwości działania makropoleceń w edytorach tekstu. O ile aplikacja podpisująca uniemożliwia fałszowanie podpisu lub zmianę danych do podpisu przygotowanych przez podpisującego na inne, podmienione przez wrogie oprogramowanie (np. wirusy, konie trojańskie, robaki sieciowe), to nie każde środowisko składania e-podpisu zapewnia podobny poziom bezpieczeństwa. Użytkownik powinien mieć zawsze pewność, że podpisuje to co widzi, lub przynajmniej to co chce podpisać. Chociaż oprogramowanie podpisujące powinno prezentować wizualnie prawdziwe dane przed ich podpisaniem to w praktyce jest to trudne do wykonania. Krajowe rozwiązania w tym zakresie nie odbiegają poziomem bezpieczeństwa od przyjętych w Unii Europejskiej (por. pkt. 6.5 oraz 9.4 w dokumencie CWA 14170). **Zasadnicze znaczenie przy składaniu podpisu elektronicznego ma więc zachowanie należytej staranności w zakresie zabezpieczenia środowiska w którym będzie on składany, w tym m.in. przez stosowanie łat systemu operacyjnego, programów antywirusowych i firewalla oraz najnowszej wersji programu do tworzenia i weryfikacji podpisów elektronicznych. Nadmienić należy, że również w przypadku podpisu odrecznego nie można wykluczyć ewentualnego nadużycia.**

2.3 Oprogramowanie

Oprogramowanie wykorzystujące klucze prywatne i publiczne oraz certyfikaty klucza publicznego jest niezwykle popularne wśród użytkowników sieci globalnej. Umożliwia ono bowiem nawiązanie bezpiecznej komunikacji między dwoma, dowolnymi punktami w Internecie, zawieranie transakcji elektronicznych, przesyłanie poufnych danych

oraz dystrybucję oprogramowania, bez obawy o jego sfałszowanie bądź zarażenie wirusem. Oprogramowaniem tego typu jest przede wszystkim przeglądarka internetowa (np. Internet Explorer, Mozilla czy Opera) oraz programy do obsługi poczty elektronicznej (np. Lotus Notes, Novell GroupWise, Outlook Express, TheBat!). Popularne oprogramowanie biurowe (np. Adobe Acrobat, Microsoft Office XP) również posiadają wsparcie procesu składania podpisu elektronicznego, który zabezpieczy utworzone na ich bazie dokumenty. Wielu producentów oprogramowania przygotowało również dla użytkowników końcowych „wtyczki" (ang. plug-in) integrujące się ze standardowymi procesorami tekstów.

2.4 Technologia podpisu elektronicznego

Podpis elektroniczny – definicja ustawowa

PODPIS ELEKTRONICZNY – definicja ustawowa (Art. 3 Ustawy z dnia 18 września 2001r. o podpisie elektronicznym, Dz. U. Nr 130, Poz.1450 , z dnia 15.11.2001r.):

1) podpis elektroniczny – 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,
2) bezpieczny podpis elektroniczny - podpis elektroniczny, 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 i danych służących do składania podpisu elektronicznego.

2.5 Podpisywanie dokumentów elektronicznych

Sposób składania podpisu elektronicznego z wykorzystaniem algorytmu szyfrowego RSA i schematu podpisu z załącznikiem (opis schematu można znaleźć np. w PN-ISO/IEC 14888-1:2000 *Technika informatyczna - Techniki zabezpieczeń - Podpis cyfrowy z załącznikiem - Opis ogólny*) ilustrują zamieszczone poniżej rysunki. Czynności opisane jako wykonywane przez składającego podpis faktycznie realizowane są przez oprogramowanie. Od strony użytkownika złożenie podpisu wiąże się z wydaniem jednego polecenia przekazywanego przez naciśnięcie odpowiedniego przycisku widocznego na monitorze komputera.

Dokument elektroniczny widziany przez nas w zrozumiałej postaci na ekranie komputera jest w jego pamięci zapisany jako ciąg zer i jedynek. Pierwszym etapem składania podpisu (z punktu widzenia wykonywanych operacji) jest obliczenie tzw. skrótu dokumentu, czyli charakterystycznej dla niego liczby o określonej długości, zależnej od użytej funkcji skrótu.

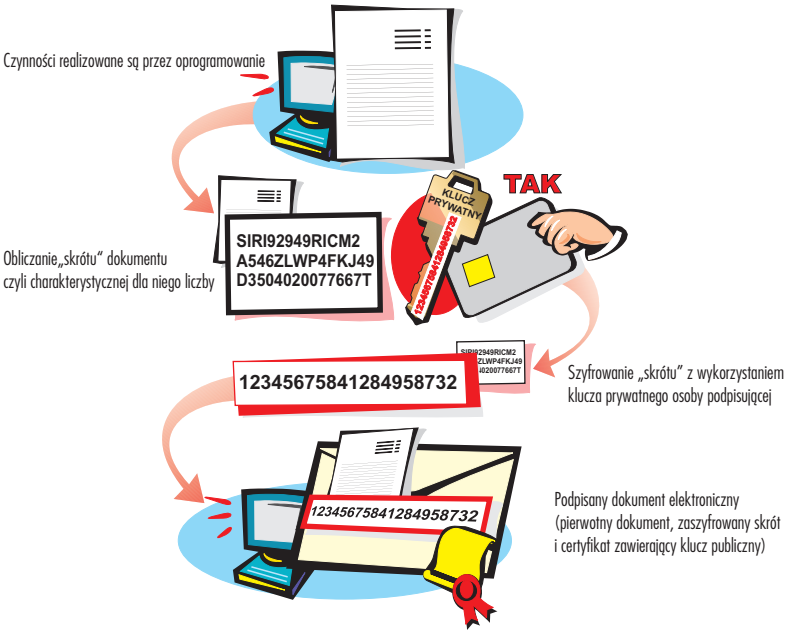
Kolejnym etapem konstruowania podpisu jest szyfrowanie uzyskanego skrótu przy wykorzystaniu klucza prywatnego osoby podpisującej. W trakcie wykorzystywania klucza prywatnego użytkownik proszony jest o udzielenie zgody na takie użycie. W praktyce wyrażenie zgody jest równoważne np. z podaniem kodu PIN karty, na której znajdują się klucze. Po zaszyfrowaniu skrótu dokument elektroniczny jest już podpisany.

Funkcja skrótu

Funkcja skrótu spełnia rolę podobną do „odcisku palca" (i tak jest czasami nazywana). Umożliwia ona powiązanie wiadomości o dowolnej długości z charakterystyczną dla tej wiadomości liczbą z ustalonego zakresu, o określonej długości reprezentacji liczby w przyjętym systemie zapisu – dziesiętnym, binarnym lub innym. „Dobra" funkcja skrótu wykorzystywana w kryptografii jest funkcją jednokierunkową, tzn. obliczanie wartości tej funkcji dla dowolnej wiadomości powinno być łatwe, lecz odtworzenie na podstawie wartości funkcji skrótu domniemanej wiadomości pierwotnej jest problemem trudnym obliczeniowo. Ponadto dla „dobrej" funkcji skrótu problemem trudnym obliczeniowo jest wyznaczenie dwóch wiadomości o tej samej wartości funkcji skrótu.

Podpisywanie dokumentów elektronicznych

Podpisywanie dokumentów elektronicznych



Podpisanym dokumentem elektronicznym jest dokument pierwotny wraz z załączonym do niego zaszyfrowanym skrótem. Opcjonalnie w skład podpisu może wchodzić również certyfikat osoby podpisującej, zawierający jej klucz publiczny oraz informacja o tym, czy certyfikat był ważny w momencie podpisywania dokumentu.

Różnice pomiędzy podpisem bezpiecznym, a zwykłym

Różnice pomiędzy bezpiecznym podpisem, a podpisem zwykłym można rozpatrywać w trzech płaszczyznach:

- technologii realizacji podpisu,
- powiązania z certyfikatem,
- odpowiedzialności prawnej.

Dwa pierwsze aspekty wymagają, aby bezpieczny podpis został złożony za pomocą bezpiecznego urządzenia do składania podpisu i przy użyciu klucza prywatnego, komplementarnego z kluczem publicznym, umieszczonym w certyfikacie, wydanym osobie ten podpis składającej. Podpis zwykły nie musi spełniać wymogów dotyczących urządzenia.

W zakresie odpowiedzialności prawnej jedynie bezpieczny podpis złożony na dokumencie elektronicznym może być równoważny pod względem skutków prawnych podpisowi własnoręcznemu złożonemu na dokumencie papierowym, o ile poprawność bezpiecznego podpisu można zweryfikować za pomocą certyfikatu kwalifikowanego należącego do podmiotu składającego podpis (Art. 5. 2 Ustawy z dnia 18 września 2001 o podpisie elektronicznym). Tego rodzaju bezpieczny podpis elektroniczny weryfikowany za pomocą certyfikatu kwalifikowanego nazywany jest często kwalifikowanym podpisem elektronicznym.

2.6 Weryfikacja podpisu

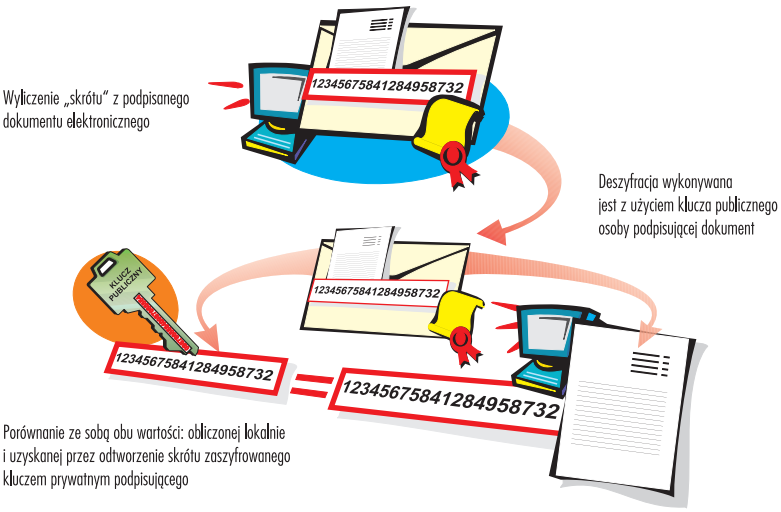
Sprawdzenie podpisu elektronicznego obejmuje weryfikację w dwu płaszczyznach. Uzyskanie pozytywnego wyniku na poziomie technologii daje odbiorcy dokumentu informację o tym, czy dokument zachował od momentu podpisania integralność (tzn. czy nie została zmieniona jego treść) oraz, że dokument był podpisany przy użyciu atrybutów należących do konkretnej osoby. Obie wymienione cechy są sprawdzane w sposób łączny i wykrycie błędu w procesie weryfikacji nie wskazuje, jakiego typu naruszenie dokumentu nastąpiło.

Drugim poziomem sprawdzenia podpisu jest stwierdzenie, czy podpis został złożony z wykorzystaniem kluczy posiadających ważny certyfikat. Od strony formalnej jest to równoznaczne ustaleniu czy w momencie składania podpisu może zachodzić domniemanie, że jedynym posiadaczem kluczy był ich prawowity właściciel. W praktyce, weryfikacja drugiego poziomu związana jest ze sprawdzeniem u wydawcy, czy certyfikat nie został unieważniony (np. z powodu zagubienia lub kradzieży nośnika klucza prywatnego) przed złożeniem podpisu elektronicznego.

Weryfikacja podpisu dokumentu elektronicznego na poziomie technologicznym, złożonego przy wykorzystaniu algorytmu RSA, została zilustrowana na poniższym rysunku.

Weryfikacja podpisu

Weryfikacja podpisu



Program odbiorcy podpisanego dokumentu elektronicznego wykonuje sekwencję następujących czynności:

- wylicza skrót z podpisanego dokumentu elektronicznego. Jest to czynność identyczna z funkcją realizowaną przez program osoby podpisującej dokument,
- deszyfruje zaszyfrowany skrót z wiadomości, będący częścią podpisanego dokumentu elektronicznego - deszyfrowanie wykonywana jest z użyciem klucza publicznego osoby podpisującej dokument. Klucz publiczny może zostać pobrany

z certyfikatu załączonego do podpisywanego dokumentu lub bezpośrednio ze stron wydawcy,

- porównuje ze sobą obie wartości: obliczoną lokalnie i uzyskaną poprzez odtworzenie skrótu zaszyfrowanego kluczem prywatnym podpisującego.

O ile sprawdzenie ważności podpisu od strony technologicznej może być realizowane w trybie off-line, gdyż wszystkie niezbędne komponenty zawarte są w weryfikowanym dokumencie, o tyle sprawdzenie ważności certyfikatu wymaga kontaktu z urzędem certyfikacji.

Ważność certyfikatu może być weryfikowana w dwu trybach. Podjęcie decyzji o wyborze jednego z nich uwarunkowane jest tym, jaki przedział czasu, w którym mogło mieć miejsce unieważnienie certyfikatu uznajemy za wystarczający do uznania otrzymanego dokumentu za ważny. W przypadku szybko przebiegających transakcji, realizowanych na przykład na handlowych platformach internetowych lub na rynkach giełdowych powinniśmy być zainteresowani uzyskaniem informacji możliwie najbardziej aktualnej (liczonej w minutach lub sekundach). Dla odróżnienia weryfikacja dotycząca otrzymanej umowy handlowej, zawieranej ze znanym nam partnerem handlowym, może być prowadzona z przyjęciem horyzontu czasowego mierzonego w dniach.

Certyfikat klucza publicznego

Certyfikat klucza publicznego w chwili jego wydania subskrybentowi otrzymuje status Ważny (ang. Valid). Posiadacz certyfikatu, w przypadku stwierdzenia utraty wyłącznej kontroli nad swym kluczem prywatnym (np. na skutek zagubienia nośnika) może żądać jego unieważnienia. W momencie zgłoszenia żądania certyfikat otrzymuje status Unieważniony (ang. Revoked), a wydawca certyfikatów publikuje nową wersję listy certyfikatów unieważnionych (CRL, ang. Certificate Revocation List).

Praktycznie weryfikacja ważności certyfikatu realizowana jest następująco:

- jeżeli nie istnieje możliwość kontaktu z serwerem wydawcy certyfikatu program korzysta z ostatnich posiadanych list CRL, lub informuje, że nie jest w stanie sprawdzić, czy certyfikat używany do podpisu nie został unieważniony.
- sytuacji gdy odbiorca informacji jest w stanie połączyć się z serwerem urzędu certyfikacji, program może dokonać aktualizacji list CRL, lub przesłać zapytanie do serwera o aktualny status certyfikatu. W przypadku sprawdzania statusu w trybie on-line (protokół OCSP, ang. Online Certificate Status Protocol) serwer wydawcy przesyła pytającemu podpisany dokument elektroniczny zawierający żądaną informację. Zaświadczenie takie może być wykorzystane jako materiał dowodowy w przypadku sporu dotyczącego ważności podpisanego dokumentu.

2.7 Szyfrowanie informacji

Szyfrowanie dokumentu elektronicznego przeznaczonego dla konkretnego odbiorcy jest procesem realizowanym w nieco inny sposób niż podpisywanie dokumentu. O ile podpis elektroniczny realizowany jest z wykorzystaniem własnego klucza prywatnego, o tyle do szyfrowania należy skorzystać z publicznego klucza odbiorcy.

Nie wszystkie algorytmy szyfrowe stosowane do składania podpisu elektronicznego mogą być także stosowane do szyfrowania za pomocą klucza publicznego. Ograniczenie to nie dotyczy jednak wspomnianego już wielokrotnie algorytmu RSA.

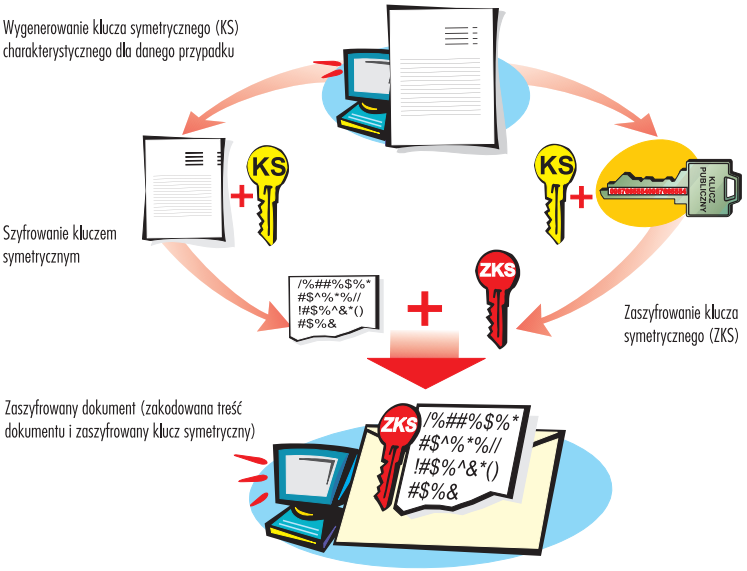
Jednak algorytmy asymetryczne, w których szyfrowanie danych wykonywane jest przy użyciu jednego z pary kluczy, zaś ich deszyfrowanie przy pomocy drugiego, nie są zbyt wydajne. W trakcie podpisywania wiadomości kodowany jest jedynie jej skrót, a sama wiadomość przesyłana jest w postaci jawnej. Szyfrowanie całej treści dokumentu mogłoby trwać bardzo długo. Dlatego też w praktyce do szyfrowania

treści wykorzystuje się inne metody, zwane algorytmami symetrycznymi (kodowanie i dekodowanie informacji wykonywane jest z użyciem tego samego klucza kryptograficznego, który po zaszyfrowaniu za pomocą klucza publicznego odbiorcy dołączany jest do przesyłki i przekazywany odbiorcy).

