

STOWARZYSZENIE PEMI

Przewodnik użytkownika

„wstęp do podpisu elektronicznego – kryptografia
asymetryczna „

© Stowarzyszenie PEMI
Podpis elektroniczny – Mobile – Internet
2005

1. Dlaczego podpis elektroniczny?

Podpis elektroniczny i cyfrowe certyfikaty, poświadczające tożsamość właściciela narzędzi, które umożliwiają składanie podpisu opracowano aby zabezpieczyć elektroniczny obrót dokumentów. Certyfikaty te wydawane są np. przez wskazane przez ustawodawcę urzędy, które jednocześnie udostępniają je wszystkim chętnym, chcącym sprawdzić prawdziwość (wiarygodność) podpisu. W dalszej części opracowań objaśnimy te pojęcia i powiemy, czym dokładnie jest certyfikat, w jaki sposób go zdobyć i zainstalować.

Wprowadzenie cyfrowego podpisu elektronicznego oraz szyfrowania stało się możliwe dzięki wykorzystaniu zaawansowanych technik szyfrowania (kryptografii), będących wynikiem osiągnięć w matematyce w ostatnich kilkudziesięciu latach. W efekcie nikt, nawet specjalizujące się w łamaniu szyfrów agencje rządowe i wojskowe, nie są w stanie odczytać zawartości przesyłki.

Znaczenie elektronicznego obiegu dokumentów doceniła również Rzeczpospolita Polska, która wzorem innych krajów wprowadziła ustawę o podpisie elektronicznym. Jej zadaniem jest zrównanie skutków prawnych podpisu elektronicznego z jego odpowiednikiem - podpisem odręcznym. Obecnie trwają prace nad prawem dotyczącym obiegu dokumentów, dzięki któremu będzie można między innymi zawierać umowy drogą elektroniczną tak by miały one moc prawną. Podpis elektroniczny wykorzystują powszechnie banki (system Eliksir), co pozwala błyskawicznie dokonać przelewów i innych operacji finansowych oraz ZUS (system Płatnik).

2. Cechy podpisu elektronicznego i cyfrowych certyfikatów

Poniżej przedstawiamy zestawienie głównych zalet elektronicznych certyfikatów:

Integralność - czyli pewność, że podpisany dokument od momentu złożenia podpisu elektronicznego nie został zmodyfikowany. Jeśli dokument został zmodyfikowany, odbiorca dokumentu zostanie o tym fakcie niezwłocznie poinformowany np. w formie komunikatu (forma powiadamiania zależy od oprogramowania używanego przez odbiorcę).

Wiarygodność - czyli pewność, że dokument lub wiadomość poczty elektronicznej (e-mail) pochodzi od osoby, która ją wysłała. Można łatwo sprawdzić, czy ktoś się pod tę osobę nie podszył

Niezaprzeczalność - czyli brak możliwości zaprzeczenia faktu złożenia podpisu. Zapewniają to techniki kryptograficzne, które zostały wykorzystane do złożenia podpisu - jedynie właściciel odpowiedniego narzędzia może złożyć podpis

Poufność - możliwość szyfrowania dokumentów oznacza, że dane zawarte w nim lub w wiadomości poczty elektronicznej (e-mail) nie zostaną odczytane przez osoby nieuprawnione. Zasyfrowana wiadomość lub dokument możliwy jest do odczytania tylko przez jedną osobę - osobę, która ma tę przesyłkę otrzymać (odbiorca).

3. Aspekty techniczne

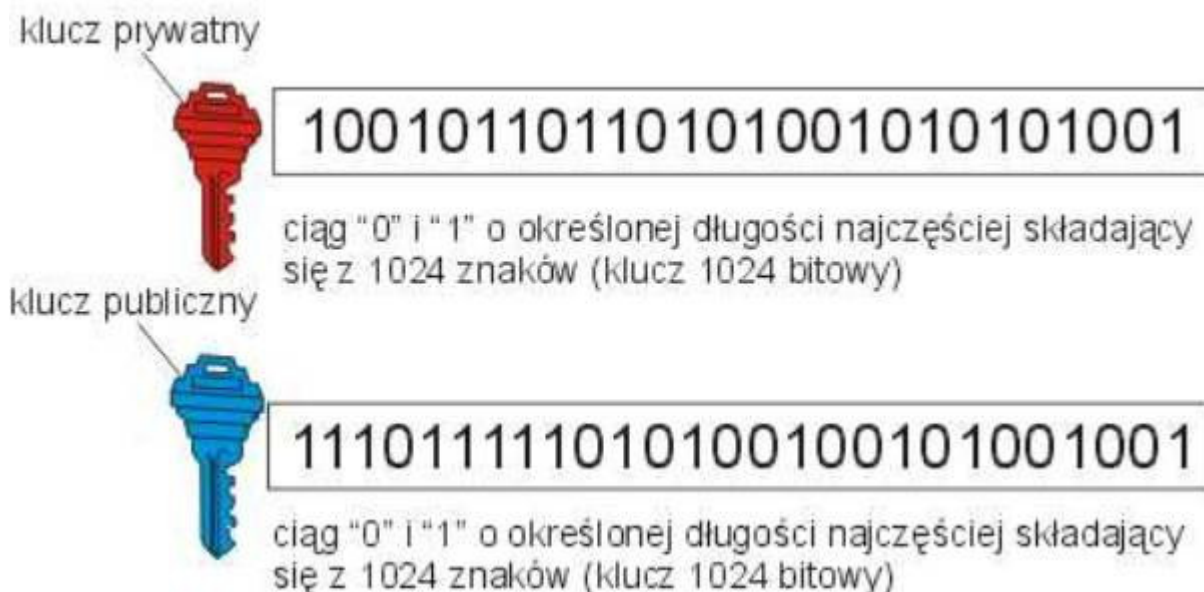
Zanim zacniemy posługiwać się podpisem elektronicznym musimy uzyskać niezbędne narzędzia do jego składania. Powinniśmy wybrać również nośnik dla naszego klucza prywatnego (karta lub system). Aby złożyć podpis musimy posiadać:

- certyfikat z kluczem publicznym oraz klucz prywatny.
- jeśli nośnikiem klucza prywatnego ma być karta mikroprocesorowa to dodatkowo musimy mieć taką kartę i czytnik.

Więcej szczegółów (oraz instrukcja krok po kroku) na temat pobierania certyfikatu znajduje się w dziale „podręczniki użytkownika” na www.podpiselektroniczny.pl

Kryptografia asymetryczna

Zanim zacniemy przedstawiać czym jest podpis elektroniczny skupmy się na chwilę na technologii, która jest wykorzystywana podczas tworzenia podpisu elektronicznego. Mowa tu oczywiście o „kryptografii asymetrycznej” czyli metodzie szyfrowania z wykorzystaniem dwóch kluczy (prywatnego i publicznego).



Jak sama nazwa wskazuje klucz prywatny jest znany i używany tylko przez jedną osobę (osobę składającą podpis) natomiast klucz publiczny jest ogólnie dostępny ze względu na to, że to właśnie przy jego użyciu możliwa jest weryfikacja podpisu. Klucze są to ciągi znaków o określonej długości np. 1024 bitów (ciąg składający się z 1024 zer i jedynek) wykorzystywane

w procesie szyfrowania i deszyfrowania (podpis elektroniczny to zaszyfrowany ciąg znaków). Chcielibyśmy w tym miejscu wyjaśnić dlaczego klucz publiczny zawarty jest w certyfikacie (Certyfikacie Klucza Publicznego) oraz jaką rolę pełni certyfikat w procesie weryfikacji podpisu.

Jak wspomnieliśmy wcześniej klucz publiczny (ciąg zer i jedynek) umieszczony jest w certyfikacie i wraz z certyfikatem bierze czynny udział w procesie weryfikacji podpisu. Gdybyśmy złożony podpis elektroniczny weryfikowali tylko przy pomocy klucza publicznego moglibyśmy jedynie stwierdzić że podpis został złożony przez posiadacza klucza prywatnego skojarzonego z kluczem publicznym przy pomocy którego dokonujemy weryfikacji i że dokument nie został zmodyfikowany.

Jeśli do weryfikacji użyjemy certyfikatu z kluczem publicznym dodatkowo możemy sprawdzić czy klucze są jeszcze ważne (to w certyfikacie zawarte są dane o miejscu przechowywania list CRL). Możemy sprawdzić również kto tak naprawdę jest autorem podpisu (w certyfikacie zawarte są informacje według jakiej polityki oraz w jaki sposób została przeprowadzona weryfikacja tożsamości), możemy również sprawdzić kto te dane potwierdzał (jakie centrum certyfikacji). Poniżej została przedstawiona ogólna struktura certyfikatu.



Przypuśćmy że chcemy coś zaszyfrować a następnie odszyfrować. Aby tego dokonać komputer musi postępować według określonych reguł (według algorytmów np. RSA, DH, DSA itp.) Upraszczając, proces szyfrowania moglibyśmy przedstawić wzorem np. $x * y = z$ gdzie:
x- to dane (treść wiadomości, dokumentu, lub jakieś dane elektroniczne)
y- to jeden z kluczy
z- to zaszyfrowany dokument.

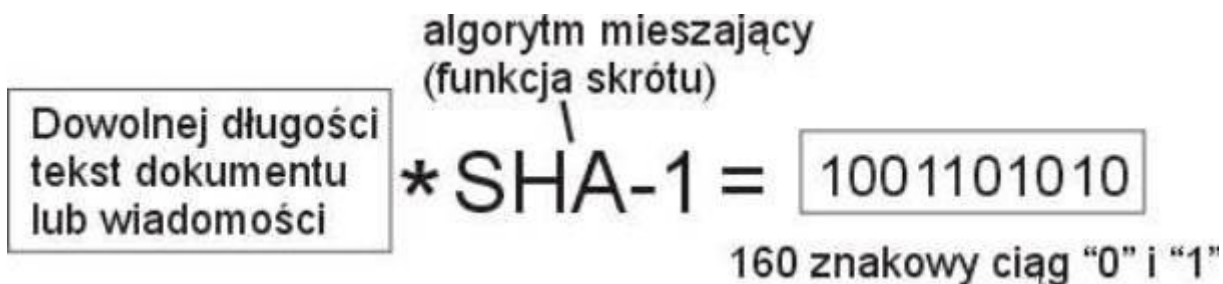
Aby odszyfrować dokument musimy użyć klucza przeciwnego czyli dane zaszyfrowane kluczem prywatnym rozszyfrowujemy kluczem publicznym i na odwrót dane zaszyfrowane kluczem publicznym rozszyfrowujemy kluczem prywatnym.



