



(12)

BREVET DE INVENȚIE

(21) Nr. cerere: **a 2010 01303**

(22) Data de depozit: **09.12.2010**

(45) Data publicării mențiunii acordării brevetului: **30.09.2014** BOPI nr. **9/2014**

(41) Data publicării cererii:

30.07.2012 BOPI nr. **7/2012**

(73) Titular:

• **UNIVERSITATEA TEHNICĂ DIN
CLUJ-NAPOCA, STR.MEMORANDUMULUI
NR.28, CLUJ-NAPOCA, CJ, RO**

(72) Inventatori:

• **AȘTILEAN ADINA, ALEEA CIOPLEA NR.9,
BL.S 9, SC.2, ET.2, AP.26, CLUJ-NAPOCA,
CJ, RO;**
• **FOLEA SILVIU, STR.METEOR NR.6,
BL.O 22, SC.2, ET.3, AP.21,
CLUJ-NAPOCA, CJ, RO;**
• **AVRAM CAMELIA, STR.REPUBLICII
NR.74/E, AP.7, TÂRNĂVENI, MS, RO;**
• **HULEA MIHAI, STR.BISTRIȚEI NR.7,
CLUJ-NAPOCA, CJ, RO;**

• **MIRON RADU FLORIN, STR.SLĂNIC
NR.5, AP.11, CLUJ-NAPOCA, CJ, RO;**

• **LEȚIA TIBERIU ȘTEFAN,
STR.MESTECENILOR NR.8, AP.19,
CLUJ-NAPOCA, CJ, RO;**

• **CIUPAN EMILIA, STR.MESTECENILOR
NR.6, AP.2, CLUJ-NAPOCA, CJ, RO**

(74) Mandatar:

**CABINET DE PROPRIETATE
INDUSTRIALĂ CIUPAN CORNEL,
STR. MESTECENILOR NR. 6, BL. 9E, AP. 2,
CLUJ NAPOCA, JUDEȚUL CLUJ**

(56) Documente din stadiul tehnicii:

**WO 2007/117914 A2; EP 1077555 A2;
US 2006/0242423 A1; EP 1370022 A1**

(54)

METODĂ SECURIZATĂ DE COMUNICAȚIE ÎNTRE DISPOZITIVE FIXE ȘI MOBILE



1 Invenția se referă la o metodă securizată de comunicație între dispozitive fixe și mobile,
pe baza amprentelor digitale, în vederea accesului la "Internet Banking", ATM, într-o zonă
3 cu acces limitat sau la o componentă software. De asemenea, metoda poate fi utilizată și
numai în scopul identificării personale, la distanță, a utilizatorilor.

5 Este cunoscută invenția **KR 20010039815 A**, care prezintă un sistem și o metodă de
criptare, utilizate în transmiterea de date. Acestea presupun existența unor mijloace hardware
7 și software atât la emisie, cât și la recepție, și parcurgerea unor etape precise. Într-o primă
fază, care se derulează la partea transmițătoare, se rețin, în memoria unui dispozitiv de
9 memorare, amprentele persoanelor autorizate să acceseze sistemul, mai precis,
caracteristicile amprentelor într-o formă criptată. La folosirea sistemului, se citește amprenta
11 utilizatorului, se extrag caracteristicile acesteia și se compară cu cele stocate anterior în
memoria dispozitivului de memorare. Dacă există o corespondență între amprenta citită și
13 una dintre amprentele memorate anterior, atunci se generează o cheie de criptare Y, care
va servi la criptarea unui mesaj introdus de utilizator de la o tastatură sau selectat dintr-o listă
15 de mesaje afișate pe un display. În continuare, se decriptează caracteristicile amprentelor
memorate anterior și criptate cu un algoritm general, se compară cu caracteristicile amprentei
17 examinate și, pe baza comparației, se determină un scor care este apoi folosit la generarea
unei a doua chei de criptare X. Cheia X este folosită în continuare la criptarea caracteristicilor
19 amprentei examinate. Mesajul transmis părții receptoare este format din ID-ul utilizatorului
a cărui amprentă a fost citită, din caracteristicile amprentei citite, criptată cu cheia X, și din
21 mesajul propriu-zis, introdus de utilizator, criptat cu ajutorul cheii Y. La partea receptoare,
mesajul recepționat este prelucrat și analizat după aceeași logică, dar parcursă în sens invers.

