Ryszard Kossowski

PODPIS CYFROWY
klasyfikacja i standardy

Mechanizm podpisu cyfrowego jest technika kryptografii asymetrycznej, która moze byc uzywana w celu zapewnienia

- uwierzytelnienia danych,
- uwierzytelnienia podmiotów,
- niezaprzeczalnosci [ISO14888-1].

Podpis cyfrowy powinien spelniac nastepujace wymagania:

- Podpis jest tworzony przy pomocy klucza podpisu; utworzenie waznego podpisu dla jakiejkolwiek wiadomosci przy pomocy klucza weryfikacji jest obliczeniowo niewykonalne,
- Podpisy utworzone przez podpisujacego w czasie obowiazywania jego klucza podpisu nie moga byc uzyte do produkcji waznego podpisu dla jakiejkolwiek nowej wiadomosci. W szczególnosci, podpisy nie moga byc uzyte do odzyskania klucza podpisu,
- Znalezienie dwóch róznych wiadomosci z tym samym podpisem jest obliczeniowo niewykonalne nawet dla podpisujacego. [ISO14888-1]

Istnieje kilka klasyfikacji mechanizmów podpisu cyfrowego:

I. Jesli powiazanie poprawnego klucza weryfikacji z podmiotem podpisujacym jest w pewien sposób wlasciwe samemu kluczowi weryfikacji, to schemat powinien byc oparty na identyfikacji tozsamosci. Jesli nie, to powiazanie pomiedzy poprawnym kluczem weryfikacji a danymi identyfikujacymi podpisujacy podmiot musi byc zapewnione innymi srodkami. Niezaleznie od tego, jaka nature mialyby te srodki, schemat powinien wtedy byc oparty na certyfikacie.

II. Jesli mechanizm podpisu cyfrowego uzywa randomizera i podpisu wstepnego, to mówimy o schemacie losowym. Jesli taki generator nie jest uzywany to mówimy o mechanizmie, ze jest deterministyczny. W przypadku deterministycznego schematu cyfrowego, jesli wiadomosc i klucz podpisu sa takie same, to wartosc podpisu cyfrowego tez bedzie taka sama. Czesto konieczne celowe jest w takiej sytuacji otrzymanie innej wartosci. W takim przypadku powinien zostac uzyty schemat losowy.

III. Z punktu widzenia wiadomosci mechanizmy podpisu cyfrowego mozemy podzielic na trzy klasy:

IIIa. Odtworzenie wiadomosci na podstawie podpisu cyfrowego jest niemozliwe. W tym przypadku jest konieczne wyslanie wiadomosci do odbiorcy inna metoda. Zazwyczaj uzywa sie tak zwanego schematu podpisu cyfrowego z zalacznikiem.

IIIb. Wiadomosc moze byc czesciowo odtwarzana na podstawie podpisu cyfrowego. W przypadku tej metody wiadomosc musi byc podzielona na dwie czesci:

- Wlasciwa czesc wiadomosci M_{clr} jest ciagiem bitów o nieokreslonej dlugosci. Powinna byc oddzielnie przechowywana i przekazywana.
- Odtwarzalna czesc wiadomosci M_{rec} jest ciagiem bitów ustalonej dlugosci L_{rec}. Jesli mechanizm podpisu cyfrowego jest uzywany do podpisywania wiadomosci o zmiennej dlugosci, zaleca sie dodanie do wiadomosci kontrolnego pola, w którym bedzie definiowana dlugosc wiadomosci. Odtwarzalna czesc wiadomosci jest laczona razem z tokenem skrótu by uformowac wejsciowe dane, które maja byc podpisane [ISO9796-4].

W przypadku czesciowego odtworzenia, funkcja skrótu powinna byc odporna na kolizje. Zazwyczaj dlugosc skrótu wynosi 128 lub 160 bitów. [ISO9796-2].

IIIc. Jesli wiadomosc jest dostatecznie krótka moze byc w calosci zawarta w podpisie. W tej sytuacji jest mozliwe uzycie schematu podpisu cyfrowego zwanego schematem podpisu cyfrowego umozliwiajacym odtworzenie wiadomosci. W takim przypadku wysylany jest tylko zalacznik; nie ma potrzeby wysylania wiadomosci. W przypadku calkowitego odtworzenia, nie jest wymagana odpornosc na kolizje. Zazwyczaj dlugosc skrótu wynosi 64 lub 80 bitów. [ISO9796-2].

