

Podpis elektroniczny

Opracowanie na podstawie:

- ★ Ustawa o podpisie elektronicznym z dnia z dnia 18 września 2001 r.
- ★ Dąbrowski W., Kowalczyk P.: Podpis elektroniczny. Mikom 2003. Warszawa
- ★ Zawartość stron internetowych centrów certyfikacji
- ★ <http://pl.wikipedia.org>

Dr hab. Wacław Laskowski, Katedra Organizacji i Ekonomiki Konsumpcji

Podpis elektroniczny

Co to jest, do czego służy?

Podpis elektroniczny to nowy sposób potwierdzania autentyczności dokumentu

lub ogólniej
obiekту elektronicznego i tożsamości nadawcy

Integralność (obiekt nie został zmieniony)

Wiarygodność (zapewnienie, że wiadomość została wysłana przez osobę, która się podpisała pod tą wiadomością)

Niezaprzeczalność (osoba, która wysłała/otrzymała wiadomość nie może zaprzeczyć, że dokonała tej czynności)

Podpis elektroniczny

Co to jest, do czego służy?

Ustawa o podpisie elektronicznym z dnia 18 września 2001 roku jest tylko jednym z pierwszych kroków do możliwości czynienia podpisów elektronicznych, zwłaszcza bezpiecznych podpisów

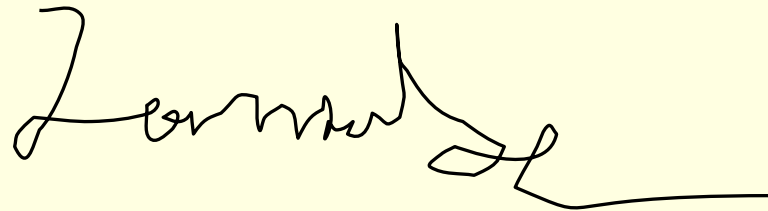
Podpis elektroniczny znajdzie zastosowanie m. innymi w kontaktach z administracją publiczną, sądownictwem, bankami i innymi usługodawcami a także przy podpisywaniu umów na odległość.

Podpis elektroniczny

Podpis elektroniczny to zgodnie z ustawą 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 i sprawdzeniu integralności

```
1 1 0 0 1 0 1 0 1 1 0 1 1 0 0 1
1 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1
1 1 1 0 0 1 0 1 1 1 1 1 0 1 0 1
0 1 1 0 0 1 0 1 1 0 1 0 1 1 0 0
1 1 0 1 1 1 0 1 0 1 1 0 1 1 0 1
0 1 1 0 0 1 0 1 0 1 1 0 1 1 0 0
1 0 1 1 0 1 0 1 0 0 1 1 . . .
```

zamiast np:

A stylized, handwritten signature in black ink, consisting of a series of loops and a long horizontal stroke at the end.

Podpis elektroniczny

Ustawa o podpisie elektronicznym określa ogólne warunki, jakie muszą być spełnione, by nie można było odmówić ważności i skuteczności podpisu elektronicznego, a zatem by nie można było uniknąć skutków tego podpisu.

Ustawa o podpisie elektronicznym w szczególności określa

- wymagania odnoszące się do podmiotów świadczących usługi certyfikacyjne
- wymagania odnoszące się do urządzeń służących do składania podpisu

Podpis elektroniczny

Aby skutki wywołane przez podpis elektroniczny były takie same jak skutki wywołane przez podpis własnoręczny tradycyjny, powinien on spełniać takie same funkcje jak podpis własnoręczny. Oznacza to, że podpis elektroniczny powinien być:

- trudny (wręcz niemożliwy) do podrobienia,
- możliwy do zweryfikowania,
- łączyć się z dokumentem, czyli źródłowym obiektem elektronicznym.

Bezpieczny podpis elektroniczny

To taki, który:

- jest przyporządkowany wyłącznie **do osoby składającej podpis,**
- 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,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna

Jeśli posiadamy kwalifikowany certyfikat i bezpieczne urządzenie to możemy mówić o bezpiecznym podpisie elektronicznym.