23 Sistemul și metoda, descrise în brevetul **KR 20010039815 A**, prezintă mai multe de-
zavantaje, unul dintre cele mai importante fiind acela că necesită transportul prealabil al unor
25 informații inițiale de la emisie la recepție, sub formă înregistrată. Sistemul necesită o
multitudine de dispozitive hardware și software, plasate atât la emițător, cât și la receptor;
27 dispozitivele părții transmițătoare par a fi plasate într-o locație fixă.

De asemenea, metoda descrisă în brevetul **KR 20010039815 A** nu beneficiază de
29 o fundamentare matematică corespunzătoare, probabilitatea de a genera aceeași cheie de
două ori nefiind suficient studiată.

31 Problema tehnică, pe care o rezolvă invenția, este realizarea unei comunicații securi-
zate între dispozitive fixe și mobile.

33 Metoda securizată de comunicație, conform invenției, presupune transmite-
rea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică și cu
35 durată de viață limitată. Metoda de generare a cheii simetrice se bazează pe un algoritm de
tipul Diffie-Hellman și utilizează informațiile rezultate din citirea amprentei digitale a partici-
37 panților la sesiunea de comunicație (minuțiile) și pe cele referitoare la pozițiile acestora.
Autentificarea se realizează conform unui protocol, care implică, pe lângă cele două infor-
39 mații enumerate mai sus (amprenta digitală și poziția utilizatorului), codurile de identitate ale
entităților implicate în procesul de comunicație, precum și numărul sesiunii de comunicație
41 între utilizatorii implicați. Acesta modifică cele două coduri de identitate, conform unui
algoritm prestabilit.

43 Metoda de securizare a comunicației între dispozitive fixe și mobile, conform invenției,
prezintă următoarele avantaje:

45 - generarea automată a unei chei unice pe sesiune, aceeași la emisie și recepție, fără
a necesita, sub nicio formă, transportul prealabil și riscant al unor date înregistrate. Volumul
47 necesar de date memorate este mic;