Proces szyfrowania ilustruje poniższy rysunek.

Szyfrowanie informacji

Szyfrowanie informacji



Pierwszą realizowaną czynnością jest wygenerowanie unikalnego, innego dla każdego przypadku szyfrowania, klucza symetrycznego. Przy użyciu tego klucza zaszyfrowana zostaje treść informacji. Następnie klucz symetryczny jest szyfrowany przy pomocy klucza publicznego odbiorcy.

Kompletny zaszyfrowany dokument składa się więc z:

- zaszyfrowanej treści dokumentu oraz
- zaszyfrowanego klucza symetrycznego.

Odbiorca zaszyfrowanej informacji, chcąc poznać jej treść, wykonuje następujące czynności:

- deszyfruje zaszyfrowany klucz symetryczny,
- używając klucza symetrycznego deszyfruje dokument pierwotny.

W praktyce operacje te inicjowane są jednym poleceniem i wykonywane przez używany program.

Każdy dokument elektroniczny może być jednocześnie zaszyfrowany i podpisany. W takim przypadku dokument jest najpierw podpisywany, a dopiero później szyfrowany. Szyfrowanie całego dokumentu zapewnia poufność przekazywanych danych, ale nie jest konieczne dla ważności złożonego podpisu elektronicznego.

2.8 Znakowanie czasem

Podstawowym celem usługi znakowania czasem (ang. time stamping) jest zabezpieczanie długookresowych podpisów elektronicznych oraz transakcji finansowych realizowanych za pośrednictwem sieci globalnej. Znacznik czasu jest elektronicznym odpowiednikiem datownika wiążącym czas z dowolnymi danymi (n.p. dokumentami, podpisami elektronicznymi, transakcjami finansowymi itd.) zapisanymi w postaci skrótu kryptograficznego i w sposób umożliwiający ich uporządkowanie. Usługa znakowania wiarygodnym czasem (tzn. pochodzącym ze źródła niezależnego od autora dokumentu) jest niezbędne przy realizacji usługi niezaprzeczalności (ang. non-repudiation).

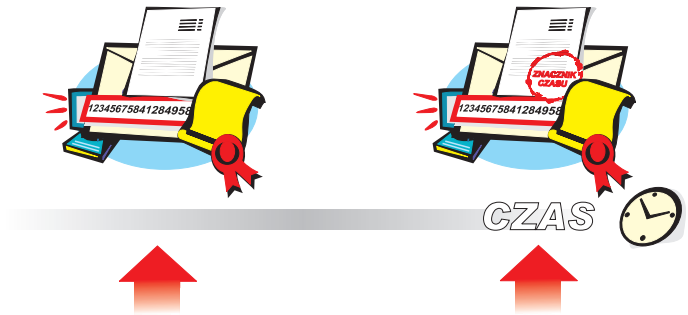
Powiązanie znacznika czasu z danymi polega na dodaniu do nich elementu, który dowodzi, że dane zostały utworzone przed, po lub w ściśle określonym momencie czasu. Dzięki tej właściwości możliwe staje się wskazanie dokładnego czasu zajścia określonego zjawiska, takiego jak utworzenie dokumentu lub złożenie podpisu elektronicznego.

Powiązania opisanego wyżej typu realizowane są przez urząd znacznika czasu (TSA, ang. Time-Stamping Authority). Podstawowe zadania urzędu obejmują:

- dostarczanie elektronicznego poświadczenia (ang. token) o istnieniu i autentyczności danych,
- stworzenie możliwości zweryfikowania, czy podpis elektroniczny dokumentu został złożony jeszcze przed unieważnieniem klucza użytego do podpisu.

Znacznik czasu

Znacznik czasu



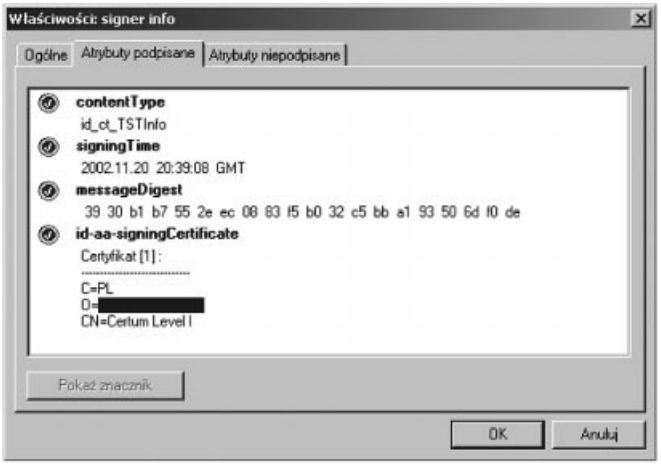
Utworzenie podpisu pod dokumentem

Oznaczenie podpisanego dokumentu wiarygodnym czasem przez Urząd Znacznika Czasu

Na rysunku przedstawiono przypadek oznaczenia wiarygodnym czasem zarówno samego dokumentu, jak też podpisu pod tym dokumentem. Proces znakowania czasem polega na:

- wysłaniu żądania do urzędu TSA,
- pobraniu znacznika czasu oraz
- umieszczenie pobranego znacznika czasu w strukturze podpisu elektronicznego dokumentu.

Dzięki realizacji takiej procedury istnieje możliwość udowodnienia, że:
(a) podpis pod określonym dokumentem został złożony w okresie wyznaczonym przez czas zapisany w znaczniku,
(b) dokument jest autentyczny i nie został zmodyfikowany po oznaczeniu czasem oraz dodatkowym podpisaniu go przez właściciela. Znacznik taki jest przydatny w trakcie rozstrzygania sporu, co do czasu utworzenia dokumentu.



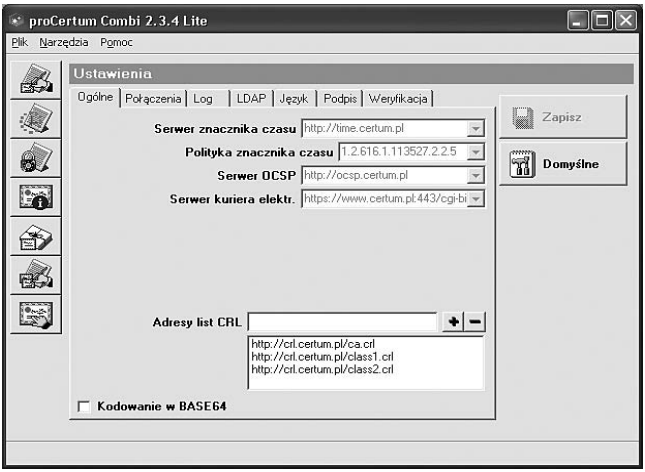
Urzędy TSA, świadczące publiczne usługi oznaczania wiarygodnym czasem działają zgodnie z zasadami opisanymi w politykach oznaczania czasem. Zgodność praktyk z polityką oznaczania czasem oraz standardami międzynarodowymi powinna być potwierdzona przez niezależnych audytorów.

Aby prawidłowo świadczyć usługi urzędy TSA korzystają z tzw. źródeł czasu, które są oficjalnymi zegarami kraju, na terenie którego dany urząd świadczy usługi, bądź stanowią część globalnego systemu atomowych zegarów czasu uniwersalnego (UTC, ang. Universal Time Coordinated). W Polsce oficjalnymi źródłami czasu są serwisy internetowe Głównego Urzędu Miar. Maksymalna różnica czasu między czasem uniwersalnym, a czasem systemowym urzędu TSA nie powinna być większa niż 1s. Urzędy TSA mogą dysponować również własnymi źródłami czasu, takimi jak zegary atomowe). Stosowane zegary atomowe mimo swojej dokładności wymagają okresowej synchronizacji ze źródłami zewnętrznymi. Operacja ta jest niezbędna do wprowadzenia poprawek zegara, którym dysponuje urząd TSA. Synchronizacja ta może być realizowana drogą radiową, za pośrednictwem odbiorników satelitarnych oraz sieci globalnej (protokół NTP - synchronizacji czasu w sieci).

Urzędy TSA wydając znaczniki czasu używają (podobnie jak urzędy certyfikacji) zaawansowanych systemów kryptograficznych w celu ochrony kluczy prywatnych. Klucze urzędu chronione są przed kradzieżą oraz zniszczeniem za pośrednictwem modułów kryptograficznych. Weryfikacja podpisów składanych przez urząd znacznika czasu odbywa się na podstawie identyfikatorów (certyfikatów) urzędu, które zostały wydane przez zaufaną stronę trzecią. System teleinformatyczny urzędu znacznika czasu są wyposażone w systemy wykrywania intruzów (ang. IDS) oraz systemy zapór sieciowych (firewall) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

2.9 Podpis elektroniczny w praktyce Konfiguracja przykładowych programów

Poniższy opis ilustruje sposób ustawiania parametrów przykładowego oprogramowania, służącego do składania długookresowych podpisów elektronicznych. Po uruchomieniu programu należy kliknąć zakładkę Narzędzia, a następnie Ustawienia. Program podpowiada wartości domyślne, lecz użytkownik może bez problemu wprowadzić inne parametry.



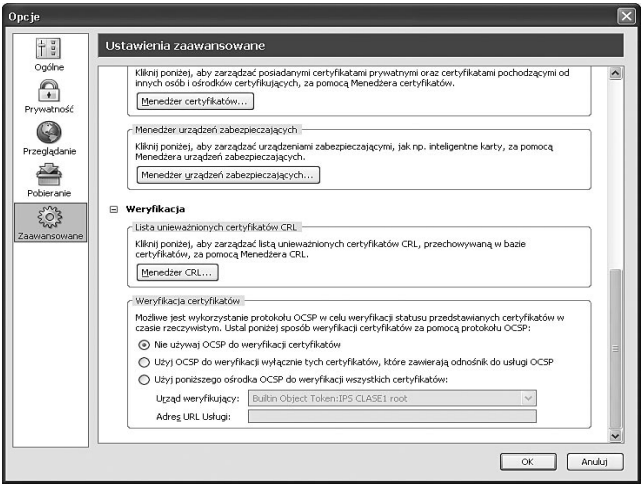
Ze względu na ograniczoną liczbę publicznych serwisów świadczących usługi znakowania czasem oraz serwerów do weryfikacji statusu certyfikatów w czasie rzeczywistym (OCSP) zalecane jest pozostawienie wartości domyślnych. W przypadku klientów komercyjnych, znajdujących się w sieci komputerowej chronionej zaporą sieciową należy włączyć obsługę PROXY. Zmiany ustawień zatwierdzane są przyciskiem *Zapisz ustawienia*. Po wykonaniu tych operacji program gotowy jest do pracy. Aby sprawdzić poprawność konfiguracji należy np. oznaczyć wiarygodnym czasem dowolny dokument elektroniczny. W dalszej kolejności użytkownik powinien podłączyć i skonfigurować czytnik kart kryptograficznych. Instrukcje instalacji i uruchomienia czytnika kart dostarczane są zawsze przez producenta.

Serwer PROXY

Serwer PROXY jest to serwer pośredniczący w komunikacji między Klientem, a docelowym serwerem. Jego zadaniem jest zapamiętywanie odwiedzonych stron WWW w celu szybszego wyświetlenia stron w przypadku ponownego żądania od Klienta.

Kolejna ilustracja prezentuje sposób konfigurowania oprogramowania Mozilla Firefox, pełniącego rolę przeglądarki internetowej.

Aby prawidłowo skonfigurować program do obsługi podpisów elektronicznych należy wybrać polecenie Preferencje, a następnie zakładkę Weryfikacja. Ustawienie opcji automatycznej weryfikacji certyfikatu spowoduje odwołanie do serwisu OCSP w trakcie weryfikacji certyfikatu. W przypadku korzystania z usług urzędu certyfikacji, który nie świadczy usług weryfikacji statusu certyfikatów w trybie on-line, należy



wybrać opcje zarządzania listami CRL i skonfigurować je zgodnie z zaleceniami urzędu wydającego certyfikat.

W analogiczny sposób można konfigurować inne programy posiadające wsparcie dla podpisu elektronicznego. Zasada działania jest ta sama, chociaż różne programy mogą posiadać oddzielne bazy z certyfikatami urzędów w oparciu, o które realizowana jest weryfikacja oraz sam podpis. Wybór oprogramowania, z którego korzysta użytkownik uzależniony jest od indywidualnych potrzeb i wymaganego poziomu bezpieczeństwa.

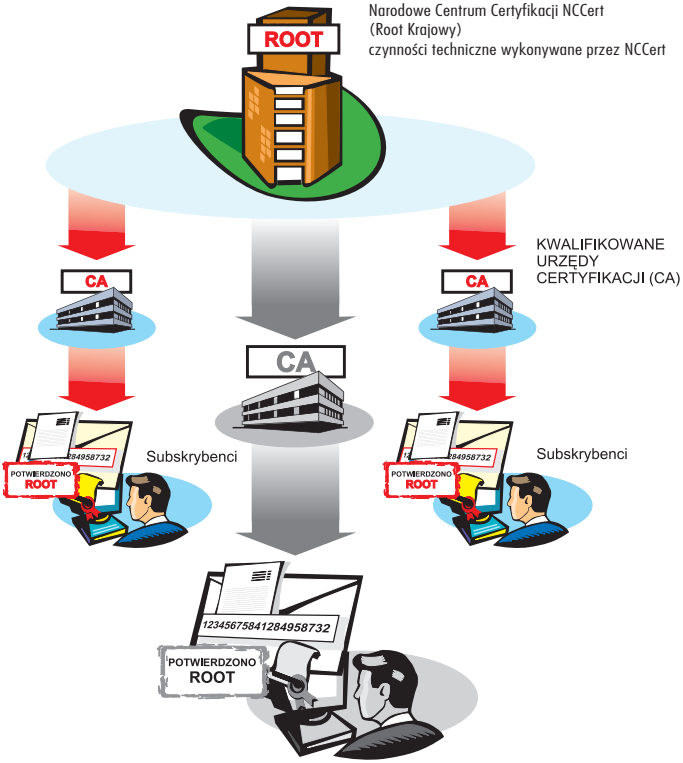
2.10 Infrastruktura klucza publicznego Zaufana Strona Trzecia (rola, zaufanie w elektronicznej wymianie danych)

Proces generowania kluczy asymetrycznych, a następnie wykorzystanie ich do składania oraz weryfikacji podpisu elektronicznego, szyfrowania danych i realizacji innych usług udostępnianych przez PKI nie stanowi większego problemu, ani na płaszczyźnie organizacyjnej, ani też technicznej.

Kryptografia asymetryczna jest stosowana do szyfrowania i podpisywania informacji od wielu lat. Jednak możliwości wykorzystania technologii do identyfikacji podpisujących i zabezpieczenia danych zależy od sposobu przekazywania kolejnym użytkownikom „sieci wzajemnego zaufania" informacji o tożsamości nieznanego wcześniej subskrybenta.

Infrastruktura klucza publicznego odzwierciedla model zakładający „dziedziczenie" zaufania po centralnym punkcie infrastruktury, jakim jest bezpośrednio zaufany urząd certyfikacji (w skrócie punkt zaufania). Każdy urząd certyfikacji podejmuje się realizacji zadań związanych z weryfikacją tożsamości subskrybentów. Zasady, według których prowadzona jest ta weryfikacja opisane są w publicznie dostępnym dokumencie, jakim jest **polityka certyfikacji**, zaś jakość wykonywanych czynności oraz ciągłość świadczenia usług jest gwarantowana finansowo. Dostępność polityki

Ścieżka weryfikacji certyfikatu



Ścieżka certyfikacji każdego certyfikatu kwalifikowanego składa się z certyfikatu root'a oraz urzędu kwalifikowanego

certyfikacji pozwala wszystkim zainteresowanym na podjęcie decyzji o obdarzeniu zaufaniem wydawcę certyfikatów.

Z wymienionych wyżej powodów, w odniesieniu do podmiotów świadczących usługi certyfikacyjne, a jednocześnie niezależnych od usługobiorców, używane jest pojęcie zaufana strona trzecia (ang. Trusted Third Party).

