PrPN-ISO/IEC 9798-5

Uwierzytelnianie podmiotów

Mechanizmy wykorzystujace techniki wiedzy zerowej

5 Mechanizm oparty na identyfikacji tozsamosci

Wymagania

1. Srodki generacji liczb losowych.
2. Istnieje organ akredytujacy OA majacy zaufanie wszystkich.
3. Parametry dziedziny sa dostepne dla wszystkich (np. funkcja skrótu).
4. Kazdy czlonek musi dostac od OA dane identyfikacyjne.
5. Kazdy czlonek musi dostac od OA prywatna informacje akredytacyjna.

Parametry

1. Publiczny wykladnik akredytacji v.
2. Modul $n = p*q$, (p i q tajne) takie, ze
   nwd(p-1,v) = nwd(q-1,v) = 1 jesli v nieparzyste
   nwd((p-1)/2,v) = nwd((q-1)/2,v) = 1 jesli v parzyste
   $p - q$ nie moze byc wielokrotnoscia 8.
   k_S = ?log$_2$(n)? czyli n ma k_S+1 bitów.
   Stad tez wyznacza sie „prywatny wykladnik akredytacyjny” u OA, jest to
   Najmniejsza liczba calkowita u taka, ze $u*v$+1 jest wielokrotnoscia
   nww(p-1,q-1) jesli v nieparzyste
   nww(p-1,q-1)/2 jesli v parzyste.
3. Parametr krotnosci akredytacji m. Jest powiazany z v i krotnoscia wymiany t.
4. Parametr krotnosci wymiany t. Jest powiazany z v i m.

Wybór identyfikatora tozsamosci

Dane identyfikacyjne skladaja sie z m czesci: I_{A1}, I_{A2}, ... I_{Am},
gdzie $|I_{Ai}|$? 8?(k_S+3)/16? bitów.

?? Taki I_{Ai} moze skladac sie z bitowego ciagu identyfikujacego i numerów kolejnych 1, 2, ... ,m (tej samej dlugosci).

?? Jesli $|I_{Ai}|$ jest za dluga, mozna wziac skrót.

?? Do I_{Ai} moze byc dolaczana data utraty waznosci.

PrPN-ISO/IEC 9798-5

Uwierzytelnianie podmiotów

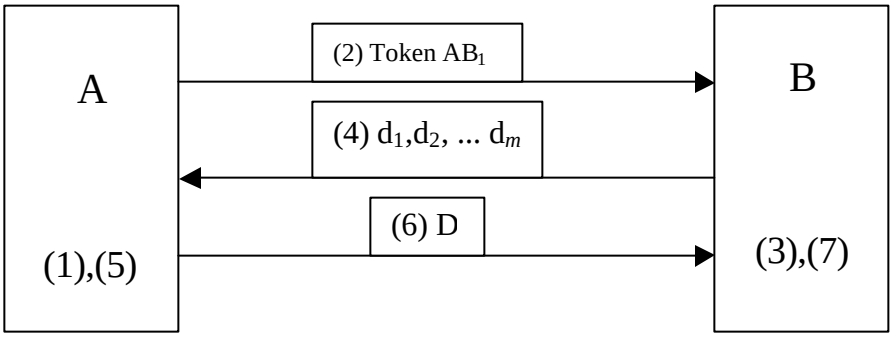
Mechanizmy wykorzystujace techniki wiedzy zerowej

5 Mechanizm oparty na identyfikacji tozsamosci

c.d.

Tworzenie akredytacji

I_{Ai} --- 4 1-sze kroki z ISO9796 -✍ IR -----✍ JA_i -----✍ $C_{Ai} = (J_{Ai})^u \bmod n$
Wlasnosc: $(C_{Ai})^u J_{Ai} = 1 \pmod n$.



(1) A wybiera liczbe losowa 1<r<n-1 (r tajne)
TokenAB$_1$ = W lub TokenAB$_1$ = h(W||tekst), W - poswiadczenie
(3) B losuje) $d_1,d_2, ... d_m$: $0 < d_i < v$-1. (wyzwanie)
(5) A liczy D – odpowiedz:

$$D \stackrel{?}{=} r \prod_{i=1}^{m} (C_{Ai})^{d_i} \bmod n$$

(7) B sprawdza

a) czy 0 < D < n/2. Jesli nie, odrzuca
b) oblicza J_{Ai} z I_{Ai}
c) oblicza

$$W' \stackrel{?}{=} D^v \prod_{i=1}^{m} (J_{Ai})^{d_i} \bmod n$$

d) sprawdza, czy $W = W'$ (lub h(W||tekst) h(W'||tekst)

Wszystkie kroki wykonuje sie t razy.