RO 127706 B1

- metoda se bazează pe o combinație formată nu numai din elemente de unicitate caracteristice persoanei (amprenta), ci și din elemente de unicitate generate prin aplicarea unor funcții cunoscute (SHA), ale căror proprietăți au fost riguros stabilite;	1
- pentru realizarea comunicației, nu este neapărat necesar ca utilizatorul să dispună de un calculator sau de un telefon mobil, fiind suficient un dispozitiv hardware mobil, special realizat și prevăzut cu o unitate de procesare și capacitate de memorie. Dispozitivul se caracterizează prin costuri, dimensiuni și consum de putere reduse, și este prevăzut cu posibilități de comunicație radio, bazate pe tehnologii larg răspândite (Wi-Fi, Bluetooth, GPRS);	3
- dispozitivul hardware, utilizat la citirea amprentei, la generarea cheii de criptare și la criptarea informațiilor de transmis, este mobil, cu precizarea că utilizarea acestuia trebuie să se facă în perimetrul unor locații prestabilite;	5
- terminalul mobil (aflat la partea transmițătoare) nu trebuie să dispună de o bază de date care să stocheze informațiile folosite la compararea cu amprenta citită. Această bază de date este stocată la nivelul unui server de aplicație distribuit;	7
- includerea informației, privind poziția actuală și poziția anterioară a utilizatorilor, printre informațiile care fac obiectul verificării înaintea autorizării accesului, sporește securitatea comunicației.	9
Se dă, în continuare, un exemplu de realizare a invenției, în legătură cu fig. 1...3, care reprezintă:	11
- fig. 1, arhitectura hardware a sistemului de acces securizat;	13
- fig. 2, arhitectura software a sistemului de acces securizat;	15
- fig. 3, schema de generare a cheii unice pe sesiune.	17
Sistemul de acces securizat permite comunicația între dispozitive mobile (subsistem emițător) și dispozitive fixe (subsistem receptor) sau între dispozitive fixe (adică între emițător fix și receptor fix). Un subsistem emițător 1 are în componența sa un cititor de amprentă FPS (Finger Print Sensor), prevăzut cu unitate de memorare și procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth, Wi-Fi (la distanță mică) sau GPRS (la distanță mare), un dispozitiv GPS (Global Positioning System) care comunică cu senzorul de amprentă FPS și un terminal mobil MT (de exemplu, un telefon mobil sau un PDA) care are înglobată tehnologie GPRS, sau un PC, prin intermediul acestui ultim dispozitiv (MT sau PC), realizându-se, de regulă, conectarea la subsistemul receptor 2. Conectarea unui subsistem emițător 1, cu subsistemul receptor 2, se poate realiza într-un punct de acces 4, cu ajutorul tehnologiei de comunicație fără fir sau într-un nod de comunicație 3, prin intermediul unei legături fizice (cu fir). Subsistemul receptor 2 constă într-un server de aplicație distribuit S_x , $x = 1, 2, \dots, m$, conectat la Internet, serverele componente S_x , $x = 1, 2, \dots, m$ fiind fixe.	19
Metoda de securizare, conform invenției, este implementată pe un dispozitiv hardware, mobil, FPS, special realizat, prevăzut cu o unitate de procesare și capacitate de memorie. Dispozitivul FPS este prevăzut cu posibilități de comunicație radio, bazate pe tehnologii larg răspândite (Wi-Fi, Bluetooth, GPRS). Nu este necesară, în mod obligatoriu, existența suplimentară a unui PC sau a unui telefon mobil, dispozitivul putând funcționa și independent.	21
Operațiile destinate procesării locale a amprentelor au loc la nivelul dispozitivului FPS și sunt urmate de transmiterea informațiilor esențiale (amprente, locația și codul de identificare) către un server de aplicație distribuit. Validarea datelor și accesul sunt posibile numai în locații având poziții predefinite, care pot fi determinate folosind GPS-ul în exteriorul clădirilor, respectiv, cu ajutorul tehnologiei Wi-Fi, în interiorul clădirilor. Transmiterea securizată a informațiilor între entitățile implicate se poate face utilizând tehnologii de comunicație fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.	23

1 În cazul subsistemului emițător 1, cheia de criptare unică pe sesiune se generează
la nivelul dispozitivului FPS, fără a necesita transportul prealabil și riscant al unor date
3 înregistrate.

Inițializarea sesiunii de comunicație pe canalul securizat și prelucrarea datelor în
5 vederea autorizării accesului la informație se realizează folosind un server de aplicație, la
nivelul căruia sunt verificate amprente, locația și codurile de identificare. Acestea sunt
7 stocate într-un sistem distribuit de baze de date.

Comunicația cu fir este utilizată doar între PC-uri, prin intermediul unor noduri de
9 comunicație. Terminalele mobile MT și calculatoarele PC comunică cu senzorul de amprentă
FPS și cu receptorul GPS, folosind tehnologie Bluetooth B sau Wi-Fi (W).

11 Conform fig. 2, aplicația software, care rulează pe terminalul mobil (calculator sau
telefon mobil), conține funcțiile prezentate în continuare, împreună cu rolurile acestora:

- 13 - FPSFunction - realizează interfața cu senzorul de amprentare;
- GPSReader - citește periodic datele de la receptorul GPS;
- 15 - BluetoothInterface - comunicația cu senzorul de amprentare și receptorul GPS se
face folosind tehnologia Bluetooth. Această interfață interpretează datele din formatul
17 Bluetooth și le convertește într-un format utilizat mai departe;
- Autentification - modulul realizează verificarea și identificarea locală a amprentei;
- 19 - Security - informațiile transmise către/dinspre server sunt criptate/decriptate folosind
mai mulți algoritmi de criptare, în funcție de nivelul de securitate impus;
- 21 - GPRSComm / WiFiLAN - în funcție de tipul de acces la Internet, informația este
structurată pe pachete de date (GSM sau LAN).

23 Terminalele mobile MT sau/și serverul sunt inițializate cu amprente martor ale
partenerilor de dialog, date de senzorul FPS și pozițiile lor furnizate de receptorul GPS sau
25 determinate prin tehnologia Wi-Fi.