Na świecie funkcjonuje wiele urzędów certyfikacji. Urzędy te mogą być połączone w różny sposób, pozwalając jednak na przenoszenie zaufania, jakim obdarzamy wydawcę, na inne podmioty. Dzięki temu możliwe jest uznanie certyfikatów wydawanych przez nieznany nam urząd, pod warunkiem, że jest on rekomendowany jako godny zaufania przez uznawanego przez nas wydawcę certyfikatów. W polskim systemie prawnym przyjęto, że kwalifikowane urzędy certyfikacji, określane w ustawie mianem kwalifikowanych podmiotów świadczących usługi certyfikacyjne, będą podlegać rejestracji udzielanej przez główny urząd krajowy (tzw. root centralny).

Certyfikaty kwalifikowane może wydawać jedynie podmiot sprawdzony i wpisany do rejestru kwalifikowanych podmiotów, prowadzonego przez ministra właściwego ds. gospodarki. Zgodnie z upoważnieniem, rejestr w wersji elektronicznej w imieniu ministra właściwego ds. gospodarki prowadzi Narodowy Bank Polski w ramach Narodowego Centrum Certyfikacji NCCert (zob. http://www.nccert.pl). Na początku ścieżki certyfikacji kwalifikowanego certyfikatu znajduje się autocertyfikat (autozaświadczenie) wydany przez urząd dla siebie samego (tzn. głównego urzędu narodowego). Podmiotom kwalifikowanym wydawane są zaświadczenia certyfikacyjne (rodzaj certyfikatu potwierdzający kwalifikowany podmiot).

Ścieżka certyfikacji

Ścieżka certyfikacji jest zapisem hierarchicznej struktury, w której weryfikowany jest określony certyfikat. Elementem najniższego poziomu jest certyfikat konkretnego subskrybenta. Kolejne szczeble to urzędy wydające certyfikaty położonym niżej w hierarchii podmiotom. Na szczycie struktury znajduje się główny urząd certyfikacji.

Jeśli osoba weryfikująca certyfikat kwalifikowany przyjmie za punkt zaufania główny narodowy urząd certyfikacji, to zbudowana dla tego kwalifikowanego certyfikatu ścieżka certyfikacji – bez względu na to, od którego z akredytowanych urzędów on pochodzi – zaczynać się będzie od autocertyfikatu urzędu narodowego. Fakt ten pozwala na weryfikowanie każdego kwalifikowanego certyfikatu tylko poprzez stwierdzenie zaufania do głównego urzędu narodowego. W przypadku certyfikatów wykorzystywanych do składania i weryfikacji podpisu elektronicznego zwykłego, nie wskazano żadnych kryteriów budowania hierarchii urzędów. Nadmienić jednak należy, że nadzór ministra właściwego ds. gospodarki w zakresie przestrzegania ustawy o podpisie elektronicznym rozciąga się również na podmioty świadczące usługi certyfikacyjne dla zwykłego podpisu elektronicznego.

Powszechnym źródłem informacji o urzędach certyfikacji są przeglądarki i inne oprogramowanie internetowe, w których producenci umieszczają wykazy urzędów certyfikacji uznawanych za godne zaufania. Użytkownicy certyfikatów urzędów niewymienionych na tego typu listach podejmują decyzję o uznawaniu ich za zaufane na podstawie analizy polityki certyfikacji i własnej oceny wiarygodności urzędu.

Klasyfikacja urzędów certyfikacyjnych

Producenci przeglądarek internetowych tworzą i publikują w swych programach **listy zaufanych urzędów certyfikacyjnych**. Decyzja o klasyfikacji urzędu podejmowana jest na podstawie audytu obejmującego analizę zasad funkcjonowania i praktyki działania wydawcy certyfikatów.

2.11 Bezpieczeństwo, jako czynnik dostarczany przez PKI

Infrastruktura

Infrastruktura – system urządzeń, działań i instytucji, które wspierają bezpośrednio lub pośrednio produkcyjną sferę gospodarki lub są niezbędnym zapleczem dla funkcjonowania społeczeństwa (Popularny Słownik Języka Polskiego, Wydawnictwo Wilga, Warszawa 2000).

Infrastruktura klucza publicznego, podobnie jak każda inna infrastruktura dostarcza podmiotom korzystającym z jej usług pewnych produktów. **Infrastruktura klucza publicznego dostarcza cechy identyfikujące stronom korespondencji elektronicznej oraz mechanizmy zabezpieczające poufność i integralność informacji uczestnikom elektronicznego obrotu dokumentów.**

Pojęcie infrastruktury klucza publicznego (PKI) jest definiowane w różny sposób. Norma X.509 określa infrastrukturę jako:

Zbiór sprzętu, oprogramowania, ludzi, polityki oraz procedur niezbędnych do

tworzenia, posługiwania się, przechowywania, dystrybucji i unieważniania certyfikatów opartych na kryptografii klucza publicznego.

Inne definicje infrastruktury klucza publicznego oprócz określenia celów działania PKI, wskazują także potencjalne obszary zastosowania kluczy publicznych.

2.12 Elementy składowe PKI

Wymienione wyżej elementy składowe infrastruktury klucza publicznego określane są mianem komponentów PKI.

Najważniejszymi komponentami PKI są:

- urząd certyfikacji (ang. Certification Authority, CA) – tworzący i przypisujący certyfikat do osoby ubiegającej się o jego wydanie,
- punkt rejestracji (ang. Registration Authority, RA) – odpowiedzialny za identyfikowanie i rejestrowanie osób w sposób pozwalający na przyporządkowanie im certyfikatów,
- repozytorium (ang. repository) – odpowiedzialne za składowanie i udostępnianie certyfikatów klucza publicznego, listy certyfikatów unieważnionych (ang. Certificate Revocation List, CRL) oraz innych informacji związanych z PKI,
- subskrybent – posiadacz wydanego certyfikatu klucza publicznego,
- strona ufająca - klient, który potwierdza ważność podpisu elektronicznego, np. odbierając podpisaną przesyłkę e-mail i weryfikując ważność certyfikatu i tożsamość podpisującego.

Kwalifikowany certyfikat oraz bezpieczne urządzenia do składania bezpiecznych podpisów elektronicznych tworzą nierozłączna parę, której posiadanie daje subskrybentowi możliwość składania bezpiecznych podpisów elektronicznych, w tym także podpisów kwalifikowanych równoważnych, pod względem skutków prawnych podpisom własnoręcznym.

Z powyższego wynika, że system PKI oprócz podstawowych komponentów powinien zawierać elementy dodatkowe, które obejmują:

- dostawcę bezpiecznych urządzeń do składania podpisów elektronicznych,
- urząd weryfikacji statusu certyfikatu, który na żądanie strony ufającej sprawdza, czy certyfikat jest umieszczony na liście CRL oraz wystawia potwierdzenia ważności certyfikatu,
- urząd znacznika czasu, który wydaje tokeny znacznika czasu, zawierające dane w postaci elektronicznej, wiążące dowolny dokument elektroniczny z określonym momentem w czasie.

Token

Token znacznika czasu, są to dane w postaci elektronicznej, które wiążą zaistnienie dowolnego faktu lub działania z określonym momentem czasu, ustanawiając w ten sposób poświadczenie, że fakt lub działanie miało miejsce jeszcze przed tym momentem.

Funkcjonowanie komponentów PKI związanych z wydawaniem, unieważnianiem oraz weryfikacją certyfikatów realizowane jest przez odpowiednio dobrany sprzęt i oprogramowanie, obsługiwane przez posiadających stosowne kwalifikacje specjalistów. Działania personelu są precyzyjnie określone i regulowane przez odpowiednie polityki certyfikacji, regulaminy i procedury postępowania, opisujące jego role w danym systemie.

Polityka certyfikacji

Polityka certyfikacji: spisany zbiór zasad, który określa zakres stosowania certyfikatów w obrębie określonego kręgu użytkowników lub klas zastosowań o podobnych wymaganiach w zakresie bezpieczeństwa. Przykładowo polityka certyfikacji może ograniczyć zakres stosowania danego typu certyfikatu tylko do uwierzytelniania transakcji w elektronicznej wymianie danych, występujących w handlu towarami o ściśle określonym zakresie cen.

System PKI, wykorzystywany przez podmiot świadczący usługi certyfikacyjne, jest złożonym systemem informatycznym oraz dużym przedsięwzięciem organizacyjnym. Jego funkcjonowanie znajduje odzwierciedlenie we wspominanej wcześniej polityce certyfikacji. Polityka certyfikacji określa stopień zaufania jaki można związać z określonym typem certyfikatu.

2.13 Subskrybenci i strona ufająca: prawa i obowiązki

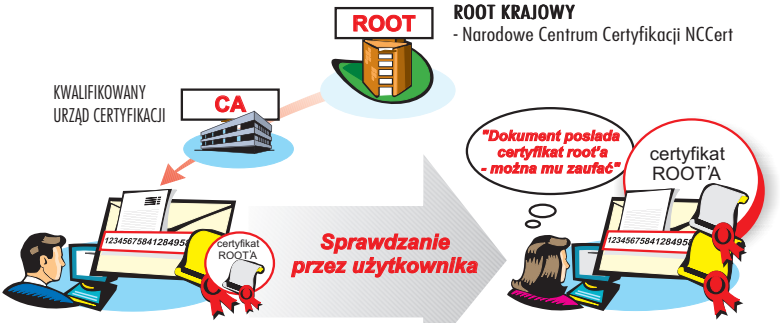
Każdy system nadaje swoim użytkownikom określone prawa i obowiązki. W infrastrukturze klucza publicznego nadawane one są przy uwzględnieniu norm oraz ustawy o podpisie elektronicznym i wydanych na jej podstawie aktów wykonawczych.

Subskrybent decyduje o tym, jaki typ certyfikatu jest najbardziej odpowiedni do jego potrzeb oraz do jakich zastosowań mu posłuży. Jednocześnie subskrybent jest zobowiązany do podawania prawdziwych danych we wnioskach o certyfikat przekazywanych do punktu rejestracji i powinien być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych. Ma on obowiązek nie udostępniania swoich kluczy prywatnych oraz związanych z nimi haseł lub numerów PIN osobom trzecim, a w przypadku podejrzenia lub naruszenia ochrony klucza prywatnego powiadomić o tym niezwłocznie wydawcę certyfikatu.

Subskrybent może i powinien wykorzystywać certyfikat klucza publicznego zgodnie z przeznaczeniem określonym w otrzymanym certyfikacie oraz celami i ograniczeniami określonymi w umowie pomiędzy nim, a urzędem certyfikacji, lub polityce certyfikacji.

Subskrybenci i strona ufająca

Subskrybenci i strona ufająca



Strona ufająca odpowiada za weryfikację aktualnego statusu certyfikatu subskrybenta. Decyzję taką podejmuje każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego. Każdy dokument z wykrytą wadą w podpisie elektronicznym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność.

2.14 Zadania realizowane przez urzędy certyfikacji Podstawowe funkcje PKI

Funkcje infrastruktury klucza publicznego realizowane są przez dostawców usług PKI, wykorzystywane zaś przez subskrybentów. Do funkcji tych należą:

- **Rejestracja** (ang. registration) – zbiór procedur, które umożliwiają zgromadzenie danych identyfikujących subskrybenta. Rejestracja może być realizowana bezpośrednio przez urząd certyfikacji lub za pośrednictwem punktu rejestracji, na podstawie udzielonego mu przez urząd certyfikacji umocowania. Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po zweryfikowaniu tożsamości, subskrybent zostaje wpisany na listę uprawnionych użytkowników usług urzędu certyfikacji.
- **Certyfikacja** (ang. certification) – stosowane przez urząd certyfikacji procedury tworzenia certyfikatu klucza publicznego, publikowania go w repozytorium oraz przekazywania certyfikatu subskrybentowi.
- **Uaktualnienie pary kluczy** (ang. key pair update) – zastępowanie poprzedniej pary kluczy asymetrycznych nową parą, mające miejsce w przypadku ujawnienia związanego z certyfikatem klucza prywatnego lub upływu okresu ważności certyfikatu.
- **Recertyfikacja** (ang. certificate update) – potwierdzenie ważności tej samej pary kluczy na następny okres czasu (zgodny z polityką certyfikacji) przed upływem poprzedniego okresu ważności.
- **Unieważnienie certyfikatów** (ang. certificates revocation) – procedury odwołania ważności pary kluczy, tj. wycofania certyfikatu.
- **Certyfikacja wzajemna** (ang. cross certification) – procedura wydawania certyfikatu przez urząd certyfikacji innemu urzędowi certyfikacji, w celu uproszczenia budowy i weryfikacji ścieżek certyfikatów.
- **Publikowanie certyfikatów i list certyfikatów unieważnionych** (CRL) – procedury dystrybucji utworzonych certyfikatów (przesyłanie do subskrybenta, publikowanie w repozytorium) oraz informacji o certyfikatach unieważnionych (w postaci list CRL).
- **Weryfikacja statusu certyfikatów** – weryfikacja statusu certyfikatu umożliwia określenie, czy certyfikat jest unieważniony, czy też nie.

Omawiając podstawowe funkcje PKI warto zwrócić uwagę na sytuację odbiegającą od podstawowego cyklu życia certyfikatu. Przypadek taki ma miejsce wtedy, gdy występuje faktyczna zmiana danych umieszczonych w certyfikacie, w okresie ważności certyfikatu. Sytuacja taka nie jest regulowana przepisami ustawy o podpisie elektronicznym, ale wymaga dookreślenia (n.p. w Kodeksie Postępowania Certyfikacyjnego). Najczęściej klauzula o informowaniu wydawcy certyfikatu o zaistnieniu faktu zmiany danych wykorzystywanych do wystawienia certyfikatu przez subskrybenta jest zawarta w umowie o przystąpieniu do usług certyfikacyjnych, której treść nie

podlega negocjacji. Od subskrybenta zależy, czy powiadomi urząd certyfikacji o zmianie danych osobowych. Sytuacja ta jest podobna do występującej w przypadku zmiany nazwiska (np. po wyjściu kobiety za mąż). Obowiązkiem osoby zmieniającej nazwisko jest zgłoszenie się do odpowiedniego urzędu i wyrobienie nowego dowodu tożsamości.

W sytuacji, gdy występuje konieczność zmiany informacji zawartych w certyfikacie, wystawca certyfikatu dokonuje następujących czynności:

- unieważnia certyfikat zawierający nieaktualne dane,
- modyfikuje dane w bazie tworzonej w trakcie rejestracji subskrybentów (na podstawie dokumentów potwierdzających zmianę danych),
- wydaje certyfikat zawierający aktualne dane.

3. Ramy prawne wykorzystywania podpisu elektronicznego

3.1 Podstawowe definicje i uregulowania

Warunki oraz skutki prawne stosowania podpisu elektronicznego, zasady świadczenia usług certyfikacyjnych, a także zasady nadzoru nad podmiotami świadczącymi te usługi określa Ustawa z dnia 18 września 2001r. o podpisie elektronicznym, zwana dalej ustawą. Ustawa obowiązuje od 16 sierpnia 2002r., a część jej postanowień zyskała moc obowiązującą z dniem wstąpienia Polski do Unii Europejskiej.

Wydawać certyfikaty, znakować czasem lub wykonywać inne usługi związane z podpisem elektronicznym mogą przedsiębiorcy, Narodowy Bank Polski oraz organy władzy publicznej (np. organy samorządu terytorialnego). Podmioty te, zwane podmiotami świadczącymi usługi certyfikacyjne mogą wystąpić z wnioskiem do ministra właściwego do spraw gospodarki o wpisanie do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Wpis do rejestru stanowi potwierdzenie, że podmiot ten jest instytucją posiadającą wystarczający potencjał merytoryczny i techniczny dla wystawcy kwalifikowanych certyfikatów i spełnia wymagania ustawowe. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest jawny oraz publicznie dostępny. Każdy kwalifikowany podmiot musi przygotować i opublikować ***politykę certyfikacji*** zawierającą szczegółowe rozwiązania dotyczące sposobu, zakresu oraz warunków bezpieczeństwa tworzenia i stosowania certyfikatów

Odbiorcami usług certyfikacyjnych mogą być osoby fizyczne, osoby prawne lub jednostki organizacyjne nie posiadające osobowości prawnej, które zawrą z usługodawcami certyfikacyjnymi umowę o świadczenie tych usług lub w granicach określonych w polityce certyfikacji działają w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne. Kwalifikowany certyfikat może być wydany osobie fizycznej. Osoby fizyczne mogą reprezentować firmy, w których pracują, o ile tylko posiadają stosowne pełnomocnictwa.

Podpis elektroniczny to dane w postaci elektronicznej, służące do identyfikacji osoby, która go składa. Dane te, powinny być logicznie powiązane z innymi danymi elektronicznymi lub do nich dołączone, tak aby tworzyły „nierozerwalną" całość. Podpis ten, będzie miał charakter bezpiecznego podpisu elektronicznego, o ile spełni następujące cechy:

- jest przyporządkowany wyłącznie do osoby, która go składa,
- jest niepowtarzalny, czyli tylko jedna osoba mogła go złożyć,
- jest sporządzany przy pomocy bezpiecznego urządzenia i klucza prywatnego, do którego dostęp ma wyłącznie osoba składająca podpis,

- umożliwia wykrycie ewentualnych prób jego podrobienia podejmowanych po jego złożeniu.