IV. Mechanizm podpisu cyfrowego moze sie opierac na:

IVa. Problemie faktoryzacji; jest niemozliwe znalezienie liczb pierwszych a i b znajac ich iloczyn $n = a*b$.

IVaEC. Problemie faktoryzacji krzywych eliptycznych; jest niemozliwe znalezienie P i Q znajac ich sume $S = P + Q$, gdzie P,Q,S – punkty na krzywej eliptycznej. (Schemat ten nie jest uzywany).

IVb. Problemie logarytmu dyskretnego; jest niemozliwe znalezienie dodatniej liczby calkowitej X znajac tylko Y, g i p zwiazanych równaniem $Y = g^X \bmod p$.

IVbEC. Problem logarytmu dyskretnego na krzywych eliptycznych; jest niemozliwe znalezienie dodatniej liczby calkowitej d na podstawie znajomosci tylko P i Q zwiazanych równaniem $Q = dP$, gdzie P i Q sa punktami na krzywej eliptycznej.

Kazdy mechanizm podpisu cyfrowego zawiera trzy podstawowe operacje:

1. Proces generowania kluczy,
2. Proces wykorzystujacy klucz podpisu; zwany procesem podpisu,
3. Proces wykorzystujacy klucz weryfikacji; zwany procesem weryfikacji.

Proces generowania kluczy

Proces generowania kluczy dla mechanizmu podpisu cyfrowego sklada sie z nastepujacych dwóch procedur:

1.1 Generowanie parametrów domeny.

Procedura generowania parametrów domeny jest wykonywana jeden raz w momencie powstawania domeny. Stanowiacy rezultat tej procedury zbiór Z parametrów domeny jest potrzebny do realizacji kolejnych procesów i funkcji. Ustawienie parametrów domeny moze zawierac dane takie, jak identyfikator funkcji skrótu, modul domeny, wykladnik weryfikacji domeny, czy tez parametry polityki bezpieczenstwa.

1.2 Generowanie klucza podpisu i klucza weryfikacji.

Ta procedura jest wykonywana dla kazdego podpisujacego podmiotu w domenie. Produktem procedury jest klucz podpisu X i klucz weryfikacji Y.

Proces podpisu

Proces podpisu moze sie skladac z nastepujacych procedur:

2.1 Tworzenie randomizera.

Randomizer to tajna wartosc tworzona przez podmiot podpisujacy i wykorzystywana tylko przez proces podpisu. Dla kazdej wiadomosci musi byc uzyta rózna wartosc randomizera, aby zachowac klucz podpisu w tajemnicy.

2.2 Tworzenie podpisu wstepnego

Podpis wstepny jest wartoscia wyliczona w procesie podpisu, bedaca funkcja randomizera która nie zalezy od podpisywanej wiadomosci.

2.3 Przygotowanie wiadomosci do wyslania

Danymi wejsciowymi procesu podpisu moze byc cala lub czesc wiadomosci, sluzaca do wyliczenia albo poswiadczenia albo samego podpisu (jego drugiej czesci albo obu tych elementów). W tym celu wiadomosc, która ma byc podpisana jest podzielona na dwie czesci (patrz III). Czesci te nie musza byc rozlaczone i jedna z tych czesci moze byc pusta. Wiadomosc powinna byc odtwarzalna za pomoca tych dwóch czesci [ISO14888-1].

Wiadomosc nie musi byc napisana w jezyku naturalnym jezyku. Moze to byc jakikolwiek dowolny ciag bitów. Przykladami takich wiadomosci sa kryptograficzne materialy kluczowe czy skrót innej dluzszej wiadomosci, co jest równiez nazywane „reprezentantem wiadomosci” („imprint of a message”). [ISO9796-1].

2.4 Obliczenie poswiadczenia

Poswiadczenie podpisu cyfrowego jest dana, której wartosc jest determinowana w procesie podpisu. Prawidlowosc wartosci poswiadczenia jest weryfikowana w procesie weryfikacji. Poswiadczenie jest obliczane jako funkcja wiadomosci, podpisu wstepnego lub obu. [ISO9796-1].

2.5 Obliczenie drugiej czesci podpisu.

2.6 Obliczenie podpisu,

2.7 Tworzenie zalacznika.

Zalacznik jest ciagiem bitów utworzonym przez podpis i dowolne pole tekstowe

2.8 Tworzenie podpisanej wiadomosci

Podpisana wiadomosc jest otrzymywana przez konkatenacje wiadomosci M i zalacznika.

