(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 135286 A0**
(51) **Int.Cl.**
G06F 21/60 (2013.01),
H04L 9/28 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2020 00382**

(22) Data de depozit: **06/07/2020**

(41) Data publicării cererii:
29/10/2021 BOPI nr. **10/2021**

(71) Solicitant:
• **CITYDOCK S.R.L.**, *STR.AVIONULUI, NR.26, BIROU B, ET.1, SECTOR 1, BUCUREŞTI, B, RO*

(72) Inventatori:
• **MUŞAT MARIAN**, *SAT PĂULEŞTI NR.942, COMUNA PĂULEŞTI, PH, RO*

(74) Mandatar:
APPELLO BRANDS S.R.L., *STR.ŞOIMULUI NR.18, SC.A, ET.5, AP.M6, SIBIU, SB*

(54) # SISTEM ŞI METODĂ DE PROTECŢIE A DATELOR CONFIDENŢIALE DIN CORESPONDENŢA ELECTRONICĂ

(57) **Rezumat:**

Invenţia se referă la un sistem, un dispozitiv electronic şi o metodă de protecţie a datelor confidenţiale din corespondenţa electronică atunci când fişierele electronice sunt transmise prin orice metodă. Metoda conform invenţiei cuprinde o primă etapă de detectare automată, într-un fişier de tip text sau imagine, a datelor confidenţiale ale unui utilizator, pe baza unei baze de date pe care utilizatorul o completează în prealabil cu date precum: nume proprii, nume de companii, informaţiii comerciale, urmată de o etapă de înlocuire a acestor date confidenţiale cu markeri de poziţie, obţinând două fişiere, unul ce va conţine markerii de poziţie în locul datelor confidenţiale extrase şi un al doilea fişier de bază care conţine doar elementele neconfidenţiale, primul fişier fiind transmis pe o cale de comunicaţie separată (GSM/GPRS) de al doilea fişier care este transmis prin Ethernet, destinatarul recepţionând cele două fişiere transmise pe cele două căi de comunicaţie, iar un dispozitiv receptor al destinatarului recrează fişierul original, cu ajutorul unui algoritm. Dispozitivul electronic, conform invenţiei, cuprinde: un procesor (**1**) care execută algoritmul de extragere a datelor confidenţiale, un circuit de memorie (**7**) volatilă de tip RAM şi o memorie (**8**) nevolatilă de tip ROM, un circuit de memorie (**3**) de tip flash în care utilizatorul introduce datele considerate confidenţiale, o cartelă SIM (**4**) şi un microcontroler (**5**) prin intermediul cărora fişierul cu date confidenţiale se transmite pe canalul GSM/GPRS şi sistemele (**2** şi **6**) de coenxiune USB şi, respectiv, I2C.

Revendicări: 4
Figuri: 3

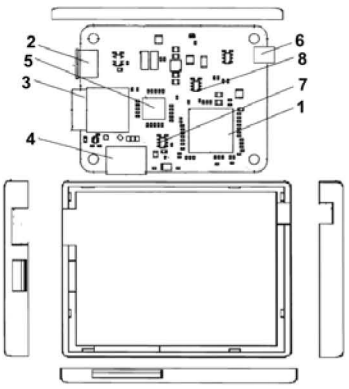

Fig. 3

Cu începere de la data publicării cererii de brevet, cererea asigură, în mod provizoriu, solicitantului, protecţia conferită potrivit dispoziţiilor art.32 din Legea nr.64/1991, cu excepţia cazurilor în care cererea de brevet de invenţie a fost respinsă, retrasă sau considerată ca fiind retrasă. Întinderea protecţiei conferite de cererea de brevet de invenţie este determinată de revendicările conţinute în cererea publicată în conformitate cu art.23 alin.(1) - (3).

RO 135286 A0

OFICIUL ... DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2020 00382
Data depozit 06 -07- 2020

SISTEM ŞI METODĂ DE PROTECŢIE A DATELOR CONFIDENŢIALE DIN CORESPONDENŢA ELECTRONICĂ

Invenţia se referă la un sistem şi o metodă care protejează datele confidenţiale din corespondenţa electronică atunci când fişierele electronice sunt transmise prin orice metodă.