Podpis elektroniczny mogą składać wyłącznie osoby fizyczne. Mogą to czynić w imieniu własnym lub w imieniu innej osoby fizycznej, bądź osoby prawnej, a także w imieniu jednostki organizacyjnej nieposiadającej osobowości prawnej.

Bezpieczny podpis elektroniczny składany za pomocą bezpiecznych urządzeń służących do ich składania, które podlegają wyłącznej kontroli osoby składającej podpis. Bezpieczne urządzenie do składania podpisu to zespół środków technicznych spełniających wszystkie wymagania określone w ustawie, umożliwiających osobie składającej podpis elektroniczny złożenie go pod dokumentem elektronicznym.

Szczegółowe wymagania w zakresie „bezpiecznych urządzeń" zostały określone przepisami art. 18 ust. 1 i 2 ustawy oraz wskazanego wyżej rozporządzenia. Badania zgodności powyższych urządzeń z wymaganiami ustawy odbywają się zgodnie z przepisami *Ustawy z dnia 30 sierpnia 2002 r. o systemie oceny zgodności* (Dz. U. 04 Nr 204, poz. 2087 ze zmianami). Jeżeli urządzenia te miałyby służyć do ochrony informacji niejawnych muszą uzyskać stosowne certyfikaty bezpieczeństwa wydane przez Agencję Bezpieczeństwa Wewnętrznego lub Wojskowe Służby Informacyjne.

Pełny wykaz bezpiecznych urządzeń służących do składania i weryfikacji podpisów elektronicznych wraz z ich specyfikacją techniczną powinien być udostępniany każdemu odbiorcy usług certyfikacyjnych przez kwalifikowanego usługodawcę.

3.2 Skutki prawne bezpiecznego podpisu elektronicznego

Podstawowym skutkiem prawnym złożenia podpisu elektronicznego jest dokonanie czynności prawnej w postaci elektronicznej. Innymi słowy, każdy posiadacz tego „instrumentu" będzie mógł drogą elektroniczną składać ważne oświadczenia woli i zawierać umowy, czyli uczestniczyć w handlu drogą elektroniczną.

Zdecydowanie najwygodniej, a zarazem najbezpieczniej – zarówno z punktu widzenia nadawcy, jak i odbiorcy dokumentu elektronicznego – posługiwać się bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu (inaczej – kwalifikowanym podpisem elektronicznym), albowiem użycie go powoduje następujące skutki prawne przewidziane ustawą:

- zastosowanie, w okresie ważności certyfikatu kwalifikowanego, **jest równoważne ze złożeniem podpisu własnoręcznego** przez osobę fizyczną. Jeżeli certyfikat był w tym czasie unieważniony, to podpis elektroniczny weryfikowany przy jego użyciu nie wywoła takiego skutku prawnego. W przypadku złożenia podpisu w czasie trwania zawieszenia (w trakcie wyjaśniania przesłanek do unieważnienia) certyfikatu, ustawa przyznaje mu skutek w postaci zrównania z podpisem własnoręcznym dopiero od momentu uchylenia tego zawieszenia,
- dane w postaci elektronicznej sygnowane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu **są równoważne dokumentom opatrzonym podpisem własnoręcznym (zwykła forma pisemna)**. Nie dotyczy to tzw. kwalifikowanej formy pisemnej, której przykładem jest akt notarialny lub forma pisemna z datą poświadczoną urzędowo,
- ze złożeniem wyłącznie tego podpisu związane jest dopuszczające dowód przeciwny domniemanie prawne, w którym przyjmuje się, że **osobą składającą ten podpis jest osoba uprawniona** (dane tej osoby są zawarte w treści kwalifikowanego certyfikatu). W związku z tym odbiorca danych

elektronicznych ma prawo działać w oparciu o te dane, dopóki osoba, której przypisuje się złożenie oświadczenia woli wykaże, że tego nie uczyniła.

Interesy odbiorcy dokumentu elektronicznego sygnowanego podpisem elektronicznym, dodatkowo chroni usługa znakowania czasem. Gwarantuje ona, że dokument elektroniczny istniał w przedstawionej do oznakowania formie w czasie określonym w znaczniku (często przyjmuje się, że czas ten jest rzeczywistym czasem wysłania dokumentu). **Jeżeli znakowania czasem dokona kwalifikowany podmiot, to taki dokument będzie miał walor dokumentu pisemnego z datą urzędowo poświadczoną, tzw. datą pewną.**

W obrocie cywilnoprawnym, a zwłaszcza w handlu elektronicznym można stosować zwykłe podpisy elektroniczne, a możliwość wykorzystania dowodu z tego podpisu jest zagwarantowana ustawowo. Należy jednak pamiętać, że mają one niższy poziom zabezpieczenia przed fałszerstwem i nie wywołują większości skutków prawnych przedstawionych wyżej.

3.3 Obowiązki podmiotów świadczących usługi certyfikacyjne

Generalnie prowadzenie działalności w zakresie świadczenia usług certyfikacyjnych opiera się na zasadzie swobodnego świadczenia tych usług, czyli nie wymaga uzyskania zezwolenia ani koncesji. Jednakże ustawa wprowadza pewne ograniczenia w stosunku do organów władzy publicznej, Narodowego Banku Polskiego i jednostek samorządu terytorialnego oraz w przypadku podmiotów o statusie kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Do obowiązków kwalifikowanych podmiotów świadczących usługi certyfikacyjne należą:

1) obowiązek zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych,
2) obowiązki związane z zawarciem umowy o wydanie certyfikatu z odbiorcą usług certyfikacyjnych, które obejmują:
   - stwierdzenie tożsamości osoby ubiegającej się o certyfikat,
   - poinformowanie osoby ubiegającej się o certyfikat, przed zawarciem z nią umowy, o warunkach uzyskania i używania certyfikatu, w tym o wszelkich ograniczeniach jego użycia,
   - udostępnienie odbiorcy usług certyfikacyjnych pełnego wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych, a także warunków technicznych, jakim te urządzenia powinny odpowiadać,
   - jeśli podmiot zapewnia publiczny dostęp do certyfikatów uzyskanie zgody osoby ubiegającej się o certyfikat na jego późniejszą publikację (n.p. na stronie www),
3) obowiązki techniczno-organizacyjne, w tym:
   - obowiązek zapewnienia technicznej i organizacyjnej możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów, a także określenia czasu dokonania tych czynności,
   - obowiązek zapewnienia środków przeciwdziałających fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez osoby ubiegające się o certyfikat,
   - obowiązek używania systemów do tworzenia i przechowywania certyfikatów w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym,

- obowiązek zapewnienia, poufność procesu tworzenia klucza prywatnego oraz jego niepowtarzalności,
- obowiązek publikacji danych, które umożliwią weryfikację, w tym również w sposób elektroniczny, autentyczności i ważności certyfikatów oraz innych danych poświadczanych elektronicznie przez ten podmiot oraz zapewnić nieodpłatny dostęp do tych danych odbiorcom usług certyfikacyjnych
- obowiązek powierzania czynności związanych ze świadczeniem usług certyfikacyjnych wyłącznie osobom posiadającym pełną zdolność do czynności prawnych i nie skazanym prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe lub przestępstwa określone w ustawie o podpisie oraz dysponującym niezbędną wiedzą i umiejętnościami w zakresie technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym.

Podmioty świadczące usługi certyfikacyjne odpowiadają wobec odbiorców tych usług za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że są one skutkiem nieprawidłowego użycia certyfikatu bądź wynikły z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny.

Ustawodawca zadbał o bezpieczeństwo odbiorców kwalifikowanych usług certyfikacyjnych. Zgodnie z rozporządzeniem Ministra Finansów z dnia 8 sierpnia 2002r. w sprawie sposobu i szczegółowych warunków spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot *minimalna suma gwarancyjna ubezpieczenia odpowiedzialności cywilnej w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia, wynosi równowartość w złotych kwoty 250.000 euro, ale nie więcej niż 1.000.000 euro w odniesieniu do wszystkich takich zdarzeń*. W przypadku certyfikatów zwykłych wysokość gwarancji nie jest regulowana przepisami prawa, a stosowne zapisy umieszczane są w Kodeksie Postępowania Certyfikacyjnego.

Wysoki poziom bezpieczeństwa świadczenia usług certyfikacyjnych mają dodatkowo zapewnić rozwiązania wprowadzające tajemnicę certyfikacyjną, określające zasady przechowywania i archiwizacji dokumentów elektronicznych, a przede wszystkim nakazujące niezwłoczne niszczenie kluczy prywatnych podmiotów świadczących usługi certyfikacyjne we wskazanych przypadkach.

Podmiot świadczący usługi certyfikacyjne jest zobowiązany do bezpiecznego przechowywania i archiwizacji dokumentów i danych w postaci elektronicznej bezpośrednio związanych z wykonywanymi usługami certyfikacyjnymi. Dokumenty i dane będące w posiadaniu podmiotu kwalifikowanego zaprzestającego działalności przechowuje minister właściwy ds. gospodarki, pobierając opłatę w wysokości do 1 euro za każdy wydany certyfikat, którego dokumentacja podlega przechowaniu.

3.4 Zasady świadczenia usług certyfikacyjnych

Świadczenie usług certyfikacyjnych następuje na podstawie umowy, która z zasady jest umową przystąpienia. Umowa o wydanie certyfikatu musi być zawarta w formie pisemnej pod rygorem nieważności i podpisana przez wnioskodawcę własnoręcznie. Często w przypadku, gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem

elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez ten sam podmiot i w ramach tej samej polityki certyfikacji (sprawdzenie prawdziwość danych następuje przez porównanie ich z danymi zawartymi w umowie dotyczącej kwalifikowanego certyfikatu uwierzytelniającego bezpieczny podpis elektroniczny, którego użyto do podpisania umowy). Umowa o wydanie kwalifikowanego certyfikatu powinna zawierać, co najmniej następujące dane wnioskodawcy:

1) imię, nazwisko,
2) datę i miejsce urodzenia,
3) numer PESEL,
4) serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego dowód osobisty lub paszport, na podstawie którego potwierdzono tożsamość wnioskodawcy.

Przed zawarciem umowy wydawca zobowiązany jest poinformować o dokładnych warunkach użycia certyfikatu (zakres i ograniczenia jego stosowania, skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu, informację o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i ich znaczeniu), a także podać sposób rozpatrywania skarg i sporów. Informacja ta powinna zostać przedstawiona w sposób jasny i powszechnie zrozumiały, na piśmie lub za pomocą danych trwale zapisanych na nośniku elektronicznym, a fakt zapoznania się z jaj treścią winien być pisemnie potwierdzony. Podmiot, który wydaje kwalifikowane certyfikaty, powinien stosować procedury gwarantujące uzyskanie od osoby ubiegającej się o jego wydanie pisemną zgodę na stosowanie danych służących do weryfikacji jej podpisu elektronicznego (tj. klucza publicznego), które są zawarte w wydanym certyfikacie. Spełnienie powyższych warunków nie pociągnie za sobą nieważności certyfikatu w przypadku nieważność samej umowy, np. jeżeli zostanie zawarta bez przewidzianej ustawą formy.

W szczególności przepisy prawa cywilnego, za nieważną uznają umowę zawartą przez osobę, która nie ma zdolności do czynności prawnych (osoby, które nie ukończyły lat trzynastu, oraz osoby ubezwłasnowolnione całkowicie). Ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat trzynaście, oraz osoby ubezwłasnowolnione częściowo, np. z powodu choroby psychicznej, niedorozwoju umysłowego albo innego rodzaju zaburzeń psychicznych, w szczególności pijaństwa lub narkomanii. W związku z koniecznością posiadania pełnej zdolności do czynności prawnych osoby małoletnie nie będą mogły uzyskać kwalifikowanego certyfikatu niezbędnego do składania bezpiecznego podpisu elektronicznego. Warto w tym miejscu zaznaczyć, iż zgodnie z art. 21 ust. 2 pkt 7 ustawy o podpisie elektronicznym podmiot świadczący usługi certyfikacyjne unieważnia certyfikat kwalifikowany przed upływem okresu jego ważności, jeżeli osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych.

Ochrona klucza prywatnego i PINU

Istotne jest, aby odbiorca usług certyfikacyjnych przechowywał dane służące do składania podpisu elektronicznego (klucz prywatny oraz PIN) w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu służącego do weryfikacji tych podpisów.

Jak już wspomniano wcześniej, kwalifikowany podmiot świadczy usługi certyfikacyjne w oparciu o opracowaną przez siebie politykę certyfikacji, która m.in. określa metody i tryb tworzenia oraz udostępniania certyfikatów. Certyfikat należy uznać za kwalifikowany, jeżeli posiada numer, wskazanie, że został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji,

określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę, oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone, dane służące do weryfikacji podpisu elektronicznego (t.j. klucz publiczny), oznaczenie początku i końca okresu ważności certyfikatu, poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat, ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji, ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa.

Inne dane, których prawdziwość powinien potwierdzić podmiot wydający certyfikat, są umieszczane w kwalifikowanym certyfikacie na wniosek osoby składającej podpis elektroniczny, np. wskazanie, czy osoba ta działa w imieniu własnym albo jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo w charakterze członka organu albo organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo jako organ władzy publicznej. W takim przypadku wydawca certyfikatu informuje te podmioty o treści certyfikatu oraz poucza o możliwości unieważnienia certyfikatu na ich wniosek.

3.5 Ważność certyfikatów

Termin rozpoczęcia i zakończenia ważności certyfikatu musi być określony w jego treści. Z tym, że maksymalny okres ważności kwalifikowanego certyfikatu przewidziany przez politykę certyfikacji może wynosić nie więcej niż 2 lata. Ustawa o podpisie elektronicznym przewiduje przypadki zawieszenia bądź wyłączenia jego ważności przed upływem tego okresu.

Unieważnienia certyfikatu kwalifikowanego dokonuje jego wydawca, jeżeli:

1) zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie,
2) certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych osoby ubiegającej się o jego wydanie,
3) osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie przechowywała danych służących do składania podpisu elektronicznego (klucza prywatnego) w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu służącego do weryfikacji tych podpisów,
4) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,
5) nie dopełnił obowiązków określonych w ustawie (co nie wyłącza jego odpowiedzialności za szkodę względem osoby składającej podpis elektroniczny),
6) zaprzestaje świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejmie inny kwalifikowany podmiot,
7) żądanie takie złoży minister właściwy do spraw gospodarki, które może zostać przedstawione w przypadku zaistnienia wskazanych wyżej okoliczności z wyłączeniem punktu 1).

Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.

Zawieszenie certyfikatu następuje w przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu. Zawieszenie nie może trwać dłużej niż 7 dni. W tym czasie, wydawca certyfikatu

podejmuje działania niezbędne do wyjaśnienia tych wątpliwości. Zawieszenie może zostać uchylone, jeżeli wystawca wyjaśni wszystkie wątpliwości, w przeciwnym razie następuje niezwłocznie unieważnienie certyfikatu.

O unieważnieniu lub zawieszeniu certyfikatu podmiot świadczący usługi certyfikacyjne zawiadamia niezwłocznie osobę składającą podpis elektroniczny weryfikowany na jego podstawie. Zawieszenie lub unieważnienie certyfikatu nie może następować z mocą wsteczną. **Podmiot świadczący usługi certyfikacyjne publikuje *listę zawieszonych i unieważnionych certyfikatów*, tzw. „listę CRL".**

Unieważnienie lub zawieszenie certyfikatu

Zawieszenie i unieważnienie certyfikatu wywołuje skutki prawne od momentu, określonego w polityce certyfikacji, który nie może być wcześniejszy niż data i czas publikacji poprzedniej listy zawieszonych i unieważnionych certyfikatów.

Informacje o zawieszeniu lub unieważnieniu certyfikatu umieszcza się na liście CRL przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu. Publikacja tej informacji powinna następować na zasadach określonych w polityce certyfikacji jednak nie później niż w ciągu 1 godziny od unieważnienia lub zawieszenia certyfikatu. Prawidłowo opublikowana **lista CRL** powinna zawierać:

1) numer kolejny listy i wskazanie, że została opublikowana zgodnie z określoną polityką certyfikacji i dotyczy certyfikatów wydanych zgodnie z tą polityką,
2) datę i czas jej opublikowania z dokładnością określoną w polityce certyfikacji,
3) datę przewidywanego opublikowania kolejnej listy,
4) określenie podmiotu świadczącego usługi certyfikacyjne wydającego listę i państwa, w którym ma on siedzibę, oraz numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
5) numer każdego zawieszonego lub unieważnionego certyfikatu oraz wskazanie, czy został on unieważniony, czy zawieszony,
6) datę i czas, z dokładnością określoną w polityce certyfikacji, zawieszenia lub unieważnienia każdego certyfikatu,
7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, publikującego listę.