Proces weryfikacji

Proces weryfikacji mechanizmu podpisu cyfrowego moze skladac sie z nastepujacych procedur:

3.1 Uzyskanie klucza weryfikacji.

Weryfikacja podpisu cyfrowego wymaga klucza weryfikacji podmiotu podpisujacego. Jest wazne dla podmiotu weryfikujacego by mógl on powiazac wlasciwy klucz weryfikacji z podmiotem podpisujacym, lub mówiac dokladniej, z danymi identyfikujacymi podmiot podpisujacy.

Podmiot weryfikujacy uzyskuje klucz weryfikacji Y z zalacznika lub uzyskuje wiedze o nim innymi srodkami, i sprawdza waznosc Y.

3.2 Przygotowanie wiadomosci do weryfikacji

Ta procedura musi byc identyczna z 2.3

3.3 Przywrócenie poswiadczenia i podpisu

3.4 Obliczenie funkcji weryfikacji

3.4.1 Obliczenie podpisu wstepnego

3.4.2 Obliczenie poswiadczenia

3.5 Weryfikacja poswiadczenia

W tym kroku dwie wartosci poswiadczenia sa porównywane, ta przywrócona w 3.3, i ta ponownie obliczona w 3.4.2. Jesli te dwie wartosci sa identyczne, to podmiot weryfikujacy otrzymuje dowód swiadczacy o tym, ze podmiot, który wytworzyl podpis ? dla wiadomosci M posiada klucz podpisu X korespondujacy z kluczem publicznym Y uzywanym w procesie weryfikacji.

Przyklady

W ponizszych przykladach zostaly opisane najbardziej znane i w wiekszosci juz ustandaryzowane algorytmy podpisu cyfrowego. Kazdy algorytm zostal przypisany (sklasyfikowany) do jednej z klas – I, II, IIIa, IIIb itd., które zostaly zdefiniowane powyzej. Algorytmy zostaly opisane w konwencji kolejnych kroków, zeby byly widoczne podobienstwa i róznice. W szczególnosci pokazano, ze nie we wszystkich algorytmach wystepuja podobne kroki.

We wszystkich ponizszych formalnych opisach uzyto wspólnych oznaczen:

M – podpisywana wiadomosc,
? – podpis cyfrowy,
text – dodatkowy tekst,
TTP – trzecia zaufana strona (centrum certyfikacji kluczy),
lcm – najmniejsza wspólna wielokrotnosc),

(a | b) – symbol Jacobiego.

Standard podpisu cyfrowego DSS

Klasyfikacja: I-oparty na certyfikacie, II-randomizowany, IIIa, IVb

1.1 Parametry stale i jawne:
- p – modul, liczba pierwsza, gdzie $2^{L-1}<p<2^{L}$ dla 512?L?1024 i L bedacego wielokrotnoscia 64,
- q – czynnik pierwszy p-1, gdzie $2^{159}<q<2^{160}$,
- g = $i^{(p-1)/q} \bmod p$, jezeli istnieje liczba calkowita 1<i<p-1 taka ze $i^{(p-1)/q} \bmod p>1$.

1.2 X – losowo lub pseudolosowo generowana liczba calkowita z 0<X<q – zwana kluczem podpisu,
Y = $g^{X} \bmod p$ - klucz weryfikacji.

2.1 K – losowo lub pseudolosowo generowana liczba calkowita z 0<K<q
2.2 ? = $g^{K} (\bmod p)$
2.3 - *nie wystepuje*
2.4 R = ? mod q
2.5 S = $(K^{-1}(H+X*R)) \bmod Q$, H = h(M) gdzie h( ) – funkcja skrótu, SHA - Secure Hash Algorithm
2.6 ? = (R,S)
2.7 zalacznik = (? ,text)
2.8 M || (? ,text)

3.1 Z zaufanego zródla otrzymany klucz Y.
3.2 - *nie wystepuje*
3.3 Z zalacznika ? ? R,S
3.4.1 ? '? $Y^{s'^{-1}R \bmod q} g^{s'^{-1}H' \bmod q} \bmod p$, H'=h(M')
3.4.2 R' = ? ' mod q
3.5 Weryfikacja, czy R' =? R