Protocolul de autentificare și asigurare a confidențialității informațiilor transmise între
27 dispozitive fixe și mobile se bazează pe execuția următorului algoritm de pe un terminal mobil
MT sau de pe server, ce execută:

- 29 - autentificarea utilizatorului terminalului prin citirea amprentei și compararea acesteia
cu amprenta martor, de care trebuie să difere cu mai puțin decât o valoare specificată;
- 31 - citirea poziției curente a terminalului;
- crearea cheii parțiale de criptare K' din amprenta curentă și poziția curentă.
- 33 - transmiterea cheii K', partenerului de dialog;
- recepționarea cheii parțiale de criptare similare, K'', de la partenerul de dialog.
- 35 - calculul cheii de criptare K din cheile parțiale K' și K'';
- criptarea cu ajutorul cheii K și transmiterea spre partenerul de dialog a informațiilor
37 cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii;
- recepționarea, de la partenerul de dialog, a unui mesaj criptat cu ajutorul cheii K,
39 ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară și
identificatorul sesiunii;
- 41 - extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta
curentă a partenerului de dialog, a poziției sale curente și anterioare;
- 43 - compararea amprentei curente a partenerului de dialog cu cea martor, corespunză-
toare. Se refuză dialogul, dacă diferența dintre amprenta transmisă a partenerului și cea
45 martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziția anterioară
nu coincide cu cea stocată în terminalul curent;
- 47 - actualizarea pozițiilor celor două perechi de terminale mobile;
- desfășurarea sesiunii de comunicație în mod criptat;
- 49 - închiderea sesiunii de lucru.

RO 127706 B1

Generarea cheii unice pe sesiune și transmiterea acesteia între utilizatori, conform fig. 3, se bazează pe algoritmul Diffie-Hellman, modificat, noutatea constând în modul în care se generează exponenții cheii secrete. Caracteristicile distinctive ale acestor exponenți se datorează caracteristicilor diferite ale amprente, respectiv, minuțiilor, precum și aplicării funcțiilor Hash, în scopul prelucrării minuțiilor. Chiar și în cazul aceleiași persoane, citirea succesivă a aceleiași amprente prezintă modificări, datorită poziționării diferite a degetului pe cititorul de amprente.	1 3 5 7
Suplimentar, aplicarea funcțiilor SHA asupra șirului de biți, care reprezintă un număr de minuții, va conduce la reprezentări binare sensibil diferite, pentru fiecare citire de amprentă.	9
Aceste șiruri de biți vor fi partajate și transmise bidirecțional între cele două terminale (emițător - receptor), pentru a genera cheia secretă.	11
Generarea cheii private K, din algoritmul de autentificare și asigurarea confidențialității informațiilor prezentate mai sus se realizează parcurgând următorii pași:	13
- se concatenează șirul de biți care reprezintă minuțiile cu șirul de biți care reprezintă poziția utilizatorului;	15
- se aplică un algoritm de tipul Secure Hash Algorithm (SHA) șirului de biți;	17
- se segmentează șirul de caractere rezultate în urma aplicării funcției SHA, în scopul efectuării operațiilor ulterioare; subșirurile obținute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subșiruri);	19
- se alege un număr prim, notat cu b în fig. 3;	21
- se alege un număr prim, suficient de mare, p;	
- terminalul 1 calculează valorile $u_1 = b^{t_{1j}}, \text{ mod } p$;	23
- terminalul 1 transmite, utilizatorului 2, valorile b, p și u_1 ;	
- terminalul 2 calculează valorile $u_2 = b^{t_{2j}}, \text{ mod } p$;	25
- terminalul 2 transmite, utilizatorului 1, valorile u_2 ;	
- ambii utilizatori calculează aceleași componente ale cheii secrete K_j :	27
$K_j = b^{t_{1j} * t_{2j}}, \text{ mod } p$, pentru $j = 1, 2, \dots, n$;	
- utilizând componentele K_j și o relație de compunere prestabilită, la cele două terminale, se calculează aceeași cheie secretă K' ;	29
- în scopul obținerii unei chei finale K, de lungime precizată, se aplică o funcție SHA, cheii secrete K' .	31

Revendicări

1. Metodă securizată de comunicație între dispozitive fixe și mobile, pentru transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică și cu durată de viață limitată, **caracterizată prin aceea că:**