3.6 Przepisy karne

Ustawa o podpisie elektronicznym zakazuje posługiwania się bezpiecznym podpisem elektronicznym za pomocą danych służących do składania tego podpisu przyporządkowanym do innej osoby. Za taki czyn, przewidziana jest kara grzywny lub kara pozbawienia wolności do lat 3 albo obie te kary łącznie (art. 47)

Przepisy karne zawarte w ustawie są skierowane głównie do podmiotów świadczących usługi certyfikacyjne.

Ustawa pod groźbą kary zakazuje jednak posługiwania się bezpiecznym podpisem elektronicznym za pomocą danych służących do składania tego podpisu przyporządkowanym do innej osoby. Bez znaczenia dla realizacji znamion tego przestępstwa będzie, w jaki sposób osoba trzecia wejdzie w posiadanie klucza prywatnego innej osoby. Za taki czyn, przewidziana jest kara grzywny lub kara pozbawienia wolności do lat 3 albo obie te kary łącznie (art. 47). Należy pamiętać, że w myśl art. 53 ustawy karom wyżej wymienionym podlegać będzie także ten, kto dopuści się czynów, o których mowa powyżej, działając w imieniu lub w interesie innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Jeżeli podmiot świadczący kwalifikowane usługi certyfikacyjne nie poinformuje osoby ubiegającej się o certyfikat o warunkach uzyskania i używania certyfikatu, podlega karze grzywny do 30.000 złotych (zob. art. 46). Zdecydowanie surowsza sankcja grozi mu w przypadku, gdy będzie kopiować lub przechowywać dane służące do składania bezpiecznego podpisu (tzw. klucze prywatne osób fizycznych) lub poświadczenia elektronicznego (tzw. *klucze prywatne podmiotów świadczących usługi certyfikacyjne*) lub inne dane, które mogłyby służyć do ich odtworzenia - grzywna lub kara pozbawienia wolności do lat 3 albo obie te kary łącznie (art. 48). Taka sama kara jest przewidziana za zaniechanie unieważnienia certyfikatu na żądanie osoby składającej podpis elektroniczny lub osoby trzeciej wskazanej w certyfikacie bądź na żądanie ministra właściwego do spraw gospodarki (art. 50). Identyczna sankcja grozi podmiotowi świadczącemu usługi certyfikacyjne, jeżeli wyda kwalifikowany certyfikat zawierający nieprawdziwe dane. Za czyn ten odpowie także osoba, która w jego imieniu umożliwiła wydanie certyfikatu (prawdopodobnie pracownik punktu rejestracji, w których najczęściej zawiera się umowę o świadczenie usług certyfikacyjnych oraz w którym wydawane są certyfikaty). Dokładnie taka sama kara może zostać nałożona na osobę, która się posługuje tym certyfikatem. Dlatego też osoba ta, aby uwolnić się od odpowiedzialności karnej powinna sama sprawdzić czy wszystkie dane wpisane przez podmiot do kwalifikowanego certyfikatu są zgodne ze stanem faktycznym i prawnym (art. 49).

Jeżeli podmiot świadczy usługi certyfikacyjne jako kwalifikowany podmiot świadczący usługi certyfikacyjne bez uprzedniego zawarcia wymaganej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom tych usług, podlega grzywnie do 1.000.000 zł. (art. 45). Natomiast kwalifikowanym podmiotom świadczącym usługę znakowania czasem zakazuje się oznaczenia danych czasem innym niż z chwili wykonywania tej usługi oraz poświadczania elektronicznie tak powstałych danych. Za manipulowanie czasem określonym w znaczniku dołączanym do podpisu elektronicznego może zostać wymierzona kara grzywny lub kara pozbawienia wolności do lat 3, albo obie te kary łącznie (zob. art. 51).

Z odpowiedzialnością karną (w postaci grzywny do 1.000.000 zł. lub kary pozbawienia wolności do lat 3, a nawet - obu tych kar łącznie) musi liczyć się każdy, na kim spoczywa obowiązek zachowania tajemnicy związanej ze świadczeniem usług certyfikacyjnych, jeżeli ujawni lub wykorzysta, wbrew warunkom określonym w ustawie te informacje. Sankcja wzrasta (grzywna do 5.000.000 zł. lub kara pozbawienia wolności do lat 5 albo obie te kary łącznie) w przypadku, gdy dokona tego przestępstwa podmiot świadczący usługi certyfikacyjne lub kontroler, albo jeżeli sprawca działał w celu osiągnięcia korzyści majątkowej lub osobistej.

3.7 Podpis elektroniczny w prawie cywilnym

Przyjęta w polskim prawie cywilnym zasada swobody umów (art. 353^1 kc) odnosi się także do wyboru formy przez strony, co odpowiada potrzebom rozwiniętego obrotu gospodarczego i sprzyja szybkiemu i prostemu dokonywaniu wymiany dóbr i usług. Art. 60 Kodeksu cywilnego, przewiduje, iż oświadczenie woli osoby prowadzące do wywołania skutku prawnego, tj. do ustanowienia, zmiany, zniesienia skutku cywilnoprawnego (np. zawarcia umowy) może być złożone w dowolnej formie, o ile przepisy ustawy nie przewidują dla jego złożenia formy szczególnej.

Kodeks Cywilny, Art. 60

„**Art. 60 KC** Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli)."

Zasadniczo, więc wola danej osoby może być wyrażona w dowolny sposób pod warunkiem, że jej treść jest zrozumiała dla odbiorcy. Może być to, zarówno wypowiedź słowna, przyjęty zwyczajowo gest jak i oświadczenie złożone drogą elektroniczną z wykorzystaniem podpisu elektronicznego, kwalifikowanego lub zwykłego.

Uregulowania prawne w zakresie formy czynności prawnych w życiu codziennym charakteryzuje brak formalizmu. Praktyka profesjonalnego obrotu gospodarczego jest nieco inna. Transakcje zawierane bez zachowania formy pisemnej należą raczej do rzadkości. Kontrahenci - profesjonalni uczestnicy obrotu gospodarczego dążą z reguły, ze względów dowodowych, do sporządzenia pisemnego dokumentu zawartej umowy.

Bezpieczny podpis elektroniczny może przyspieszyć negocjowanie i zawieranie transakcji z wykorzystaniem Internetu. Stosowanie podpisu elektronicznego umożliwia jednoznaczną identyfikację stron umowy oraz potwierdzenie faktu złożenia oświadczeń woli i ich treści. Odbiorca dokumentu elektronicznego sygnowanego podpisem elektronicznym, otrzymuje podstawę do przekonania, że jego nadawca przyjmuje odpowiedzialność za zawartą w oświadczeniu woli treść. Jeżeli nadawca posłuży się bezpiecznym podpisem weryfikowanym przy pomocy kwalifikowanego certyfikatu (podpisem kwalifikowanym), odbiorca ma dodatkową gwarancję, że nadawca jest osobą wskazaną w certyfikacie.

Kodeks Cywilny, Art. 78 §2

„**Art. 78 KC** §2 Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej."

Ponadto, **stosowanie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu umożliwia dokonywanie czynności prawnych, dla których formą (wynikającą z przepisu ustawy albo woli stron) jest forma pisemna,** np. udzielenie pełnomocnictwa ogólnego, umowa leasingu, poręczenia, umowa spółki jawnej. Natomiast podpis elektroniczny znakowany czasem będzie mógł być wykorzystywany np. dla ustanowienia zastawu na prawie, ponieważ dla tej czynności przepisy kodeksu cywilnego przewidują formę szczególną, w postaci daty pewnej.

Zalecaną praktyką zawarcia umowy z wykorzystaniem podpisu elektronicznego może być następujący przykład:

- Firma „A" zamieszcza na stronach WWW ofertę sprzedaży, określając istotne postanowienia umowy, jaka zawarta zostanie z nabywcą (cena, termin dostawy, gwarancja, warunki serwisu itp.). Oferta ma charakter informacyjny i jest zaproszeniem do negocjacji dla osób i podmiotów zainteresowanych zakupem.
- Firma „B" jest zainteresowana kupnem produktu i przesyła do firmy „A" zapytanie ofertowe.
- W odpowiedzi na zapytanie sprzedawca (firma „A") przesyła ofertę w postaci elektronicznej, podpisaną bezpiecznym podpisem elektronicznym za pomocą ważnego kwalifikowanego certyfikatu. Oferta ta ma charakter oferty wiążącej.
- Przyjęcie oferty przez firmę „B" następuje poprzez wysłanie podpisanej elektronicznie (podpis kwalifikowany) akceptacji oferty.

Stosowanie podpisów kwalifikowanych pozwala stronom na jednoznaczne ustalenie tożsamości kontrahenta - sprzedawca wie kto przyjmuje jego ofertę, kupujący wie

od kogo będzie kupował produkt. Wykorzystanie list CRL lub weryfikacja statusu certyfikatu w czasie rzeczywistym (OCSP) umożliwi stronom transakcji stwierdzenie, czy otrzymane dokumenty zostały podpisane przy użyciu ważnego certyfikatu. **Ważne jest, aby strony podczas transakcji używały podpisów elektronicznych wskazujących na fakt, iż występują one w charakterze przedstawicieli osób prawnych, a nie jako osoby fizyczne**

3.8 Prawne aspekty stosowania podpisu elektronicznego w bankach i biurach maklerskich

Wydaje się, że zastosowanie podpisu elektronicznego zyska popularność w bankowości elektronicznej. Wciąż rośnie liczba banków oferujących swe usługi za pomocą Internetu, działają banki w pełni wirtualne (nie mające placówek w ich tradycyjnej formie). Coraz więcej osób, korzysta z elektronicznych nośników informacji przy dokonywaniu czynności bankowych, gdyż banki honorują oświadczenia woli składane za ich pomocą.

Prawo Bankowe, Art. 7, pkt 1 i 3

> Zgodnie z przepisami prawa bankowego (art.7 pkt 1 i 3) oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażane za pomocą elektronicznych nośników informacji nawet, jeżeli dla tej czynności forma pisemna została zastrzeżona pod rygorem nieważności.

Podpis elektroniczny znajdzie zastosowanie przy dokonywaniu operacji za pomocą elektronicznych instrumentów płatniczych, co przewidziano ustawą o elektronicznych instrumentach płatniczych. Szczegółowe zasady wykorzystania podpisu elektronicznego na giełdach towarowych, w obrocie papierami wartościowymi oraz w obrocie bankowym regulują stosowne rozporządzenia. Przykładem takiej szczegółowej regulacji w przypadku prawa bankowego jest rozporządzenie Rady Ministrów w sprawie zasad tworzenia, utrwalania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego dokumentów bankowych sporządzanych na elektronicznych nośnikach informacji.

Warto zauważyć, że banki mogą w ramach czynności bankowych świadczyć usługi certyfikacyjne, z wyłączeniem wydawania certyfikatów kwalifikowanych wykorzystywanych przez banki w czynnościach, których są stronami.

Technologia podpisu elektronicznego może być wykorzystywana w sferze obrotu papierami wartościowymi oraz towarami giełdowymi. Domy maklerskie oraz towarowe domy maklerskie mogą przyjmować zlecenia klienta złożone za pomocą elektronicznych nośników informacji, o ile przewiduje to ich regulamin oraz umowa z klientem. Zlecenie złożone w ten sposób powinno zostać opatrzone przez osobę je składającą bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. Dom maklerski jest obowiązany sprawdzić, czy zlecenie zawiera stosowne dane oraz potwierdzić jego przyjęcie przy użyciu systemu informatycznego.

Należy nadmienić, iż domy maklerskie, banki prowadzące działalność maklerską oraz rachunki papierów wartościowych, Krajowy Depozyt Papierów Wartościowych S.A., oraz inne podmioty pośredniczące w zbywaniu papierów wartościowych emitowanych przez Skarb Państwa korzystają z podpisu elektronicznego w realizacji obowiązków sprawozdawczych, a kwalifikowany podpis elektroniczny wykorzystywany jest także przy przekazywaniu do Generalnego Inspektora Informacji Finansowej wiadomości o stosownych transakcjach w rozumieniu Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł. Jest również wielce

prawdopodobne, że przepisy wykonawcze do uchwalonych w lipcu tego roku ustaw dotyczących rynków finansowych i kapitałowych (Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U.05.183.1538), Ustawa z dnia 29 lipca 2005 r.o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U.05.184.1539) poszerzą zastosowanie technologii podpisu elektronicznego również i na te dziedziny.

3.9 Podpis elektroniczny w prawie publicznym

Podpis elektroniczny znajdzie swoje zastosowanie w publicznym prawie gospodarczym oraz w procedurze administracyjnej i cywilnej. Umożliwi to osobom fizycznym i prawnym korzystanie z elektronicznej formy komunikacji z administracją publiczna, co sprzyjać będzie uproszczeniu procedur i skróceniu czasu postępowania.

W związku z wprowadzeniem bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu, praktycznej doniosłości nabierają rozwiązania administracyjno-prawne przewidujące możliwość „załatwiania spraw" w drodze elektronicznej. Zgodnie z art. 5 ust. 1 ustawy o podpisie elektronicznym jest on substytutem podpisu własnoręcznego. Dotychczas przepisy te należało uznać, za „martwe", albowiem brak podpisu pod dokumentem osoby, która go przesyła stanowił brak formalny. Ponadto, art. 6 ust. 1 ustawy o podpisie elektronicznym wprowadza domniemanie, że osobą, która posługuje się bezpiecznym podpisem elektronicznym opatrzonym ważnym kwalifikowanym certyfikatem jest uprawniona osoba składająca e-podpis. Dodatkowo, przepis ten stanowi dyrektywę skierowaną do organów prowadzących wszelkiego rodzaju postępowania, aby dopuściły jako środek dowodowy w sprawie dane podpisane tym podpisem.

Podpis elektroniczny znajdzie zastosowanie w procedurze administracyjnej, gdzie art. 63 § 1 *Kodeksu postępowania administracyjnego* dopuszcza możliwość wnoszenia do organów administracji podań (żądań, wyjaśnień, odwołań, zażaleń) za pomocą poczty elektronicznej oraz (co stanowi *novum* wprowadzone ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku) za pomocą formularza umieszczonego na stronie internetowej właściwego organu administracji publicznej, umożliwiającego wprowadzenie danych do systemu teleinformatycznego tego organu. Jeszcze bardziej doniosła zmiana to dodanie do art. 63 KPA § 3, który mówi iż „Podanie wniesione w formie dokumentu elektronicznego powinno:

1) być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, przy zachowaniu zasad przewidzianych w przepisach o podpisie elektronicznym, oraz
2) zawierać dane w ustalonym formacie, zawarte we wzorze podania określonym w odrębnych przepisach, jeżeli te przepisy nakazują wnoszenie podań według określonego wzoru."

Organ administracji publicznej obowiązany jest potwierdzić wniesienie podania, jeżeli wnoszący je tego zażąda. Za pomocą poczty elektronicznej można także wnosić skargi i wnioski do organów państwowych, organów jednostek samorządu terytorialnego, organów samorządowych jednostek organizacyjnych (§5 *rozporządzenia Rady Ministrów w/s organizacji przyjmowania i rozpatrywania skarg i wniosków*), a przyjmujący skargi i wnioski potwierdza ich złożenie, jeżeli zażąda tego wnoszący.

Warto podkreślić, iż podobne rozwiązania znalazły się w ustawie z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270), która weszła w życie 1 stycznia 2004. W myśl art. 65 §3 pismo

procesowe może być doręczone za pomocą poczty elektronicznej, a zgodnie z treścią art. 47 §2 uwierzytelniony odpis wydruku poczty elektronicznej będzie równoznaczny z odpisem tego pisma.

Znacząca jest również treść artykułu 37 ustawy o informatyzacji, która modyfikuje ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Punkt 1 do pojęcia materiału archiwalnego wchodzącego do narodowego zasobu archiwalnego w art.1 ustawy o narodowym zasobie archiwalnym i archiwach dodaje pojęcie dokumentu elektronicznego rozumieniu przepisów ustawy o informatyzacji podmiotów realizujących zadania publiczne. Szczegóły dotyczące np.: wymagań technicznych, jakim powinny odpowiadać formaty zapisu i informatyczne nośniki danych określa w odpowiednich rozporządzeniach Minister właściwy do spraw informatyzacji. Powyższa zmiana ustawy o narodowym zasobie archiwalnym i archiwach weszła w życie 21 listopada 2005 roku.

Podobne przepisy zawiera *Ordynacja podatkowa*, która w art. 168 §1 przewiduje możliwość wnoszenia za pomocą poczty elektronicznej podań (żądań, wyjaśnień, odwołań, zażaleń) do organów podatkowych, a te są zobowiązane potwierdzić wniesienie podania, jeżeli wnoszący je tego zażąda. Zgodnie z art. 168 §5 podania te winny zawierać dane w ustalonym formacie elektronicznym oraz być opatrzone podpisem elektronicznym. Ustawa nowelizująca Ordynację, wprowadzi z dniem 16 sierpnia 2006r. zmiany w tym zakresie. W myśl art. 3b podatnicy będą mogli w formie elektronicznej składać deklaracje podatkowe – szczegóły dotyczące wymaganego rodzaju podpisu określone zostaną w rozporządzeniu. W myśl art. 60 §4 zlecenia płatnicze na rzecz organów podatkowych mogą być składane również w formie elektronicznej przy użyciu programu informatycznego udostępnionego przez banki lub inną instytucję finansową uprawnioną do przyjmowania zleceń płatniczych albo w inny sposób uzgodniony z bankiem lub inną instytucją przyjmującą zlecenie. Zlecenie to powinno zawierać, m. in. dane identyfikujące wpłacającego przy czym niepodanie lub błędne podanie tych informacji stanowi podstawę do odmowy realizacji wpłaty gotówkowej lub polecenia przelewu.