Este cunoscut faptul că spionajul economic funcţionează de la nivelul structurilor statale la nivelul marilor companii, fiecare încercând să afle în avans diverse informaţii, cum ar fi detalii referitoare la tranzacţii comerciale, programe de cercetare şi/sau persoanele cheie ce sunt implicate în acestea. Sistemele de criptare au evoluat spectaculos, însă evoluţia acestora a fost însoţită de evoluţia sistemelor de decodificare corespunzatoare. Implementarea sistemelor de criptare/decriptare implică, însă, existenţa unei capabilităţi tehnologice corespunzatoare, cum ar fi servere de mare putere, software specializat, personal de specialitate, toate acestea fiind foarte scumpe şi nefiind la îndemâna companiilor mici care, însă, sunt şi ele ţinta atacurilor cibernetice.

În domeniul protecţiei datelor de acest gen este cunoscut din documentul **US2003182435** o metodă şi un dispozitiv portabil ce protejează cuvinte sau pictograme ce se doreşte a fi securizate, datele extrase împreună cu cele rămase după extragere fiind separate şi apoi stocate pe suporturi într-o unitate centrală, urmând ca acestea ulterior să fie reconstruite complet sau parţial numai în prezenţa unei autorizaţii de securitate.

Documentul **RO132172** prezintă o metodă şi un sistem online de criptare, transmitere, stocare şi citire a volumelor de date, de mari dimensiuni, care constă în crearea unor imagini din pixeli, criptarea şi apoi decriptarea datelor fiind efectuată cu o imagine color ale căror pixeli sunt generaţi pe baza valorilor numerice sau alfanumerice de stocat, ce are rolul de cheie de criptare.

Din documentul **RO 133066** este cunoscut un sistem de transmitere a corespondenţei în format electronic, sistem alcătuit dintr-o reţea de terminale conectate la un calculator central prin intermediul cărora corespondenţa în format electronic este transmisă direct la destinatar prin internet, în casuţa de poştă electronică, cu stocarea acesteia într-un centru

de date, forma de transmitere a corespondenţei fiind aleasă de către utilizator, prin accesarea unei platforme de comunicare găzduită de calculatorul central şi în urma căruia i se transmite un cod de expediere.

Problema tehnică pe care o rezolvă prezenta invenţie constă în protejarea datelor confidenţiale din corespondenţa electronică, a informaţiilor confidenţiale cuprinse în cadrul fişierelor transmise prin protocoale de reţele de calculatoare bazate pe transmisia cadrelor şi utilizată la implementarea reţelelor locale de tip LAN (Ethernet).

Sistemul şi metoda de protecţie a datelor confidenţiale din corespondenţa electronică, conform invenţiei, rezolvă problema tehnică propusă prin aceea că metoda de protecţie conform invenţiei presupune o etapă de detecţie automată a cuvintelor confidenţiale, pe baza unei baze de date pe care utilizatorul o completează în prealabil cu datele confidenţiale, cum ar fi nume proprii, nume de companii, informaţii comerciale, în etapa următoare are loc o înlocuire a acestor date cu markeri de poziţie, sistemul detectând în mod automat toate numerele de orice natură şi le va înlocui cu markeri de poziţie, datele extrase, asociate cu markerii de poziţie corespunzători, urmând a fi transmise pe o cale de comunicare separată (GSM/GPRS), în timp ce fişierul de bază, conţinând doar elementele care nu sunt identificate ca şi confidenţiale, este transmis prin Ethernet, metoda conform invenţiei fiind aplicată prin intermediul unui dispozitiv electronic autonom, ce poate fi ataşat sistemelor de calcul de tip desktop sau laptop fie prin inserarea acestuia într-unul din sloturile libere ale plăcii de bază, fie prin conectarea într-unul din porturile de intrări-ieşiri de tip magistrală universală de comunicaţii externă USB, dispozitiv autonom ce va executa analiza fişierelor de tip text sau imagine trimise, pentru imagini se aplica intai algoritmi de prelucrare imagini de ex: schimbare valori biti, blur imagine, identificare forme, etc, dupa care se se extrag parti din imagine sau anumite informatii din imagine considerate senzitive dupa un algoritm stabilit de comun acord intre emitator si receptor, între persoanele ce folosesc acest tip de dispozitiv, detectează automat anumite date din respectivul fişier, identificate în prealabil drept confidenţiale, le va atribui markeri de poziţie în text şi le va înlocui cu aceşti markeri de pozitie, urmând ca datele pe care proprietarul le doreşte a fi identificate drept confidenţiale să poată fi identificate de utilizator direct în text sau pot introduse intr-o librarie – oferindu-se astfel flexibilitate aplicaţiei. În afara acestor date prestabilite de proprietarul aplicaţiei, în cadrul fişierelor tip text, dispozitivul va