- se citesc amprentele celor doi utilizatori, care comunică cu un dispozitiv mobil FPS de citire a amprente;
- se extrag minuțiile amprentelor;
- se citesc coordonatele GPS sau, în locații interioare, se utilizează tehnologia Wi-Fi, pentru precizarea pozițiilor utilizatorilor;
- se generează cheia privată, folosind datele achiziționate;
- se realizează autentificarea conform unui protocol care implică amprenta digitală și poziția utilizatorului, codurile de identitate ale entităților implicate în procesul de comunicație, precum și numărul sesiunii de comunicație între utilizatorii implicați, protocolul modificând cele două coduri de identitate, conform unui algoritm prestabilit, cheia de criptare fiind unică, pentru fiecare sesiune.

2. Metodă securizată de comunicație între dispozitive fixe și mobile, conform revendicărilor 1, **caracterizată prin aceea că** generarea cheii secrete de criptare, unice pe sesiune, se realizează astfel:

- se concatenează șirul de biți care reprezintă minuțiile cu șirul de biți care reprezintă poziția utilizatorului;
- se aplică un algoritm de tipul Secure Hash Algorithm (SHA) șirului de biți;
- se segmentează șirul de caractere rezultate în urma aplicării funcției SHA, în scopul efectuării operațiilor ulterioare; subșirurile obținute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subșiruri);
- se alege un număr prim, notat cu b ;
- se alege un număr prim, suficient de mare, p ;
- terminalul 1 calculează valorile $u_1 = b^{t_{1j}}, \text{ mod } p$;
- terminalul 1 transmite, utilizatorului 2, valorile b , p și u_1 ;
- terminalul 2 calculează valorile, $u_2 = b^{t_{2j}}, \text{ mod } p$;
- terminalul 2 transmite, utilizatorului 1, valorile u_2 ;
- ambii utilizatori calculează aceleași componente ale cheii secrete K_j :

$$K_j = b^{t_{1j} * t_{2j}}, \text{ mod } p, \text{ pentru } j = 1, 2, \dots, n;$$
- utilizând componentele K_j și o relație de compunere prestabilită, la cele două terminale, se calculează aceeași cheie secretă K' ;
- în scopul obținerii unei chei finale K , de lungime precizată, se aplică o funcție SHA cheii secrete K' .

3. Metodă securizată de comunicație între dispozitive fixe și mobile, conform revendicărilor 1 și 2, **caracterizată prin aceea că** utilizează un protocol de autentificare și asigurare a confidențialității informațiilor transmise între dispozitive fixe și mobile, care se bazează pe un algoritm ce se execută pe un terminal mobil MT sau pe un server, astfel:

- i) autentificarea utilizatorului terminalului prin citirea amprente și compararea acesteia cu amprenta martor, de care trebuie să difere cu mai puțin decât o valoare specificată;
- ii) citirea poziției curente a terminalului;
- iii) crearea cheii parțiale de criptare K' din amprenta curentă și poziția curentă;
- iv) transmiterea cheii K partenerului de dialog;
- v) recepționarea cheii parțiale de criptare similare, K'' , de la partenerul de dialog;

RO 127706 B1

vi) calculul cheii de criptare K din cheile parțiale K' și K";	1
vii) criptarea cu ajutorul cheii K și transmiterea, spre partenerul de dialog, a informațiilor cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii;	3
viii) recepționarea, de la partenerul de dialog, a unui mesaj criptat, cu ajutorul cheii K ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii;	5
ix) extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta curentă a partenerului de dialog, a poziției sale curente și anterioare;	7
x) compararea amprentei curente a partenerului de dialog cu cea martor corespunzătoare, se refuză dialogul dacă diferența dintre amprenta transmisă a partenerului și cea martor corespunzătoare diferă cu mai mult decât o valoare specificată sau poziția anterioară nu coincide cu cea stocată în terminalul curent;	9
xi) actualizarea pozițiilor celor două perechi de terminale mobile;	13
xii) desfășurarea sesiunii de comunicație în mod criptat;	
xiii) închiderea sesiunii de lucru.	15
4. Metodă securizată de comunicație între dispozitive fixe și mobile, conform revendicărilor 1, 2 și 3, caracterizată prin aceea că cheia de criptare, unică pe sesiune, se generează la nivelul subsistemului emițător (1), de către dispozitivul mobil (FPS), prin intermediul unităților de procesare și memorare, cu care acesta este prevăzut.	17
5. Metodă securizată de comunicație între dispozitive fixe și mobile, conform revendicării 1, caracterizată prin aceea că , în cadrul informațiilor de autentificare, se include și poziția actuală și poziția anterioară a utilizatorului, poziție în jurul căreia se acceptă schimbul de informații.	21
6. Metodă securizată de comunicație între dispozitive fixe și mobile, conform revendicării 1, caracterizată prin aceea că , la închiderea sesiunii de comunicație, valabilitatea cheii de criptare expiră.	23
	25