ECDSA – wersja podpisu cyfrowego DSA oparta na krzywych eliptycznych

Klasyfikacja: I-oparty na certyfikacie, II-randomizowany, IIIa, IVbEC

1.1 Parametry stale
- E – krzywa eliptyczna zdefiniowana dla ciala F_q,
- q – liczba pierwsza
- P – punkt rzedu n bedacy liczba pierwsza na $E(F_q)$

1.2 X – losowa liczba calkowita w przedziale [2,n-2] – klucz podpisu
Y = XP – klucz weryfikacji

2.1 K – losowa liczba calkowita w przedziale [2,n-2]
2.2 ? = KP = ($x_?$,$y_?$)

2.3 - *nie wystepuje*
2.4 R = $x_?$ mod n
2.5 S = $K^{-1}(H+X*R)$ mod n, H = h(M), h() – funkcja skrótu
2.6 ? = (R,S)
2.7 Zalacznik = (? ,text)
2.8 M || (? ,text)

3.1 Z zaufanego zródla otrzymany Y.
3.2 - *nie wystepuje*
3.3 Z zalacznika ? ? R,S
3.4.1 ? ‘ = $(S^{-1}R \bmod q)Y + (S^{-1}H' \bmod q)P = (x_{?\,'}, y_{?\,'})$, H’ = h(M’)
3.4.2 R’ = $x_{?\,'}$ mod n
3.5 Weryfikacja, czy R’ =? R

Podpis cyfrowy RSA

Klasyfikacja: I - oparty na certyfikacie, II - determininstyczny, IIIa, IVa

1.1 *nie wystepuje*
1.2 Parametry

p,q – liczby pierwsze, n=p*q - modul**.** Zadne dwa podmioty grupy nie moga miec takiego samego modulu n,
X – liczba calkowita, taka ze najwiekszy wspólny dzielnik gcd(X,(p-1)*(q-1))=1 – klucz podpisu,
Y – liczba calkowita, taka ze X*Y=1 mod (p-1)*(q-1) – klucz weryfikacji.

2.1 - *nie wystepuje*
2.2 - *nie wystepuje*
2.3 - *nie wystepuje*
2.4 R = H = h(M), h() jakakolwiek bezpieczna funkcja skrótu
2.5 S = R^X mod n
2.6 ? = S
2.7 Zalacznik = (? ,text)
2.8 M || (? ,text)

3.1 Z zaufanego zródla otrzymujemy Y.
3.2 - *nie wystepuje*
3.3 Z zalacznika ? ? S, H=S^Y mod n, R=H
3.4.1 - *nie wystepuje*
3.4.2 R’=H’=h(M’)
3.5 Weryfikacja, czy R’ =? R

Mechanizm podpisu Guillou-Quisquater

oparty na identyfikacji tozsamosci, klasyfikacja II-randomizowany, IIIa, IVa
[ISO14888-2]

1.1 Parametry

P,Q – liczby pierwsze, N=P*Q – modul

V – nieparzysta liczba calkowita, wzglednie pierwsza do P-1, Q-1 - wykladnik weryfikacji domeny

D – najmniejsza dodatnia liczba calkowita, taka ze DV-1 jest wielokrotnoscia lcm(P-1,Q-1). W szczególnosci dla kazdej liczby calkowitej U, 0<U<N $U^{DV} \bmod N = U$.

Publiczne parametry domeny to N i V. TTP zatrzymuje parametr D dla wlasnego uzytku. Inne podmioty nie powinny miec mozliwosci obliczenia parametru D z N i V.

Zbiór parametrów domeny zawiera funkcje tworzaca klucz publiczny y, która jest uzywana do przeksztalcenia danych identyfikacji podpisujacego sie podmiotu w dodatnia liczbe calkowita mniejsza niz N.

1.2 Kazdy podmiot (uzytkownik) posiada wlasne dane identyfikacji I.

TTP oblicza Y=y(I) i sprawdza czy Y nie jest wielokrotnoscia P lub Q. Y bedzie kluczem weryfikacji.

TTP oblicza prywatny klucz podpisu $X = Y^{-D} \bmod N$. Ten klucz podpisu spelnia równanie $X^V y(I) \bmod N = 1$.