PrPN-ISO/IEC 9798-5
Uwierzytelnianie podmiotów
Mechanizmy wykorzystujace techniki wiedzy zerowej
6 Mechanizm oparty na certyfikatach
wykorzystujacy logarytmy dyskretne
Schemat Shnorra

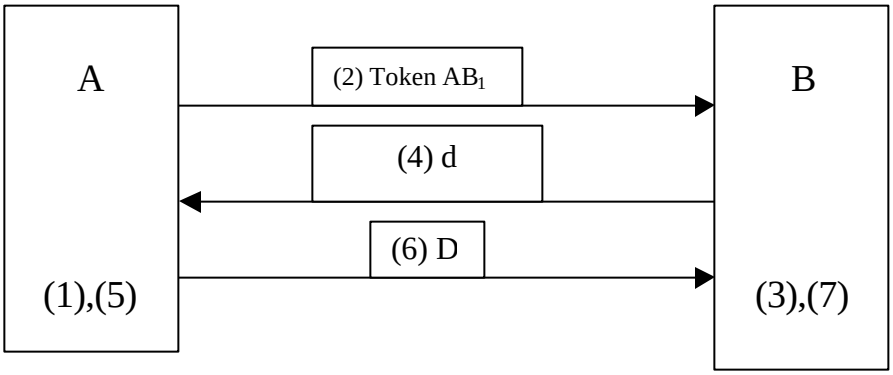
Wymagania

1. Srodki generacji liczb losowych.
2. Parametry dziedziny: p – liczba pierwsza, q – liczba pierwsza dzielaca p-1, oraz g takie, ze $g^q \bmod p = 1$, g ? 1.
3. Uzgodniona funkcja skrótu.
4. Kazdy czlonek ma pare kluczy.

Wybór kluczy

Kazdy czlonek ma klucz prywatny $0 < z_x < q$ oraz
klucz publiczny $y_x = g^{z_x} \bmod p$

Proces uwierzytelniania



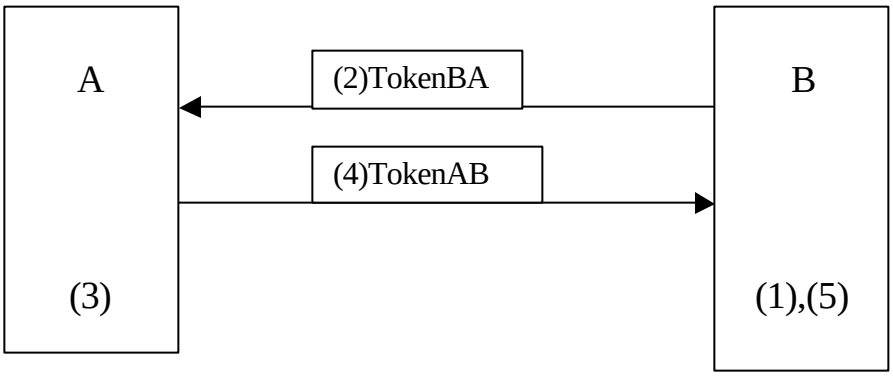
(1) A wybiera liczbe losowa 1<r<q (r tajne), $W = g^r \bmod p$
$TokenAB_1 = W$ lub $TokenAB_1 = h(W||tekst)$, W - poswiadczenie
(3) B losuje d: $0 < d < q$. (wyzwanie)
(5) A liczy $D = r - d*z_A \bmod q$ D - odpowiedz
(7) B sprawdza
a) czy 0 < D < q. Jesli nie, odrzuca
b) oblicza $W' = (y_A)^d g^D \bmod p$
c) sprawdza, czy $W = W'$ (lub $h(W||tekst) = h(W'||tekst)$). Jesli nie, odrzuca

PrPN-ISO/IEC 9798-5
Uwierzytelnianie podmiotów
Mechanizmy wykorzystujace techniki wiedzy zerowej
7 Mechanizm oparty na certyfikatach wykorzystujacy system szyfrowania asymetrycznego

Wymagania

1) Srodki generacji liczb losowych.
2) Uzgodnienie kryptosystemu asymetrycznego i funckji skrótu.
3) Kazdy czlonek ma pare kluczy.

Proces uwierzytelniania



(1) B wybiera liczbe losowa r - tajna, oblicza h(r):
r || h(r) ? P_A P_A – publiczne przeksztalcenie szyfrujace A
i oblicza d = P_A(r || h(r))

TokenBA = d d – wyzwanie

(2) A odtwarza S_A(d) = r || h(r).
Oblicza h'(r). Jesli h' ? h – przerywa.
Podstawia D = r.

TokenAB = D D – odpowiedz

(5) Jesli D = r to OK.