(51) Int.Cl.
H04L 9/12^(2006.01);
H04L 9/14^(2006.01);
H04L 9/32^(2006.01)

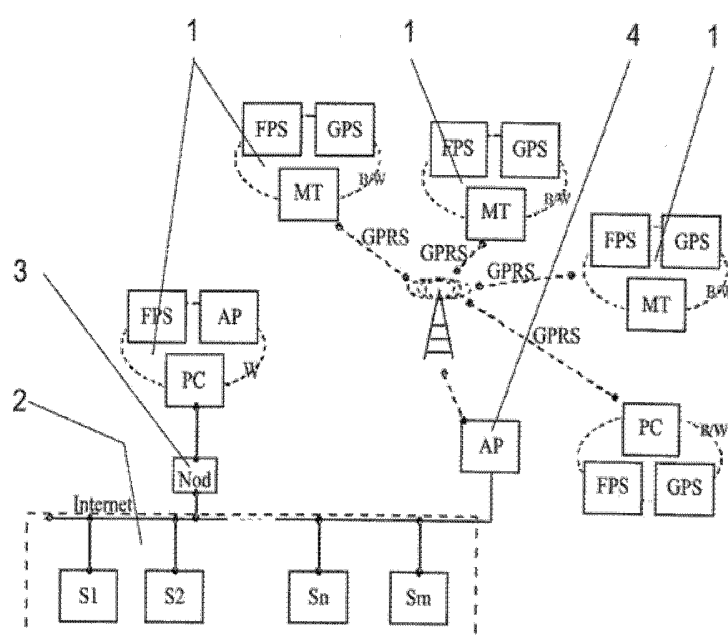


Fig. 1

(51) Int.Cl.

H04L 9/12 (2006.01),

H04L 9/14 (2006.01),

H04L 9/32 (2006.01)

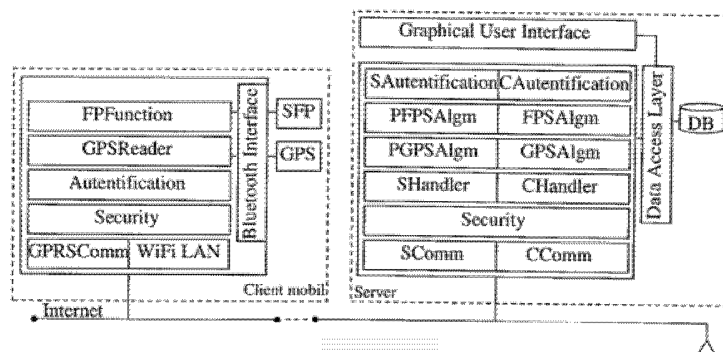


Fig. 2

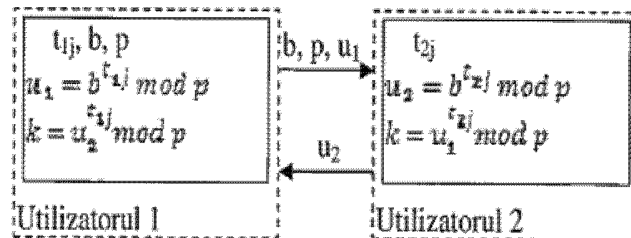


Fig. 3



Editare și tehnoredactare computerizată - OSIM
Tipărit la: Oficiul de Stat pentru Invenții și Mărci
sub comanda nr. 654/2014