Bezpieczny podpis elektroniczny

To taki, który:

- jest przyporządkowany wyłącznie **do osoby składającej podpis,**
- 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,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna

Osoba składająca podpis elektroniczny to osoba fizyczna posiadająca urządzenie służące do składania podpisu elektronicznego, która działa w imieniu własnym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej

Znakowanie czasem

Art. 7. 1. Podpis elektroniczny może być znakowany czasem.

2. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego.

3. Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi.

Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę.

Kryptologia

Podpis elektroniczny oparty jest na technikach kryptograficznych (szyfrujących, utajniania)

Kryptologia to nauka o szyfrowaniu (kryptografia) i łamaniu szyfrów (kryptoanaliza)

Otrzymałem piątkę

Algorytm szyfrujący + klucz szyfrujący

Algorytm szyfrujący: np: zamiana liter w tekście źródłowym na kolejną literę wynikającą z alfabetu

Klucz np: 2

Wynik:

O t r z y m a ł e m p i ą t k ę
R V T B A O C N G O S K C V Ł G

Kryptologia

Algorytmy mają swoje nazwy, np: DES (symetryczny) i RSA oraz DSA (asymetryczne).

Klucze tych algorytmów powstają na drodze często bardzo skąplikowanych i długotrwałych obliczeń na bazie liczb losowych lub pseudolosowych)

Podpis elektroniczny

1	1	0	0	1	0	1	0	1	1	0	1	1	0	0	1
1	0	1	1	0	1	0	1	0	1	1	0	1	1	0	1
1	1	1	0	0	1	0	1	1	1	1	1	0	1	0	1
0	1	1	0	0	1	0	1	1	0	1	0	1	1	0	0
1	1	0	1	1	1	0	1	0	1	1	0	1	1	0	1
0	1	1	0	0	1	0	1	0	1	1	0	1	1	0	0
1	0	1	1	0	1	0	1	0	0	1	1

Wyróżniamy

Dane służące do składania podpisu elektronicznego - niepowtarzalne i przyporządkowane osobie fizycznej dane (liczba), które są wykorzystywane przez tę osobę do składania podpisu elektronicznego,

Dane służące do weryfikacji podpisu elektronicznego - niepowtarzalne i przyporządkowane osobie fizycznej dane (liczba), które są wykorzystywane do identyfikacji osoby składającej podpis elektroniczny,

Dane służące do weryfikacji podpisanej treści - niepowtarzalne i przyporządkowane podpisywanemu plikowi w postaci elektronicznej dane (liczba), które są wykorzystywane do weryfikacji integralności podpisanej treści,

Klucz publiczny i klucz prywatny

Do podpisywania elektronicznego potrzebne są dwa klucze (specjalne numery) - publiczny i prywatny. Można je otrzymać (wygenerować) na specjalnych kartach mikroprocesowych lub przy użyciu odpowiedniego programu komputerowego (generatora). Karty procesorowe wymagają czytnika podłączanego do komputera.

Klucz prywatny musi być pilnie strzeżony.

Klucz publiczny jest upubliczniany, aby osoba do której wyślemy dokument podpisany elektronicznie mogła stwierdzić czy to nasz podpis i czy nikt nie zmienił treści przesłanego dokumentu.

Funkcja skrótu (haszująca, odcisk)

To funkcja matematyczna (obrachunkowa), która przyporządkowuje każdej liczbie wartość określaną jako hash (skrót, formalne streszczenie).

Jeżeli dwie liczby są różne, to ich hashe też powinny być różne z wysokim prawdopodobieństwem. Hash ma zwykle pewną z góry ustaloną długość (np. 128 bajtów) i daje się bardzo łatwo obliczyć. Funkcja haszująca powinna uniemożliwiać łatwe obliczenie oryginalnej liczby na podstawie jej skrótu (hashu).