Bezpieczny podpis elektroniczny znajdzie zastosowanie także w procedurze cywilnej. Art. 125 §2 Kodeksu postępowania cywilnego przewiduje, iż pisma procesowe wnosi się na urzędowych formularzach lub na elektronicznych nośnikach informatycznych. Pismo, podobnie jak w postępowaniu administracyjnym winno być przez stronę podpisane (art. 126 §1 pkt 4). Podpisanie go, zatem bezpiecznym podpisem weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, który jest równoważny podpisowi własnoręcznemu, spełni ten wymóg. Ponadto, dokumenty podpisane bezpiecznym podpisem elektronicznym poświadczonym ważnym kwalifikowanym certyfikatem mają walor dowodu z dokumentu według art. 245 KPC.

Terminy wprowadzenia podpisu elektronicznego w życie

Zgodnie z art. 58 ust. 2 ustawy o podpisie elektronicznym w terminie 4 lat od dnia wejścia w życie ustawy, czyli do 16 sierpnia 2006 r. organy władzy publicznej obowiązane są umożliwić odbiorcom usług certyfikacyjnych wnoszenie podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru.

Na podstawie art. 47a ustawy o systemie ubezpieczeń społecznych płatnicy składek zobowiązani są przekazywać zgłoszenia do ubezpieczeń społecznych, imienne raporty miesięczne, zgłoszenia płatnika składek, deklaracje rozliczeniowe, oraz inne dokumenty niezbędne do prowadzenia kont płatników składek i kont ubezpieczonych oraz korekty tych dokumentów poprzez teletransmisję danych w formie dokumentu elektronicznego z aktualnego programu informatycznego udostępnionego przez Zakład Ubezpieczeń Społecznych. ZUS ma prawo przekazywać informacje

w formie dokumentu elektronicznego poprzez teletransmisję danych. Zgodnie z *rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 3 lipca 2001 roku w sprawie warunków, jakie muszą spełnić płatnicy składek przekazujący dokumenty ubezpieczeniowe w formie dokumentu elektronicznego poprzez teletransmisję danych* (Dz.U. nr 73. poz. 774) podpis elektroniczny umożliwia identyfikację płatnika składek przekazującego dokumenty ubezpieczeniowe w formie elektronicznej. Na mocy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku, od 21 lipca 2007 roku dokumenty te mogą być opatrywane bezpiecznymi podpisami elektronicznymi weryfikowanymi za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, zaś od dnia 21.07.2008 w ZUS przyjmowane będą tylko dokumenty sygnowane bezpiecznym podpisem weryfikowanym za pomocą ważnego certyfikatu kwalifikowanego.

Technologia podpisu elektronicznego znajdzie również zastosowanie przy udostępnianiu informacji publicznych przez władze publiczne oraz inne podmioty wykonujące zadania publiczne, zarówno w drodze ogłaszania informacji publicznych, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej, jak i na wniosek zainteresowanego obywatela. Zgodnie z art. 12 ust. 2 pkt 2 ustawy o dostępie do informacji publicznej podmiot udostępniający tego rodzaju informację publiczną winien zapewnić możliwość jej przesłania albo przeniesienia na odpowiedni, powszechnie stosowany nośnik informacji, a zatem uczyni zadość obowiązkowi przesyłając informacje podpisaną bezpiecznym podpisem elektronicznym w drodze elektronicznej.

Kolejnym obszarem stosowania bezpiecznych podpisów elektronicznych jest tzw. e-faktura. *Rozporządzenie Ministra Finansów z dnia 14 lipca 2005 r.* w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, a także przechowywania oraz udostępniania organowi podatkowemu lub organowi kontroli skarbowej tych faktur wymaga, aby faktura elektroniczna była opatrzona bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego certyfikatu kwalifikowanego. E-fakturę stosować jednak można nie tylko w obrocie krajowym, ale tego rodzaju faktury (tj. opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu) mogą być wystawiane także kontrahentom z pozostałych krajów członkowskich UE.

4. Obszary stosowania podpisu elektronicznego i usług znakowania czasem dokumentów elektronicznych

4.1 W biznesie

Z punktu widzenia podmiotu gospodarczego podpis elektroniczny powinien być traktowany jak inwestycja w nowoczesność. Wdrożenie e-podpisu wiąże się z podjęciem konkretnych przedsięwzięć organizacyjnych związanych z określonymi nakładami. Decyzja o podjęciu działań i ich zakresie powinna wynikać z budowania przewagi konkurencyjnej, podnoszenia efektywności i bezpieczeństwa oraz innych korzyści, jakie może osiągnąć przedsiębiorstwo.

Planowanie skali i modelu stosowania podpisu elektronicznego wymaga zebrania danych początkowych, dotyczących:

- charakteru spodziewanych korzyści (oszczędności czasowe, obniżenie kosztów, zwiększenie efektywności oraz zysków),
- liczby użytkowników wraz z uwzględnieniem sytuacji, w których będą korzystali z podpisu (wewnętrzny obieg dokumentów, występowanie kontrasygnaty, wymiana informacji z otoczeniem zewnętrznym),
- uwarunkowań prawnych dla podpisywanych dokumentów i przesyłek (stosowanie certyfikatów kwalifikowanych lub zwykłych, charakter danych: informacja niejawna, tajemnica handlowa, wymagania co do archiwizacji danych),
- zakresu wdrożenia w odniesieniu do organizacji (usługi PKI udostępniane wewnątrz firmy, w centrali, w oddziałach, w firmach partnerskich),
- źródeł i sposobów finansowania przedsięwzięcia (ze środków własnych, współfinansowanie przez partnerów handlowych).

Odpowiedzi na powyższe kwestie dają podstawę do określenia optymalnego modelu korzystania z usług infrastruktury klucza publicznego w firmie. Wyróżnić można trzy podstawowe rozwiązania:

- zakup usług (certyfikatów i ewentualnie produktów dodatkowych) od dostawcy zewnętrznego,
- budowę własnej infrastruktury klucza publicznego,
- zlecenie prowadzenia dedykowanej infrastruktury podmiotowi profesjonalnie zajmującemu się świadczeniem tego typu usług.

Bez względu na wybór wariantu, niezbędne jest określenie harmonogramu wprowadzania podpisu elektronicznego w organizacji. Harmonogram taki, zarówno w ujęciu ekonomicznym, jak i dotyczącym progowych terminów zakończenia poszczególnych etapów implementacji jest podstawą do bieżącej oceny osiągania zamierzonych efektów. W trakcie tworzenia planu wdrożenia należy pamiętać, że przed osiągnięciem zamierzonej wydajności systemu wystąpić może okresowy spadek sprawności obiegu dokumentów.

Przestrzeganie przez wydawców certyfikatów norm dotyczących formatu i zawartości certyfikatów pozwala na sprawną wymianę danych między podmiotami funkcjonującymi w różnych lokalizacjach oraz branżach. Bez względu na to jakie programy pracują u nadawcy i odbiorcy informacji, mechanizm zabezpieczeń będzie zgodny.

Bezpieczny transfer danych w postaci elektronicznej umożliwia prowadzenie interesów z wykorzystaniem Internetu. Transakcje mogą być realizowane między podmiotami, które współpracowały wcześniej w sposób tradycyjny, kontaktując się ze sobą osobiście. Dzięki certyfikatowi, potwierdzającemu tożsamość, możliwe jest także rozpoczęcie współpracy na platformie elektronicznej między stronami, które wcześniej nie kontaktowały się ze sobą. W ten sposób traci dotychczasowe znaczenie odległość oraz koszty telekomunikacyjne i czasowe.

Korzyści płynące z korzystania w działalności gospodarczej z elektronicznej wymiany danych można podzielić na trzy podstawowe grupy:

- usprawnienie prowadzonej działalności,
- przyspieszenie przebiegu procesów,
- poprawa wskaźników ekonomicznych.

Wypadkowym efektem stosowania elektronicznej wymiany danych jest zmiana stylu pracy organizacji. Wymuszane przez stosowane oprogramowanie uporządkowanie rejestracji i pełniejsza kontrola zachodzących wewnątrz systemu informacyjnego firmy zdarzeń, daje znacznie więcej niż najlepiej skonstruowana procedura organizacyjna dotycząca obiegu dokumentów tradycyjnych. Wsparcie najsłabszego ogniwa jakim jest człowiek, ze strony systemów zarządzania obiegiem dokumentów pozwala na poprawę jakości funkcjonowania oraz lepszą ocenę efektywności pracy.

Podobne zjawisko występuje również w relacjach między różnymi podmiotami gospodarczymi. Współpraca prowadzona na platformie wirtualnej wymaga stosowania się do reguł narzuconych przez użytkowane oprogramowanie. Wszystkie operacje są w automatyczny sposób rejestrowane i służyć mogą zarówno do analizy podejmowanych w przeszłości decyzji, jak i stanowią dowód zaciągniętych zobowiązań.

Przedsiębiorstwa, które odczuwają pozytywne efekty systematyzacji działalności będą zainteresowane, aby wszystkie, a przynajmniej większość ich kontaktów, była prowadzona w ten sam sposób. Powoduje to, że starają się one motywować swych partnerów do korzystania z elektronicznej wymiany dokumentów. Przykładem takiej sytuacji jest oferowanie współpracującym firmom lepszych warunków handlowych (niższe ceny, wydłużone terminy płatności) w przypadku składania zamówień przez Internet.

Bez względu na branżę w jakiej działa przedsiębiorstwo e-podpis znaleźć może zastosowanie w obiegu informacji wewnątrz firmy. Wszędzie tam, gdzie podejmowane są decyzje, ma miejsce dwukierunkowy przepływ dokumentów. Przełożeni posługują się dokumentem w celu wydania poleceń służbowych, pracownicy zaś dostarczają w ten sposób żądanych analiz, zestawień lub raportów.

Przesyłanie poleceń z wykorzystaniem podpisanej poczty elektronicznej lub podpisanych dokumentów otrzymywanych z zewnątrz to rozwiązania najbardziej oczywiste, ale stanowiące zaledwie znikomy fragment możliwych zastosowań.

Jeżeli rozważymy możliwość wdrożenia prostego w obsłudze systemu agregującego wewnętrzne zapotrzebowanie na przykład na materiały biurowe, otrzymamy w efekcie usprawnienie procesu zamawiania towarów, unikniemy zbędnych zakupów oraz zoptymalizujemy wielkość zapasów. Podpis elektroniczny używany zarówno przez pracowników zgłaszających zapotrzebowanie, jak i weryfikujących zapotrzebowanie pod względem merytorycznym pozwala na posługiwanie się dokumentem wirtualnym jako alternatywą dla druków. Dodatkowo, posługując się rynku większym, zbiorczym zamówieniem, uzyskamy korzyść w postaci lepszej oferty cenowej.

Kolejnym etapem jest możliwość dokonywania zakupów na wirtualnych giełdach towarowych. Elektroniczne platformy transakcyjne, na których spotykają się dostawcy i odbiorcy, stwarzają możliwość negocjacji cen i innych parametrów handlowych. Jednocześnie pozwalają one na wykorzystywanie efektu agregacji zamówień składanych przez różnych kupujących. Najskuteczniejszym mechanizmem autoryzacji dostępu i ochrony poufności transakcji prowadzonych na giełdach internetowych jest technologia klucza publicznego.

W tym miejscu wspomnieć należy o możliwości stworzonej przedsiębiorcom przez ustawodawcę w zakresie faktur w postaci elektronicznej. Faktury takie, opatrywane bezpiecznym podpisem elektronicznym (lub przesyłane przy pomocy platformy EDI), wpłyną w dłuższym okresie czasu na obniżenie kosztów obsługi księgowej i przyspieszenie czasu obsługi e-faktury (Dz.U. 05.113.1119)

Innym obszarem, w którym znajduje zastosowanie podpis elektroniczny są zewnętrzne kontakty firmy. Wyposażenie pracowników operujących „w terenie" w certyfikaty pozwalające na autoryzację dostępu do firmowych baz danych umożliwia bieżącą aktualizację ich zawartości. Przykładowo: pracownik dostawcy odpowiedzialny za ekspozycję i ilość towarów w sklepie, na bieżąco zgłasza zapotrzebowanie na poszczególne pozycje asortymentowe przez Internet. Wykorzystanie mechanizmów PKI pozwala na rezygnację z dodatkowej autoryzacji zgłoszeń.

Posłużenie się prywatnym kluczem przy zdalnym dostępie do firmowej bazy może służyć indywidualizowaniu danych podawanych konkretnemu odbiorcy. Przykładowo: zaopatrzeniowiec partnera handlowego „przedstawiając się" swym certyfikatem dostaje dostęp do wydzielonego fragmentu serwisu WWW dostawcy.

W serwisie składa on zamówienia, nie angażując handlowców do obsługi typowego zamówienia. Jednocześnie dostaje on wgląd do informacji dotyczących jego firmy, takich jak:

- stan płatności faktur,
- przyznane limity zamówień,
- aktualne warunki handlowe dla poszczególnych grup towarowych.

Ponadto podpis elektroniczny znajduje zastosowanie w wielu innych branżach.

4.2 Banki

Ze względu na poufny charakter przekazywanych informacji produkty PKI idealnie nadają się do wykorzystywania w sektorze bankowo-finansowym. Autoryzacja i szyfrowanie danych przesyłanych między oddziałami banków bazujące na kryptografii asymetrycznej funkcjonuje w Polsce od ponad 10 lat. Banki internetowe, pozwalające na zarządzanie własnymi pieniędzmi z dowolnego miejsca w świecie, zdobywają coraz szersze rzesze zwolenników. Biura maklerskie oferują swoim klientom nie tylko możliwość bezpiecznego składania zleceń w postaci elektronicznej, ale dokładają starań, by wszelkie formalności załatwiali oni zdalnie. Wykorzystywanie

znakowania czasem staje się sposobem na uniknięcie wątpliwości i sporów dotyczących czasu złożenia zlecenia.

4.3 Ubezpieczenia

Dzięki bezpiecznemu podpisowi elektronicznemu możliwe będzie zawieranie umów ubezpieczeniowych przez Internet. Już obecnie Zakład Ubezpieczeń Społecznych przyjmuje około 90% wszystkich składanych dokumentów w postaci elektronicznej, a dokumenty te opatrzone są podpisem elektronicznym. Od 21 lipca roku 2007 stosowany będzie wyłącznie bezpieczny podpis weryfikowany za pomocą certyfikatu kwalifikowanego (Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne). Przewidywalnym rozszerzeniem funkcjonalności na biznesową część branży jest ustanowienie podobnych standardów dla kontaktów z otwartymi funduszami emerytalnymi. Najwięksi ubezpieczyciele podejmują wysiłki mające na celu wdrożenie usług infrastruktury klucza publicznego do kontaktów z odbiorcami usług i pośrednikami.

4.4 Inne sektory

Elektroniczna wymiana danych wyposażona w podpis elektroniczny może znaleźć swoje miejsce także w innych gałęziach gospodarki. W przemyśle, jako metoda prowadzenia korespondencji z dostawcami surowców, w handlu prowadzonym w sieciach dealerskich oraz w przypadku transakcji jednostkowych. Określone korzyści osiągnąć można także w logistyce, decydując się na zastosowanie e-podpisu w korespondencji ze zleceniodawcami (zlecenia, monitorowanie dostaw, elektroniczne dokumenty celne, faktury itp.).

Podsumowując, podpis elektroniczny znajduje i będzie znajdował coraz więcej zastosowań w różnych dziedzinach gospodarki. Tym bardziej, że mechanizmy kryptografii asymetrycznej wykorzystać można do tworzenia spójnych rozwiązań o różnych funkcjonalnościach. Przykładowo: karta mikroprocesorowa wykorzystywana jako nośnik kluczy i certyfikatu, służyć może jako element kontroli dostępu do stacji roboczych lub pomieszczeń, rejestracji czasu pracy, a w przyszłości jako elektroniczna portmonetka.

4.5 W administracji publicznej

Obszarem, w którym zastosowanie podpisu elektronicznego może przynieść największe efekty jest administracja publiczna. Nałożony przez ustawę o podpisie elektronicznym obowiązek stworzenia możliwości załatwiania spraw urzędowych z wykorzystaniem mediów elektronicznych stanowi dobrą prognozę dla upowszechnienia e-podpisu.

Określony przez ustawę okres czterech lat na dostosowanie się do tak postawionego wymogu wydawać się może bardzo długi. Biorąc jednak pod uwagę zakres prac związanych z dostosowaniem posiadanej infrastruktury technicznej, konieczność przeszkolenia kadry w zakresie obsługi dokumentów elektronicznych oraz w wielu przypadkach konieczność zmiany przepisów (w tym także prawa miejscowego) czas ten „kurczy się” bardzo szybko.