executa o marcare şi eliminare automată a tuturor numerelor precum şi a cuvintelor ce încep cu majuscule, asigurând astfel eliminarea informaţiei confidenţiale din textele transmise.

Dispozitivul autonom ce asigură executarea procesului este compus dintr-un procesor în care se execută algoritmul de extragere a datelor confidenţiale, un circuit de memorie volatila de tip RAM (random acces memory) şi o memorie nevolatilă ROM (read only memory) necesare pentru funcţionarea microprocesorului; un circuit de memorie de tip flash în care utilizatorul introduce cuvintele considerate confidenţiale; o cartela SIM şi un microcontroler prin intermediul cărora fişierul cu datele confidenţiale se transmite pe canalul GSM/GPRS şi sistemele de conexiune USB şi I2C .

Invenţia aduce următoarele avantaje:

- Posibilitatea securizării fişierelor transmise prin Ethernet.
- Posibilitatea eliminării automate a datelor cu conţinut confidenţial dintr-un fişier ce urmează a fi transmis prin Ethernet.
- Folosirea de resurse mult mai reduse în comparaţie cu metodele clasice de criptare.
- Dispozitivul poate fi interfaţat uşor cu orice sistem de calcul şi nu necesită cumpărarea de licenţe software specializate.
- Sunt eliminate potenţialele greşeli subiective în analiza conţinutului fişierului ce urmează a fi transmis.
- Folosirea unui canal paralel de comunicare (GSM/GPRS).

În cele ce urmează este prezentat un exemplu de realizare a invenţiei în legătură cu figurile 1- 3 care reprezintă :

Fig. 1 Algoritmul logic al dispozitivului electronic automat

Fig. 2 Schema legăturilor funcţionale ale sistemului conform invenţiei

Fig. 3 Dispozitivul ce asigură protecţia datelor confidenţiale.

Metoda de protecţie a datelor confidenţiale din corespondenţa electronică, text sau imagine, constă în detecţia automată a cuvintelor confidenţiale la discreţia utilizatorului, pe baza unei baze de date pe care acesta o completează în prealabil cu datele confidenţiale (de genul nume proprii, nume de companii, informatii comerciale). În etapa următoare are loc o înlocuire a acestor date cu markeri de poziţie. În mod automat sistemul va detecta toate numerele de orice natură şi le va înlocui cu markeri de poziţie. Datele extrase, asociate cu markerii de poziţie corespunzători, vor fi transmise pe o cale de comunicare separată (GSM/GPRS), în timp ce fişierul de bază, conţinând doar elementele care nu sunt identificate ca şi confidenţiale, poate fi transmis prin Ethernet.

Prin procesarea fişierului se vor obţine două fişiere: (i) un prim fişier „sanitizat" – în care datele confidenţiale sunt înlocuite cu markeri de poziţie şi (ii) un al doilea fişier „codat" ce conţine datele extrase, asociate markerilor de poziţie. Fişierul „sanitizat" va fi transmis către destinatar pe calea de comunicare clasică a protocoalelor de reţele de calculatoare, în timp ce fişierul ce conţine datele confidenţiale va fi transmis către modulul ataşat dispozitivului de calcul al destinatarului pe o cale de comunicare diferită de tip Sisteme Globale pentru Comunicatii Mobile (GSM/GPRS). Prin extragerea informaţiei confidenţiale şi separarea celor două fişiere ce se transmit pe căi de comunicare diferite, se realizează o securizare completă a transmisiei. Pentru reconstituirea fişierului iniţial, dispozitivul plasează datele din al doilea fişier, cel „codat", în primul fişier „sanitizat", urmărind un algoritm special de plasare, prin utilizarea markerilor de poziţie. Securizarea transmisiei este asigurată în primul rând de probabilitatea redusă de interceptare a ambelor fişiere, şi în al doilea rând de imposibilitatea asocierii celor două fişiere, fiind imposibilă asocierea unui fişier transmis prin Ethernet cu un fisier transmis prin GSM/ GPRS iar în al treilea rând de imposibilitatea plasării datelor din fişierul „codat" în fişierul „sanitizat" fără algoritmul dispozitivului.