2.1 K – losowo lub pseudolosowo generowana liczba calkowita taka, ze 0<K<N

2.2 ? $= K^V \bmod N$

2.3 - *nie wystepuje*

2.4 R = h(? ||M), h() - funkcja skrótu odporna na kolizje

2.5 $S = K*X^R \bmod N$

2.6 ? =(R,S)

2.7 zalacznik = (? ,text)

2.8 M || (? ,text)

3.1 Z danych identyfikacji podpisu I Y = y(I)

3.2 - *nie wystepuje*

3.3 Z zalacznika ? ? R,S

3.4.1 ? ‘ $= Y^R S^V \bmod N$

3.4.2 R’ = h(? ‘||M’)

3.5 Weryfikacja, czy R’ =? R

Schemat podpisu cyfrowego pozwalajacy na odtworzenie wiadomosci

Oparty na certyfikacie, klasyfikacja II-deterministyczny, IIIc, IVa
[ISO9796-1]

1.1 Parametry - p,q liczby pierwsze, n=p*q – publiczny modul

1.2 Y – publiczny wykladnik weryfikacji. Jesli Y jest liczba nieparzysta, to p-1 i q-1 powinny byc wzglednie pierwsze z Y. Jesli Y jest liczba parzysta, to (p-1)/2 i (q-1)/2 powinny byc wzglednie pierwsze z Y. Ponadto, p i q nie moga byc sobie równe mod 8.

Wartosci 2 i 3 dla wykladnika weryfikacji przynosza pewne praktyczne korzysci.

X – tajny wykladnik podpisu jest najmniejsza dodatnia liczba calkowita taka ze XY-1 jest wielokrotnoscia

- lcm(p-1,q-1) jesli Y jest liczba nieparzysta;
- lcm(p-1.q-1)/2 jesli Y jest liczba parzysta.

2.1 - *nie wystepuje*

2.2 - *nie wystepuje*

2.3 Wiadomosc M powinna byc ograniczonej dlugoscki. Najpierw M jest uzupelniana (MP), potem jest rozszerzana (ME), zamieniona na wiadomosc rozszerzona z redundancja MR i ostatecznie obcieta i obciazona (IR).

2.4 R = IR, jesli Y jest liczba nieparzysta,

= IR, jesli Y jest liczba parzysta oraz (IR | n) = +1,

= IR/2, jesli Y jest liczba parzysta i (IR | n) = –1.

2.5 - *nie wystepuje*

2.6 ? = min (R^X mod n, n-(R^X mod N)), ? jest dodatnia liczba calkowita mniejsza niz n/2.

2.7 zalacznik = (? ,text).

2.8 - *nie wystepuje*

3.1 Z zaufanego zródla otrzymujemy Y.

3.2 Odtworzenie wiadomosci: IS ? MR' ? ME' ? MP' ? M'

3.3 Z zalacznika ?

3.4.1 - *nie wystepuje*

3.4.2 IS = $?^Y$ mod n

R' = IS, jesli IS jest równy 6 mod 16,

= n-IS, jesli n-IS jest równy z 6 mod 16.

Ponadto, gdy Y jest liczba parzysta

R' = 2*IS, jesli IS jest równy 3 mod 8,

= 2*(n-IS), jesli if n-IS jest równy z 3 mod 8.

3.5 Weryfikacja, czy R' =? R

Literatura

[ISO14888-1] – ISO/IEC 14888-1 Information technology - Security techniques - Digital signatures with appendix - Part 1: General (istnieje polska norma PN ISO/IEC 14888-1 Technika informatyczna – Techniki zabezpieczenia - Podpis cyfrowy z zalacznikiem - Czesc 1: Model ogólny).

[ISO14888-2] – ISO/IEC 14888-2 Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms

[ISO14888-3] – ISO/IEC 14888-3 14888-3 Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms (istnieje polska norma PN ISO/IEC 14888-3 Technika informatyczna – Techniki zabezpieczenia - Podpis cyfrowy z zalacznikiem - Czesc 3: Mechanizmy oparte na certyfikatach).

[ISO9796-1] – ISO/IEC 9796 Information technology - Security techniques - Digital signature scheme giving message recovery (istnieje polska norma PN ISO/IEC 9796 Technika informatyczna – Techniki zabezpieczenia – Schemat podpisu cyfrowego z odtwarzaniem wiadomosci). Shemat ten zostal wycofany poniewaz zostal zlamany.

[ISO9796-2] – ISO/IEC 9796-2 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[ISO9796-3] – ISO/IEC 9796-3 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Mechanisms using a check-function

[ISO9796-4] – ISO/IEC 9796-4 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 4: Discrete logarithm based mechanisms

[DSS] – Federal Information Processing Standards Publication 186 - Digital Signature Standard

[IEEE P1363] – IEEE P1363 Standard for RSA, Diffie-Helman and related public-key cryptography