Każdy obywatel załatwia wiele spraw w urzędach. Zastosowanie podpisu elektronicznego spowoduje, iż większość czynności będzie można realizować zdalnie przed monitorem: w dogodnym dniu tygodnia i odpowiedniej dla nas porze.

Systemy projektowane i wdrażane do prowadzenia obsługi obywateli jako klientów urzędów, powinny realizować – oprócz wielu innych – kilka podstawowych funkcji:

- udzielanie czytelnej informacji na temat sposobu postępowania w trakcie załatwiania poszczególnych spraw,
- udostępnienie formularzy przystosowanych do złożenia podpisu elektronicznego,
- udzielanie informacji na temat zasad wypełniania poszczególnych formularzy.

Dodatkowo systemy informatyczne administracji publicznej powinna cechować spójność umożliwiająca obsługę procedur związanych z udziałem różnych urzędów. Istotnym elementem wpływającym na ocenę ze strony użytkowników są także ograniczenie liczby przypadków wielokrotnego wprowadzania tych samych danych i opcjonalne (za zgodą użytkownika) wykorzystywanie do uzupełniania pól formularzy danych zawartych w certyfikacie klucza publicznego.

W efekcie uzyskać można między innymi skrócenie czasu załatwiania poszczególnych spraw oraz możliwość wykorzystania informacji „importowanych" z dostarczanych dokumentów elektronicznych przez systemy informatyczne urzędów. Petenci nie czekający w kolejkach i nie wędrujący między różnymi urzędami w mniejszym stopniu będą odczuwać niedogodności związane z obciążeniami publicznymi. Wpłynie to pozytywnie na wizerunek administracji w naszym kraju.

Zwykła zmiana mieszkania nie jest niestety wyłącznie powodem do radości. Zmiana adresu wiąże się bowiem ze:

- zgłoszeniem zmiany zameldowania,
- zmianą dowodu osobistego.

Dla osób zmotoryzowanych kolejnymi czynnościami są:

- zmiana prawa jazdy,
- wymiana tablic rejestracyjnych,

Jeżeli zaś dana osoba prowadzi działalność gospodarczą czekają ją:

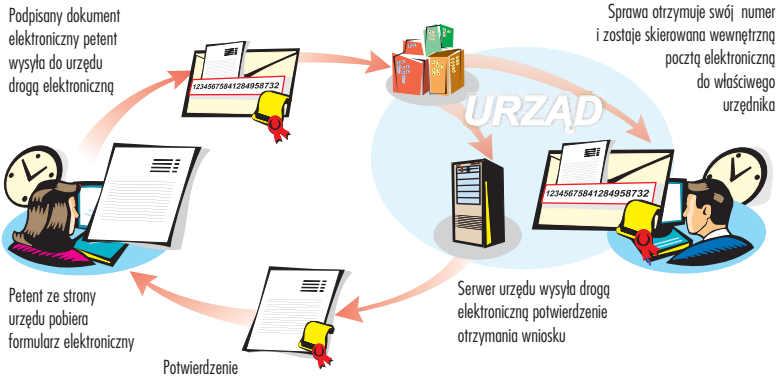
- wyrejestrowanie i ponowne zarejestrowanie działalności w urzędzie gminy,
- aktualizacja numeru REGON w urzędzie statystycznym,
- wizyta w dwóch komórkach urzędu skarbowego w celu uaktualnienia danych osoby fizycznej i danych płatnika VAT.

Cały proces trwa kilka tygodni i wiąże się z koniecznością wizyty w kilku, często odległych od siebie lokalizacjach. Tymczasem prawne uznanie dla podpisanego elektronicznie dokumentu pozwala na załatwienie sprawy w nieporównywalnie krótszym czasie, przy użyciu komputera. Administracja publiczna, rozumiana jako system instytucji służebnych wobec obywateli i przedsiębiorstw, utrzymywanych zazwyczaj z ich podatków, ma szczególny obowiązek poszukiwania rozwiązań zmniejszających koszty i oszczędzających czas.

Sygnalizowane korzyści to nie tylko poprawa jakości obsługi petentów, skutkująca lepszą oceną funkcjonowania administracji. Podobnie jak w zastosowaniach biznesowych mówić można o usprawnieniu działania urzędu, jako organizacji posiadającej wewnętrzną strukturę i system informacyjny. Dokumenty w postaci papierowej, krążące pomiędzy różnymi komórkami urzędów mogą zostać z powodzeniem zastąpione ich wirtualnymi odpowiednikami. Przechowywanie i przeszukiwanie zasobów zgromadzonych na nośnikach danych elektronicznych jest tańsze i mniej pracochłonne.

Poniżej przedstawiony został schemat przykładowego rozwiązania serwisu urzędu: Petent ze strony internetowej urzędu może pobrać formularz elektroniczny (np. plik programu MS Word) dotyczący sprawy, którą chciałby załatwić - np. otrzymania wtórnika prawa jazdy. Po zapisaniu pliku na swoim komputerze, obywatel wypełnia go i podpisuje elektronicznie. Podpisany dokument jest przesyłany do urzędu pocztą elektroniczną – sprawa otrzymuje swój numer – a następnie zostaje skierowana siecią wewnętrzną do właściwego urzędnika. Serwer urzędu wysyła pocztą elektroniczną potwierdzenie otrzymania wniosku.

Elektroniczne biuro obsługi klienta



W związku z przytaczaną wcześniej ustawą o informatyzacji podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku wizja taka już niebawem stanie się rzeczywistością. Już teraz do wizji tej dopasowuje się art. 3 Rozporządzenia MF z dnia 5 grudnia 2000 r. w sprawie sposobu pobierania, zapłaty i zwrotu opłaty skarbowej oraz sposobu prowadzenia rejestrów tej opłaty (Dz.U.00.110.1176), gdzie jednym ze sposobów uiszczenia opłaty skarbowej jest dokonanie jej bezgotówkowo, przy czym dowód wpłaty w formie elektronicznej musi być opatrzony bezpiecznym podpisem elektronicznym złożonym przez upoważnionego pracownika banku lub innej instytucji finansowej realizującej zlecenia płatnicze.

4.6 Dla obywatela

Wzajemne kontakty, dwukierunkowa wymiana informacji czy też transakcje dokonywać się mogą pomiędzy różnymi środowiskami lub grupami zawodowymi. Pierwszy omówiony dotąd obszar zastosowań dotyczył relacji między podmiotami gospodarczymi. Kolejny fragment pokazywał aplikację na polu kontaktów między administracją i przedsiębiorstwami oraz między administracją i obywatelem. Mówiąc o możliwych zastosowaniach podpisu elektronicznego nie sposób jednak pominąć spojrzenia od strony fizycznego posiadacza certyfikatu i pary kluczy. Każda z posługujących się

e-podpisem osób pełni w społeczeństwie wiele ról i jest aktywna na różnych polach działalności.

Każdy z nas jest klientem. Kupujemy różnorodne towary i usługi. Wiele produktów nabywamy w tradycyjnych sklepach. Z bezpośredniego kontaktu z dostawcą korzystamy również, gdy chcemy mieć możliwość dokładnego zapoznania się z przedmiotem ewentualnego zakupu (nieruchomość, sprzęt AGD, samochód) lub skorzystania z fachowej porady sprzedawcy. Dzieje się tak częstokroć mimo wcześniejszego zebrania za pośrednictwem Internetu informacji dotyczących funkcjonalności i ceny produktu. Decydującymi czynnikami skłaniającymi do kupowania w ten sposób stają się wartość transakcji, koszt wysyłki, przewidywany długi czas przesłania lub użytkowania nabywanych dóbr.

Istnieje jednak szeroka grupa towarów i usług, których parametry jednoznacznie wskazują na ich przydatność dla kupującego i mały rozrzut jakości w obrębie produkowanych seryjnie produktów. Przykładami tej kategorii towarów są programy komputerowe, książki, muzyka na płytach CD lub filmy na kasetach video. Jakkolwiek trudno przewidywać tutaj zastosowanie e-podpisu to jednak pewne znaczenie mieć może zawieranie tą drogą umów kredytowych. Z punktu widzenia kupującego istotnymi czynnikami są wiarygodność dostawcy funkcjonującego w Internecie oraz możliwość poufnego prowadzenia transakcji.

Obie funkcje są dostępne poprzez sygnowanie stron z serwerów sprzedawcy przez odpowiedni certyfikat.

Mechanizmy kryptografii asymetrycznej

Mechanizmy kryptografii asymetrycznej stosowane do rozpoznawania nadawcy informacji są wykorzystywane nie tylko do podpisywania korespondencji i dokumentów elektronicznych. Znajdują one również zastosowanie przy autoryzacji dostępu do zasobów, weryfikacji autentyczności serwisów internetowych czy też szyfrowania danych wymienianych przez użytkownika z serwerem. Urządzenie wyposażone w certyfikowaną parę kluczy „przedstawia się" internaucie przesyłając podpisane pakiety danych.

Wspomnieć również należy o podpisie elektronicznym w kontekście pewnych ograniczeń występujących w handlu internetowym. Związane są one z potrzebą skoordynowanej realizacji, następujących po ustaleniu warunków i zawarciu umowy, czynności obsługi płatności i dostawy zamówionego produktu. Infrastruktura klucza publicznego, rozumiana jako standard bezpiecznego porozumiewania się z wykorzystaniem mediów elektronicznych stanowi tu dużą nadzieję na najbliższą przyszłość. Odejście od lokalnych rozwiązań informatycznych wykorzystywanych w bankach i firmach logistycznych w kierunku usług PKI warunkuje bowiem:

- łatwość uzgodnienia formatów wymiany danych między podmiotami działającymi w różnych branżach,
- szybkość współpracy między różnymi systemami – poprzez wyeliminowanie interfejsów zapewniających współpracę programów zabezpieczanych na bazie odmiennych technologii,
- niższe koszty osiągnięcia bezpieczeństwa technologicznego i biznesowego w stosunku do budowy rozwiązań indywidualnych.

Wzorem innych państw można założyć dopuszczenie w najbliższych latach e-głosowań na walnych zgromadzeniach akcjonariuszy lub nawet wyborów i referendów przeprowadzanych w Internecie. Mimo, że do sytuacji takiej nie dojdzie prawdopodobnie szybko, zastosowanie podpisu elektronicznego w administracji będzie systematycznie rosło. Wynikać to będzie przede wszystkim z coraz większej liczby komputerów pracujących tak w urzędach, jak i wykorzystywanych przez petentów. Ich użytkownicy będą chcieli wykonywać swą pracę i załatwiać sprawy szybko, sprawnie oraz bez zbędnych przejazdów. Koniecznym warunkiem rozwoju

wykorzystania systemów teleinformatycznych w administracji będzie przegląd i zmiany przepisów prawa.

Warto wskazać także na łatwość organizowania na płaszczyźnie internetowej działań o charakterze lobbystycznym. W przypadku znacznego upowszechnienia e-podpisu wśród uczestników elektronicznej wymiany danych wystąpienie z inicjatywą ustawodawczą grupy obywateli może być kwestią kilkunastu dni, a nie jak dotychczas paru miesięcy.

Znaczna część użytkowników komputerów i Internetu potwierdza, że początki korzystania z nowych narzędzi nie zawsze są wystarczająco proste. Konieczność poznania nowej nomenklatury i potrzeba uporządkowania pojęć stanowią przejściową trudność w posługiwaniu się nowymi narzędziami. Bez wątpienia początkującym użytkownikom nie jest łatwo przewidzieć, w jakim stopniu dostępność informacji, szybkość i łatwość jej wymiany, będzie dla nich przydatna w dniu codziennym.

W społeczeństwie informacyjnym składanie podań w urzędach za pośrednictwem sieci, zakupy w sklepach internetowych oraz obsługa rachunków bankowych i płatności spowoduje, że narzędzia internetowe rozstrzygać będą o jakości codziennego życia.

Decyzja o wykorzystywaniu nowoczesnych, bezpiecznych technologii teleinformatycznych należeć będzie do pracodawców. Jednakże postępujący wzrost kultury informatycznej pracowników, doświadczenie oszczędności czasu poświęcanego na załatwianie spraw wymagających dotąd oczekiwania i dojazdów lub perspektywa eliminacji chodzenia z papierami po działach własnej firmy stanowi istotny argument przemawiający za wdrożeniem e-podpisu. Z czasem jedynie te instytucje i firmy, które w pełni wykorzystają sieci komputerowe i podpisane elektronicznie dokumenty będą postrzegane jako nowoczesne i przyjazne miejsce pracy.

5

5. Korzyści płynące ze stosowania podpisu elektronicznego

5.1 Bezpieczeństwo

Bezpieczeństwo dokumentu elektronicznego może być rozpatrywane w dwóch wymiarach. Po pierwsze w sensie czysto technologicznym, jako ochrona spójności podpisanego pliku. Z drugiej strony, bezpieczeństwo w ujęciu funkcjonalnym, t.j. na przykład niezaprzeczalność podjęcia zobowiązań dowodzona na podstawie podpisanego elektronicznie dokumentu. Rozważyć można także inne aspekty bezpieczeństwa związanego z podpisem elektronicznym. Stosowanie mechanizmów PKI pozwala na spójną i skuteczną ochronę zasobów informatycznych. Autoryzacja dostępu do zdalnych baz danych oraz do stacji roboczych stanowi element zabezpieczenia na poziomie fizycznym. Nie należy również zapominać, że ze względu na znikomą objętość archiwizowanych dokumentów i wykorzystywane w praktyce ich nośniki, zminimalizowane jest ryzyko utraty ważnych zbiorów dokumentów.

5.2 Usprawnienie działalności

Wiele czynności realizowanych w organizacjach, zarówno bazujących na tradycyjnym dokumencie papierowym jak i wykorzystujących elementy wymiany elektronicznej, wymaga dalszego wprowadzania informacji pochodzących z otrzymywanych dokumentów. W sytuacji, gdy przesyłane informacje docierają do odbiorcy w postaci zrozumiałej dla systemów komputerowych i dodatkowo są to informacje wiarygodne wówczas wiele czynności może zostać zautomatyzowanych. Uniknięcie etapu ponownego wprowadzania danych do systemu pozwala na inną organizację procesu obsługi korespondencji przychodzącej. Wysiłek kierowany na wprowadzanie danych do systemu przeniesiony zostaje na zarządzanie pracą programów odpowiedzialnych za weryfikację poprawności podpisu elektronicznego i prawidłowe zasilanie danymi wewnętrznych systemów teleinformatycznych.

Zastosowanie rozwiązań automatyzujących transfer danych powoduje ograniczenie liczby pomyłek. Po stronie odbiorcy nie występują przekłamania informacyjne wynikające z błędów popełnianych przez człowieka. Jednak błędy mogą mieć miejsce w przypadku zakłóceń transmisji danych. Tego zaś typu przekłamania są

łatwiejsze do wykrycia i kontroli, a także podejmowania niezależnych od człowieka działań korekcyjnych (np. wymuszenie ponownego wczytania dokumentu w przypadku stwierdzenia braku jego integralności i informowanie operatora dopiero w przypadku kolejnego wystąpienia tego samego błędu).

Istotnym czynnikiem wpływającym na optymalizację procesów zachodzących w organizacji jest także możliwość konsekwentnego stosowania reguły jednokrotnego wprowadzania danych. Obok standardowych metod związanych z prawidłowym projektowaniem oprogramowania i systemów teleinformatycznych, podpis elektroniczny (jako element chroniący integralność danych) stanowi dodatkowe potwierdzenie prawidłowości pakietu danych służącego do wielokrotnego wykorzystania w systemie. Możliwe jest zarazem wielokrotne podpisywanie tego samego dokumentu.

Świadome użytkowanie mechanizmów autoryzacji informacji, bądź dostępu do określonych zasobów, pozwala na śledzenie i analizę zachodzących procesów wewnętrznych. Otrzymane wyniki dostarczyć mogą wniosków, dotyczących zarówno przyjętej metodyki działania i architektury organizacji, jak i wspomóc poszukiwanie „wąskich gardeł" w przepływie informacji oraz procesach decyzyjnych.

5.3 Przyspieszenie realizacji zadań i obiegu informacji

Kolejna grupa pozytywnych efektów wynikających z wykorzystania wirtualnego dokumentu opatrzonego podpisem elektronicznym dotyczy przyspieszenia obiegu informacji. Przyspieszenie to w efekcie zapewnia zwiększenie szybkości funkcjonowania całej organizacji, co z kolei pozwala na bardziej dynamiczne reagowanie na potrzeby klientów oraz działania konkurencji.

Od początku wykorzystywania komputerów do tworzenia dokumentów użytkownikom towarzyszyła pokusa, by korzystać bezpośrednio z wirtualnego pierwowzoru dokumentu papierowego. Jednak dokument ten, nie mając mocy prawnej, mógł stanowić najwyżej swoiste awizo właściwej informacji dostarczanej w innej formie z charakterystycznym dla niej opóźnieniem.