Funkcja skrótu (haszująca, odcisk)

Dla komputerów podpisywane obiekty elektroniczne (dokumenty tekstowe, skoroszyty, pliki graficzne, muzyczne itp.) łańcuchy (ciągi) liczb.

Zwykle hash oblicza się właśnie dla takich ciągów.

Właściwości funkcji skrótu powodują, że zmiana choć jednego znaku w hashowanym tekście powinna powodować bardzo dużą zmianę jego skrótu.

Jeżeli mamy hash jakiegoś tekstu, to odszukanie jego oryginalnej treści wymaga ogromnej mocy obliczeniowej i jest prawie niemożliwe, czyli praktycznie jest niemożliwe.

Funkcja skrótu (haszująca)

Funkcje haszujące używane w kryptografii:

- historyczne: [..MD2](#), [..MD4](#), [..SHA](#)
- współczesne: [..MD5](#), [..SHA1](#), [..SHA2](#), [..RIPEMD](#)

Haszem (w *jakimś sensie*) jest liczba kontrolna obecnie używanych numerów bankowych.

Funkcja skrótu - przykład

Otrzymany 30-to cyfrowy ciąg cyfr (24 cyfry bankowe i 252100) dzieli się przez 97 i zapisuje resztę (działanie modulo 97),

Otrzymaną w wyniku tego działania liczbę odejmuje się od 98,

Jeżeli powstała w ten sposób liczba jest jednoznakowa (mniejsza od 10), uzupełnia się ją wiodącym zerem i umieszcza po lewej stronie numeru rachunku;

Jeżeli zaś jest większa lub równa 10, umieszcza się ją bez zmiany po lewej stronie numeru rachunku.

Istota podpisu elektronicznego

Podpis elektroniczny jest kryptograficznym przekształceniem skrótu (haszu) z wykorzystaniem odpowiedniego algorytmu asymetrycznego i klucza prywatnego, przy czym skrót powstał z dokumentu (obiektu) podpisywanego.

Czynność podpisu elektronicznego

Podpis elektroniczny jest kryptograficznym przekształceniem skrótu (haszu) z wykorzystaniem odpowiedniego algorytmu asymetrycznego i klucza prywatnego.

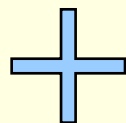
010100000100111100011010001011000010100110010111101101
10100000100111100011010001011000010100110010111101101.
.....

Dokument do podpisu



1 1 0 0 1 0 1 0 1 1 0 1 1 0 0 1
1 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1
1 1 1 0 0 1 0 1 1 1 1 1 0 1 0 1
0 1 1 0 0 1 0 1 1 0 1 0 1 1 0 0
1 1 0 1 1 1 0 1 0 1 1 0 1 1 0 1
0 1 1 0 0 1 0 1 0 1 1 0 1 1 0 0
1 0 1 1 0 1 0 1 0 0 1 1 . . .

Skrót
(hash)



10011001010010110101011
01100000001011110001010
1000011100100010101010
1010

Tajny
klucz
prywatny

111101101110101101101
011101010101101010001
00101010100010101000
11010100101010101010
10010101

Podpis

Podpis elektroniczny - weryfikacja

Certyfikat to dokument istniejący w postaci elektronicznej, bywa dostępny z określonej witryny internetowej, jest związany z użytkownikiem podpisu elektronicznego.

Jest zaświadczeniem potwierdzającym tożsamość osoby posługującej się podpisem elektronicznym oraz to, że do jej klucza prywatnego przynależy klucz publiczny umieszczony na certyfikacie.

Certyfikat, oprócz danych identyfikujących osobę i klucza publicznego, zawiera też dane informujące o tym, czy osoba, która się tym certyfikatem posługuje działa:

- w imieniu własnym, czy działa
- jako przedstawiciel innej osoby fizycznej bądź prawnej,
- jako przedstawiciel organu, instytucji,
- jako organ władzy publicznej.