Fişierul de bază, fără elementele confidenţiale poate fi recepţionat de către destinatar, însă acesta nu va avea nicio relevanţă fără datele transmise prin canalul GSM/ GPRS. Cu ajutorul dispozitivului electronic autonom receptor al destinatarului, prin intermediul unui algoritm instalat, se va putea recrea fişierul de baza. Pentru protecţie suplimentară, fişierele vor putea fi criptate.

Dispozitivul electronic autonom ce asigură protecția datelor confidențiale din fișiere, este compus dintr-un procesor **1** în care se execută algoritmul de extragere a datelor confidențiale prezentat în figura 1; un circuit de memorie **7** volatilă de tip RAM (random acces memory) și o memorie nevolatilă **8** ROM (read only memory) necesare pentru funcționarea microprocesorului; un circuit de memorie de tip flash **3** în care utilizatorul introduce datele considerate confidențiale; o cartelă SIM **4** și un microcontroler (**5**) prin intermediul cărora fișierul cu date confidențiale se transmite pe canalul GSM/GPRS și sistemele de conexiune USB **2** și I2C **6**.

Prin intermediul conectorului **2** USB, dispozitivul poate fi conectat la orice desktop, laptop, tabletă, și execută algoritmul de extragere și trimitere pe o cale de comunicare diferită (GSM/GPRS) a datelor confidențiale, separat de corpul mesajului transmis prin Ethernet.

Prin intermediul memoriei flash **3** utilizatorul are libertatea să stabilească singur și să încarce un fisier care să conțină cuvintele pe care le consideră confidențiale, acestea urmând să fie extrase din text și transmise pe o cale de comunicație diferită.

REVENDICĂRI

1. Metodă de protecţie a datelor confidenţiale din corespondenţa electronică **caracterizată prin aceea că,** într-un fişier de tip text sau imagine vor fi detectate automat anumite date confidenţiale pe baza unei baze de date pe care utilizatorul o completează în prealabil cu datele confidenţiale, cum ar fi nume proprii, nume de companii, informatii comerciale, urmată de etapa de înlocuire a acestor date confidenţiale detectate cu markeri de pozitie, obţinând două fişiere, unul ce va conţine markeri de poziţie în locul datelor confidenţiale extrase, fişier ce va fi transmis pe o cale de comunicare separată (GSM/GPRS), în timp ce un alt doilea fişier de bază, ce conţine doar elementele neconfidenţiale, este transmis prin Ethernet, destinatarul recepţionând cele două fişiere transmise prin cele două căi de comunicare, unde prin intermediul unui algoritm, va recrea fişierul de bază, procesarea fişierelor atât la utilizator cât şi la destinatar executându-se cu câte un dispozitiv electronic autonom .

2. Dispozitiv electronic autonom de protecţie a datelor confidenţiale ,**caracterizat prin aceea că** este compus dintr-un procesor (**1**) în care se execută algoritmul de extragere a datelor confidenţiale; un circuit de memorie (**7**) volatilă de tip RAM (random acces memory) şi o memorie nevolatilă (**8**) ROM (read only memory) necesare pentru funcţionarea microprocesorului; un circuit de memorie de tip flash (**3**) în care utilizatorul introduce datele considerate confidenţiale; o cartela SIM (**4**) şi un microcontroler (**5**) prin intermediul cărora fişierul cu date confidenţiale se transmite pe canalul GSM/GPRS şi sistemele de conexiune USB (**2**) şi I2C (**6**).

3. Sistem de de protecţie a datelor confidenţiale din corespondenţa electronică, **caracterizat prin aceea că** prin intermediul conectorului (**2**) USB, dispozitivul autonom poate fi conectat la orice desktop, laptop, tableta şi execută un algoritm de extragere şi trimitere pe o cale de comunicare diferită (GSM/GPRS) a datelor confidenţiale, separat de corpul mesajului transmis prin Ethernet.