Zastosowanie podpisu elektronicznego pozwala nadal na uzyskanie wydruków, jako postaci wygodniejszej w niektórych sytuacjach do analizy i „obróbki". Jest to jednak jedyne uzasadnienie dla dokumentów papierowych. W wymiarze funkcjonalnym całkowicie wystarczające okazuje się korzystanie z dokumentu elektronicznego łatwego w zwielokrotnieniu, taniego w archiwizacji, obiegającego świat w czasie nie dostępnym dla innych postaci dokumentu.

Każde przedsiębiorstwo lub instytucja tworzy wiele dokumentów, będących zapisem konkretnych wydarzeń lub podjętych decyzji. Znane od wieków sposoby gromadzenia i przechowywania informacji nie są przyjazne z punktu widzenia możliwości dotarcia do pożądanych danych. Niejednokrotnie czas poświęcany na odnajdywanie dokumentów stanowi kilkadziesiąt procent całego czasu pracy.

W efekcie uzyskane oszczędności czasu skracają, częstokroć wielokrotnie, proces wyszukiwania i przetwarzania dokumentów. Stosowanie elektronicznego obiegu dokumentów wspieranych mechanizmami PKI oznacza przejście do nowej jakości komunikacji i przyczyni się do lepszego funkcjonowania systemów informacyjnych firmy lub instytucji.

5.4 Aspekt ekonomiczny - obniżenie kosztów funkcjonowania

Podpis elektroniczny wspierając obrót dokumentów elektronicznych, przynosi wymierne efekty ekonomiczne. Dokonujący się postęp w sferze sposobu posługiwania się dokumentem generuje znaczne oszczędności. Szacuje się, że dokument elektroniczny jest co najmniej o połowę tańszy od dokumentu papierowego. Różnica w kosztach powstaje na każdym etapie życia i wykorzystania dokumentu: w trakcie jego tworzenia, nadawania, przesyłania, odbioru i przechowywania.

Nie tworząc zbędnych wydruków możemy ograniczyć znacznie koszt materiałów eksploatacyjnych dla drukarek i urządzeń wielofunkcyjnych. Koszt wysyłki dokumentów z wykorzystaniem usług tradycyjnej poczty, firmy kurierskiej albo faksów to kolejne źródło poważnych oszczędności.

Również po stronie odbiorcy czynności związane z rejestracją, archiwizacją, późniejszym wyszukiwaniem korespondencji lub powieleniem treści są tańsze w przypadku dokumentów elektronicznych, co stanowi następstwo zwłaszcza zmniejszonej pracochłonności.

Pamiętać jednak należy, że posługiwanie się podpisanym dokumentem elektronicznym, nie likwiduje kosztów, a jedynie znacznie je ogranicza. Aby wymieniać pliki musimy posiadać sieć wewnętrzną oraz połączenie z Internetem. Wymaga to nakładów na instalację, administrowanie i opłaty dostępowe. Sama możliwość składania podpisu elektronicznego wiąże się z koniecznością zakupu certyfikatu oraz odpowiedniego sprzętu (zwykle czytnika z kartą) wraz z oprogramowaniem.

Wymieniając ekonomiczne efekty uzyskiwane dzięki stosowaniu podpisu elektronicznego, nie sposób ograniczyć się jedynie do oszczędności. Nie mniej ważne są możliwości zwiększania przychodów oraz korzyści prestiżowe. Sygnalizując jedynie w tym miejscu temat, należy wskazać na sytuacje, w których atrakcyjność oferty nie jest określana wyłącznie atrakcyjnością produktu (bardzo zbliżonego u różnych dostawców), a przede wszystkim jakością obsługi. Trudno przecenić wygodę i oszczędności czasowe płynące z możliwości dokonania zakupu, porządkowania faktur, czy składania podań z dowolnego miejsca przy pomocy np. domowego komputera lub laptopa z komórkowym dostępem do Internetu.

5.5 Wypadkowa zastosowań podpisu elektronicznego

Stosowanie nowoczesnych, przyjaznych narzędzi i form obsługi klientów lub petentów powoduje, że jesteśmy w stanie więcej czasu i wysiłku poświęcić na kwestie merytoryczne, a zwłaszcza badanie i zaspokajanie oczekiwań odbiorców oferowanych usług. Typową sytuacją pożądaną przez klientów jest możliwość dokonywania zamówień oraz załatwiania spraw urzędowych w godzinach popołudniowych i wieczornych. Alternatywą dla wydłużenia godzin pracy organizacji, instytucji i przedsiębiorstw oraz zatrudniania w tych godzinach dodatkowych pracowników jest właśnie podpis elektroniczny.

Postrzeganie podpisu elektronicznego oraz nowoczesnych technologii teleinformatycznych może, ale nie musi wiązać się z redukcją zatrudnienia. Pomijając fakt konieczności obsługi infrastruktury klucza publicznego, warto wskazać na wymierne korzyści w tym zakresie. Przed przedsiębiorstwami, urzędami i instytucjami otwiera się bowiem możliwość bardziej celowego i oszczędnego czasowo wykorzystania zatrudnionej kadry. Osoby poświęcające dotąd znaczną część czasu

na wykonywanie uciążliwych czynności związanych z tworzeniem i obsługą dokumentów mają szansę na uniknięcie ich. Odzyskany czas mogą spożytkować na nawiązanie nowych kontaktów handlowych, dokładniejsze przygotowanie ofert, czy też bardziej wnikliwą obsługę petentów.

Wdrożenie podpisu elektronicznego stanowi również wyzwanie dla menedżerów. W okresie poprzedzającym wprowadzanie nowej technologii i w trakcie uruchamiania kolejnych funkcjonalności problemy mają charakter głównie wewnętrzny i dotyczą: optymalnego wyboru stanowisk i rodzaju certyfikatów, obaw pracowników oraz perturbacji z podwójnym, pisemno-elektronicznym obrotem dokumentów. Na etapie wykorzystywania podpisu elektronicznego niezbędne jest czuwanie nad satysfakcją klienta, jako końcowego beneficjenta nowej funkcjonalności ułatwiającej załatwianie spraw. Uwaga ta dotyczy, co oczywiste i zrozumiałe, podmiotów gospodarczych, ale również urzędów i organizacji nie nastawionych na osiąganie zysku.

Obniżenie kosztów funkcjonowania, zwiększenie szybkości dostępu do informacji i inne wymienione wyżej wymierne efekty korzystania z usług dostarczanych przez PKI skutkują poprawą pozycji konkurencyjnej dla uczestników dowolnego rynku.

Z jednej strony organizacja staje się zdolna do szybkiego dostosowywania się do dynamicznie zmieniającej się sytuacji biznesowej oraz w pełni gotowa do elektronicznego obiegu dokumentów. Z drugiej zaś uzyskuje bardziej elastyczne możliwości komunikacji z szerszym niż przedtem spektrum klientów oraz organów administracji publicznej. Dzięki lepszemu wykorzystaniu posiadanego potencjału organizacyjno-technicznego przedsiębiorstwo oprócz penetracji rynku, może pozwolić sobie na tworzenie nowej jakości obsługi oraz nowych, lepiej postrzeganych produktów. W tej sytuacji, przy założeniu prezentowania porównywalnej oferty produktowej istotne stają się inne elementy oddziaływania, takie jak:

- szybki dostęp do wiarygodnej i rzetelnej informacji handlowej, w niewielkim stopniu wymagający bezpośredniego angażowania pracowników,
- możliwość łatwego złożenia zamówienia – bez narażania sprzedawcy na podwyższone ryzyko (np. zawarcie kontraktu z fałszywym pełnomocnikiem),
- możliwość uzyskania przez kluczowych klientów, pośredników i dostawców indywidualnej informacji o cenach lub stanie rozliczeń, realizowana za pomocą dedykowanego serwisu lub ekstranetu przy użyciu klucza prywatnego,
- elektroniczne biuro obsługi klienta czynne non-stop i dostępne z każdej lokalizacji, które rejestruje zgłoszenia.

Dbając o nowoczesność i poprawę pozycji konkurencyjnej warto jednak pamiętać o ograniczeniach podpisu elektronicznego. Służy on do jednoznacznego potwierdzenia tożsamości osoby składającej podpis. Stąd mimo możliwości zapisania w certyfikacie limitu wysokości zobowiązań, odbiorcę dokumentu mogą spotkać przykre niespodzianki. Zarówno tradycyjny dokument papierowy, jak i jego wirtualny odpowiednik podpisany elektronicznie nie chronią bowiem przed nieuczciwością i złą wolą.

Internet jest medium, o niespotykanych wcześniej możliwościach dostarczania informacji do szerokiej grupy odbiorców. Mimo krótkiej historii ogólnoświatowej sieci, stosowane metody oddziaływania na klientów i potencjalnych klientów ulegają ciągłym modyfikacjom oraz zmianom. Entuzjazm wynikający z przełamania ograniczeń w swobodnym dostępie do informacji ustępuje powoli miejsca zapotrzebowaniu na informację potrzebną i wiarygodną. Filtrowanie otrzymywanych przesyłek, korzystanie z profesjonalnych narzędzi do wyszukiwania informacji to jedynie pierwsze sito ograniczające liczbę informacji przeznaczanych do dalszej analizy. Kwestia wiarygodności prezentowanych danych może być rozwiązana jedynie z wykorzystaniem dodatkowych mechanizmów. Podpis elektroniczny jest najbardziej wszechstronnym narzędziem potwierdzającym autentyczność elektronicznych dokumentów.

6. Bibliografia

AKTY PRAWNE

[1] Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 013 z 19.01.2000, str. 0012-0020).

[2] USTAWA z dnia 18 września 2001r. o podpisie elektronicznym, Dz.U. Nr 130, Poz.1450, z dnia 15.11.2001r.

[3] ROZPORZĄDZENIE Ministra Gospodarki z dnia 6 sierpnia 2002r. w sprawie określenia zasad wynagradzania za przeprowadzenie kontroli podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym, Dz.U. Nr 128, Poz.1100 , z dnia 12.08.2002r.

[4] ROZPORZĄDZENIE Ministra Gospodarki z dnia 6 sierpnia 2002r. 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, Dz.U. Nr 128, Poz.1099, z dnia 12.08.2002r.

[5] ROZPORZĄDZENIE Ministra Gospodarki z dnia 6 sierpnia 2002r. w sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym, Dz.U. Nr 128, Poz.1098, z dnia 12.08.2002r.

[6] ROZPORZĄDZENIE Ministra Gospodarki z dnia 6 sierpnia 2002r. w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym, Dz.U. Nr 128, Poz.1097, z dnia 12.08.2002r.

[7] ROZPORZĄDZENIE Rady Ministrów z dnia 7 sierpnia 2002r. w sprawie określenia 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. Nr 128, Poz.1094, z dnia 12.08.2002r.

[8] ROZPORZĄDZENIE Ministra Finansów z dnia 8 sierpnia 2002r. w sprawie sposobu i szczegółowych warunków spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot, Dz.U. Nr 128, Poz.1096, z dnia 12.08.2002r.

[9] ROZPORZĄDZENIE Ministra Gospodarki z dnia 9 sierpnia 2002r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym, Dz.U. Nr 128, Poz.1101, z dnia 12.08.2002r.

[10] Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64 poz. 565 z 2005 r.)

STANDARDY I NORMY

[11] ETSI Electronic Signature Formats, TS 101 733 v 1.3.1

[12] ETSI Policy requirements for time-stamping authorities, TS 102 023

[13] ETSI Policy requirements for certification authorities issuing public key certificates, TS 102 042

[14] ETSI Policy requirements for certification authorities issuing qualified certificates, TS 101 456 v1.2.1
[15] ISO/ITU-T Recommendation X.509 - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework
[16] RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[17] RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[18] RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile
[19] RFC 3161 Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)
[20] CWA 14170 "Security Requirements for Signature Creation Applications"
[21] PN-ISO/IEC 11770-1:1998 Technika informatyczna - Techniki zabezpieczeń - Zarządzanie kluczami - Struktura
[22] PN-ISO/IEC 11770-2:1998 Technika informatyczna - Techniki zabezpieczeń - Zarządzanie kluczami - Mechanizmy z zastosowaniem technik symetrycznych
[23] PN-ISO/IEC 11770-3:2000 Technika informatyczna - Techniki zabezpieczeń - Zarządzanie kluczami - Mechanizmy z zastosowaniem technik asymetrycznych
[24] PN-ISO/IEC 13888-1:1999 Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Model ogólny
[25] PN-ISO/IEC 13888-2:1999 Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Mechanizmy wykorzystujące techniki symetryczne
[26] PN-ISO/IEC 13888-3:1999 Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Mechanizmy wykorzystujące techniki asymetryczne
[27] PN-ISO/IEC 14888-1:2000 Technika informatyczna - Techniki zabezpieczeń - Podpis cyfrowy z załącznikiem - Opis ogólny

INNE MATERIAŁY

[28] Zbigniew Marański, Jerzy Pejaś, Wojciech Ślusarczyk - Budowa bezpiecznych usług internetowych na bazie certyfikatu klucza publicznego, IV Krajowa Konferencja Zastosowań Kryptografii ENIGMA'2000, Warszawa, maj 2000r.
[29] Jerzy Pejaś, Imed El Fray - Dokument elektroniczny, podpis elektroniczny i ich aspekty prawne, II Krajowa Konfrencja Naukowa E-Finanse, Szczecin, 8-9 listopada 2001r.
[30] Jerzy Pejaś - Unieważnianie i weryfikacja statusu certyfikatów kluczy publicznych, Szczecin 2001r., Wydawnictwo Informa
[31] Jerzy Pejaś, Andrzej Ruciński - Praktyczne aspekty realizacji podpisu elektronicznego, Europejskie Forum Podpisu Elektronicznego, 26-28 września 2002r., Międzyzdroje
[32] Włodzimierz Chocianowicz, Marek Witkowski - Kompozycja bezpiecznego podpisu elektronicznego – formaty i niezbędna struktura techniczno-organizacyjna, VI Krajowa Konferencja Zastosowań Kryptografii ENIGMA'2002, Warszawa, maj 2002r.
[33] Magdalena Marucha „Nowa ustawa o podpisie elektronicznym", Monitor Prawniczy 2/2002r.
[34] Dariusz Szostek, „Podpis elektroniczny - problemy cywilnoprawne", PPH 01/2002r.
[35] Mikołaj Drozdowicz, „(Nie)bezpieczny podpis elektroniczny", PPH 01/2003r.
[36] Zbigniew Radwański, „Elektroniczna forma czynności prawnej", Monitor Prawniczy 22/2001r.
[37] Mirosław Zmyślony, „Infrastruktura klucza publicznego (PKI) w strukturach administracji państwowej", Security IT Magazine, 10/2002r.

Ministerstwo Gospodarki

Wejście w życie ustawy o podpisie elektronicznym stanowi ważny krok w kierunku budowy społeczeństwa informacyjnego i gospodarki elektronicznej w naszym kraju. Wzrost znaczenia oraz bezsprzeczne korzyści z wykorzystania Internetu w biznesie, handlu lub kontaktach z urzędami sprzyjać będzie poszukiwaniu odpowiedzi na pytanie o rolę podpisu elektronicznego wśród następujących dynamicznie przemian. Niniejsza publikacja dostarcza Czytelnikowi podstawowych informacji dotyczących:

- zasad działania podpisu elektronicznego,
- organizacji infrastruktury klucza publicznego w Polsce,
- uregulowań prawnych bezpiecznego podpisu elektronicznego,
- obszarów zastosowań dla e-podpisu.

Podpis elektroniczny, wykorzystujący technologię PKI, czyli infrastrukturę klucza publicznego jest sposobem uniknięcia wielu zagrożeń w elektronicznym obrocie dokumentów. Pozwala on wiarygodnie zidentyfikować osobę podpisującą, zapewnia integralność elektronicznych dokumentów, a także może pomóc w zachowaniu ich poufności.

Przekazane w broszurze wiadomości są adresowane do każdego, komu niezbędna jest bieżąca wiedza o współczesnym obrocie prawnym i otoczeniu biznesowym. Znajomość zagadnień podpisu elektronicznego będzie zwłaszcza kluczowa dla urzędników i przedsiębiorców. Na administracji spoczywa obowiązek dokonania przeglądu istniejących przepisów prawa i wdrożenia podpisu elektronicznego do praktyki swego funkcjonowania. Ludzie biznesu powinni natomiast wykorzystać korzyści płynące z elektronicznego obrotu dokumentów i dokonać niezbędnych unowocześnień w obsłudze klientów oraz własnej organizacji.

Materiał przeznaczony do nieodpłatnego rozpowszechniania.
Wersja elektroniczna broszury dostępna na stronach internetowych Ministerstwa Gospodarki

Ministerstwo Gospodarki
DEPARTAMENT PRZEDSIĘBIORCZOŚCI , ul. Plac Trzech Krzyży 3/5, Warszawa 00-507
Tel. +22/ 628-09-81, Fax: +22/ 693-40-30, E-mail: sekretariatdwo@mg.gov.pl

ISBN: 83-914536-4-2