Podpis elektroniczny to ciąg znaków wygenerowany przez osobę składającą podpis przy użyciu jej klucza prywatnego. Jeśli dane zostały podpisane (czyli został wygenerowany wspomniany wcześniej ciąg znaków) mamy pewność że dane te zostały podpisane przez osobę mającą dostęp do klucza prywatnego oraz że od momentu podpisania dane te nie zostały zmodyfikowane.

Proces składania/weryfikacji podpisu elektronicznego.

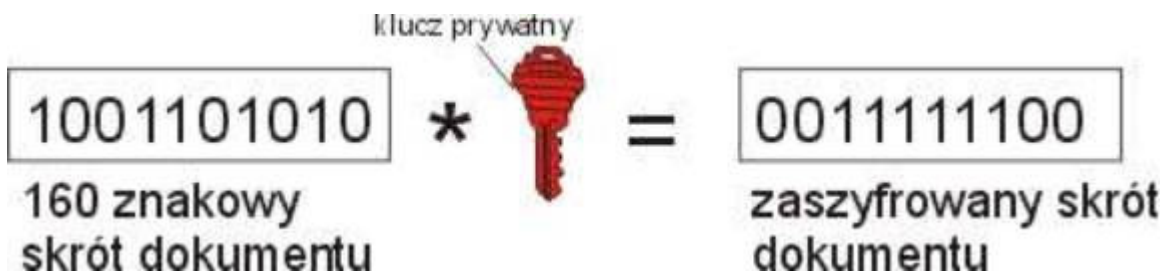
Zanim omówimy proces tworzenia podpisu powinniśmy poznać jeszcze jedno pojęcie „skrót z wiadomości lub dokumentu”. Skrót powstaje w wyniku przekształceń treści wiadomości lub dokumentu według algorytmu (wzoru) np. SHA-1 lub MD-5. Ten skrót jest reprezentacją treści np. dokumentu. Niezależnie od rodzaju sytemu operacyjnego, miejsca obliczania, wynik dla dokumentu o tej samej treści będzie zawsze taki sam. Długość takiego skrótu jest stała np. dla algorytmu SHA-1 to 160 bitów.



Składanie podpisu

Pierwszy krok - automatycznie zostaje obliczony skrót z dokumentu.

Drugi krok - obliczony skrót zostaje zaszyfrowany przy użyciu klucza prywatnego osoby podpisującej.



Trzeci krok - do dokumentu zostają dołączone: zaszyfrowany skrót oraz certyfikat z kluczem publicznym (certyfikat w celu zweryfikowania złożonego podpisu).



Tak podpisany dokument przesyłamy np. pocztą elektroniczną do odbiorcy.

Odbiorca, który otrzymał podpisany dokument może go odczytać ale aby zweryfikować podpis musi kliknąć na ikonę „zweryfikuj” (w zależności od oprogramowania polecenie weryfikuj znajduje się w różnych miejscach).

Weryfikacja podpisu

Pierwszy krok - automatycznie zostaje obliczony skrót z dokumentu.



Drugi krok - dołączony zaszyfrowany skrót zostaje rozszyfrowany przy użyciu klucza publicznego znajdującego się w załączonym certyfikacie.



Trzeci krok - rozszyfrowany skrót oraz skrót obliczony u odbiorcy zostają porównane, jeśli są równe oznacza to że podpis jest OK. A to oznacza, że dokument od momentu podpisania nie został zmodyfikowany oraz że autorem jest na pewno osoba widniejąca w certyfikacie (właściciel klucza prywatnego skojarzonego z certyfikatem i kluczem publicznym).

1001101010	=	1001101010
skrót obliczony z otrzymanego dokumentu		rozszyfrowany skrót obliczony z dokumentu w procesie podpisywania

Różnice między nośnikami klucza prywatnego (karta i system)

Klucz prywatny, czyli ta najbardziej poufna część z narzędzi do składania podpisu elektronicznego może być generowany i przechowywany w systemie użytkownika lub w karcie (jeśli klucz prywatny zostanie wygenerowany w karcie, pozostaje tam na zawsze i nigdy jej nie opuszcza). Jeśli klucz prywatny znajduje się w karcie mikroprocesorowej to sam proces tworzenia podpisu (szyfrowanie skrótu) odbywa się wewnątrz karty. Skrót jest przesyłany do karty, gdzie zostaje zaszyfrowany przy użyciu klucza prywatnego na zewnątrz wysłany zostaje już zaszyfrowany skrót czyli nasz podpis elektroniczny.