4. Sistem de protecție a datelor confidențiale din corespondența electronică conform revendicării 3, **caracterizat prin aceea că,** prin intermediul memoriei flash (**3**) utilizatorul are libertatea să stabilească singur și să încarce un fișier care sa conțină cuvintele pe care le considera confidențiale, acestea urmând să fie extrase din text și transmise pe o cale de comunicație diferită.

Figura 1 Algoritmul logic al dispozitivului electronic automat

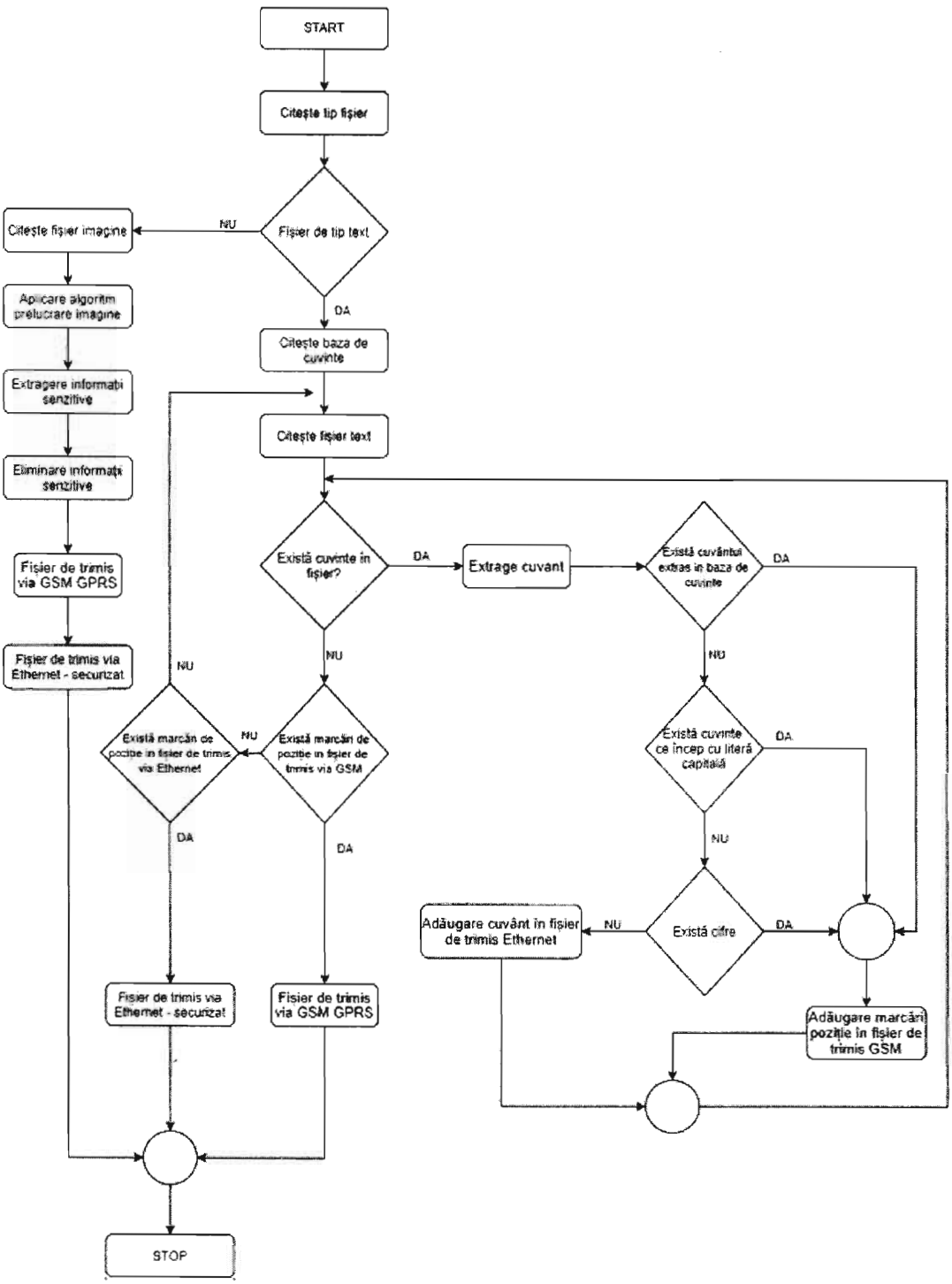

Figura 2 Schema legăturilor funcționale ale sistemului conform invenției

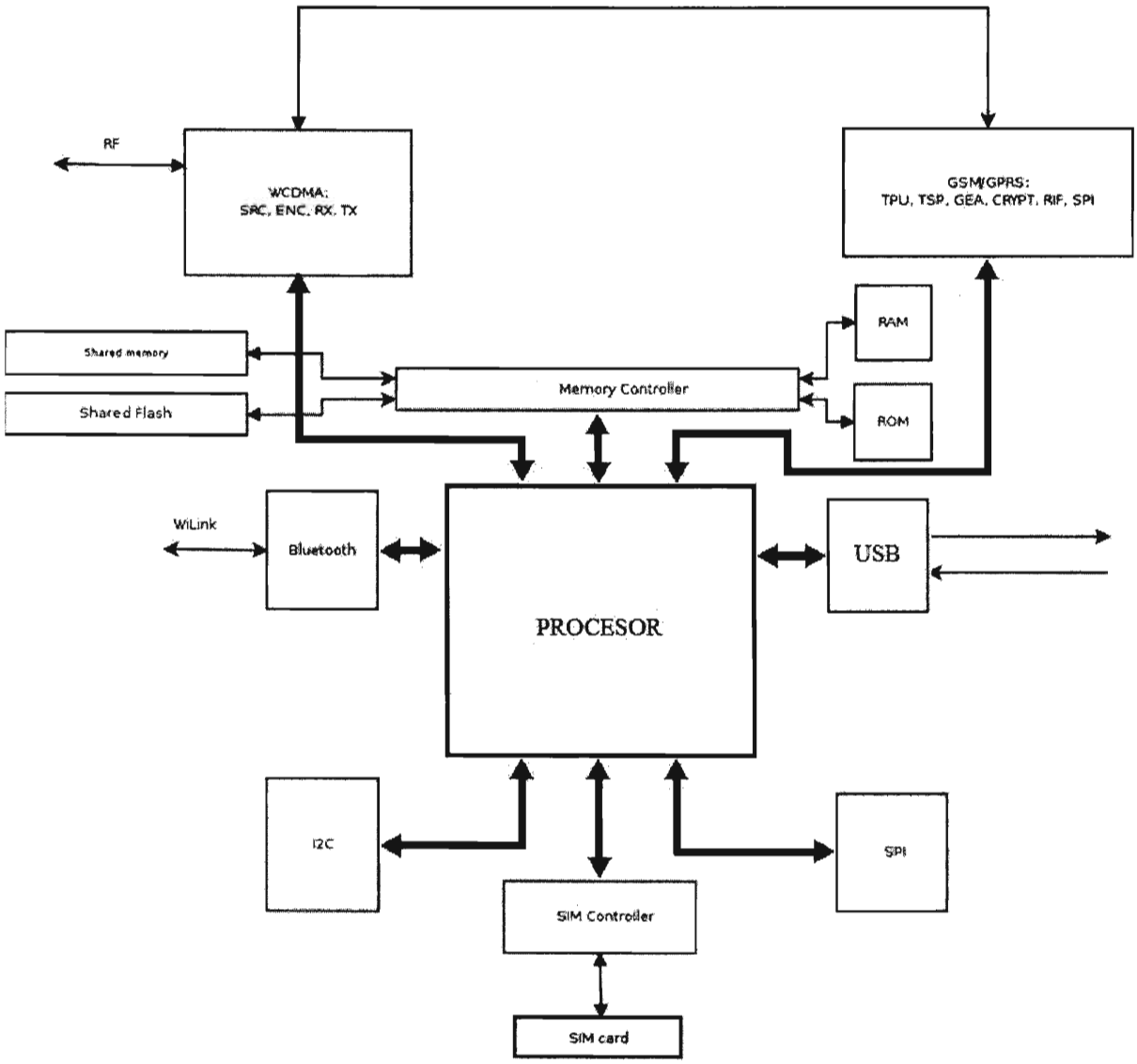

Figura 3 Dispozitivul ce asigură protecția datelor confidențiale