Zanim instytucja świadcząca usługi certyfikacyjne wyda certyfikat umożliwiający danej osobie posługiwanie się bezpiecznym podpisem elektronicznym dokona sprawdzenia autentyczności danych osoby wnioskującej o wystawienie certyfikatu.

bez

Wersja certyfikatu 3 Numer seryjny: 168499 Algorytm po dpisu: sha1WithRSAEncryption Wystawca certyfikatu: /C=PL/ST=Zachodniopomorskie/L=Szczecin/O=Zaufana Trzecia Strona Unizeto/OU=Centrum Certyfikacji CA-ZEW/CN=UNIZETOTTPCAZEW Odbiorca certyfikatu: /C=PL/ST=mazowieckie/L=Warszawa/O=ZUS/OU=Centralny Osrodek Wazny od: Sep 16 00:00:00 2003 GMT Wazny do: Sep 30 23:59:59 2004 GMT **Klucz publiczny: Modul:**
**A42F0F75363545EB89C9BDC2725C115B5A336D00576B22D0A54D39C40B27B13D303E64A29
50BC5C2F883172E90E4A0D500047CD09AF9E7572D1632B890550473FB20696E4EEA9A4FB9
1050899F992AAC5A5F586024396C15AA9622E400BC65D010D71E755106FD79C5CFF2A4913F
7E5E8B05B9A5E6C94DD47CA943D51779808F**

EkspONENTA: 03 Podpis cyfrowy:

B1025BD52D1E3E4287F3285D4C6461F6390E51530919BB849D2EC68F444058282AD2B0CFA8
37B1063B156B09858421AEC4E7E5595E2E58425E350D29AA45A53EB501D11A1A7BF61EED74
2C1224D249683Bb6B70E72D0DA6B80AB89E3C7138F6ECB22422BFBAE7721AEA2D5C1548D9
1A6187F3FEFF3B3798550BD909BEC421CB966C5705087F53B91EFDD5EE642FD7A79D2BC71
96EDE4D9BFDA2A9B7C7B43AA98FCBA9E04850FF09D9882BD0EA2A8998182379114E7B5F1C
C91FA02C654A236361D5D794C3A3CE03D9A25B23308E51AC6BE70B849D2DE840D330AF3AB
8C1778323A56FAA1AAA07E91CEA48EF34C4957776143F7E1CD8DA785F74DFDE1205D39590

Rozszerzenia: Identyfikator klucza wystawcy: F725B4937D08B47A3129C845F4A5C20D6F89CEE6 Nazwa wystawcy: UNIZETOTTPCAZEW Nr seryjny certyfikatu podpisujacego: 0F Identyfikator klucza odbiorcy: CB756D577D89D88A820793B68C61F3B1B2319826 Klucz prywatny wazny od: Sep 16 00:00:00 2003 GMT Klucz prywatny wazny do: Sep 15 23:59:59 2004 GMT Typ klucza: digitalSignature keyEncipherment Typ certyfikatu: ZUSJedOrg Alternatywna nazwa odbiorcy: abc@unet.pl Alternatywna nazwa wystawcy: cde@unet.pl basic cons cA : 0 basic cons pathLen : 0 Policy: policy 1 : X509v3 Pkix Specific OID qualifier policy 2 : X509v3 Certificate Policies Unotice policy 3 : http://www.cc.unet.pl/repozytorium/polityka Punkty dystrybucji CRL [2]: Punkt dystrybucji CLR : http://www.cc.unet.pl,ftp://ftp.cc.unet.pl Wystawca CRL: UNIZETOTTPCAZEW Punkt dystrybucji CLR : http://www.ca.unet.pl,ftp://ftp.ca.unet.pl Wystawca CRL: UNIZETOTTPCAZEW

he7
Certyfikat zawiera następujące informacje:

Nazwa:	Laskowski Wacław
Adres poczty elektronicznej:	laskowski@alpha.sggw.waw.pl
Klasa:	PolCert Class 1 Demo - 1.2
Status:	Wygasł
Ważny od:	Dec-02-2003 14:15:34 GMT
Ważny do:	Jan-02-2004 14:15:34 GMT
Numer seryjny:	010000000000F9374B619D
Klucz publiczny:	BBDC9F186ABE97033F792F71D1A41725

Co poświadcza certyfikat:

- poświadcza tożsamość osoby fizycznej będącej w posiadaniu klucza prywatnego, który odpowiada kluczowi publicznemu wskazanemu w tym certyfikacie; weryfikacji tożsamości dokonuje centrum certyfikacji lub punkt rejestracji (terenowy).

Jeszcze o podpisie i certyfikacie

- Weryfikacja podpisu elektronicznego opiera się na niezaprzeczalności powiązania tożsamości osoby podpisującej z danymi służącymi do weryfikacji podpisu, czyli z konkretnym kluczem publicznym. Powiązanie to jest nazywane popularnie certyfikatem, który jest wydawany przez podmiot świadczący usługi certyfikacyjne. Podstawą technicznego rozwiązania Infrastruktury Kluczy Publicznych (PKI - Public Key Infrastructure) jest zalecenie ITU-T X.509. Zgodnie z tą definicją, certyfikatem klucza publicznego jest sekwencja danych, która charakteryzuje się następującymi właściwościami:
- określa jednoznacznie nazwę lub identyfikator podmiotu, który używa tego certyfikatu lub urządzenia,
- zawiera publiczny klucz, który odpowiada kluczowi prywatnemu znajdującemu się w posiadaniu danego podmiotu,
- określa okres ważności tego certyfikatu (i zawiera ewentualne ograniczenia użytkowania klucza publicznego),
- jest podpisany za pomocą prywatnego klucza podmiotu świadczącego usługi, który wydał certyfikat,
- umożliwia identyfikację podmiotu świadczącego usługi, który wydał certyfikat.
- Certyfikat może zawierać szereg innych, dodatkowych informacji.

Centra certyfikacji

www.signet.pl

www.polcert.pl

www.sigillum.pl

www.certyfikat.pl

www.unizeto.pl

<http://www.epodpis.pl/>

<http://www.e-podpis.pl/>

Karta kryptograficzna/czytnik



Co już można (luty 2008)

Obecnie podpis elektroniczny umożliwia:

- elektroniczne rozliczania z ZUS-em (od 7.0 wersji Płatnika),
- składanie wniosków do Krajowego Rejestru Sądowego,
- wysyłanie raportów do Generalnego Inspektora Informacji Finansowej,
- korespondencja z Generalnym Inspektorem Ochrony Danych Osobowych,
- wysyłanie deklaracji podatkowych do urzędów skarbowych,
- wystawianie faktur elektronicznych,
- wymiany informacji z urzędami administracji publicznej (termin obowiązkowy to maj 2008),
- podpisywanie dokumentacji medycznej celem jej archiwizacji,
- zabezpieczenie w bankowości elektronicznej (Nordea Bank Polska i BPH),
- podpisywanie umów i dokumentów w codziennej działalności firm,

Powstawanie kluczy

Klucz publiczny to para liczb (n, e)

Prywatny to liczba d

$n=pq$; **p q** to dwie duże liczby pierwsze

e względnie pierwsze z $(p-1)(q-1)$,

$de = 1 \pmod{n}$

szyfrowanie m : $c = m^e \pmod{n}$

deszyfrowanie c : $m = c^d \pmod{n}$

Szyfrowanie przesyłanej treści

„Infrastruktura” kluczy prywatnego i publicznego umożliwia dodatkowo szyfrowanie, czyli utajnione przesyłanie wiadomości (treści).

Ale:

- do szyfrowania używa się klucza publicznego,
- do rozszyfrowania klucza prywatnego.