ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 137268 A2**

(51) Int.Cl.
H04L 9/10 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00442**

(22) Data de depozit: **29/07/2021**

(41) Data publicării cererii:
30/01/2023 BOPI nr. **1/2023**

(71) Solicitant:
• **UNIVERSITATEA "ALEXANDRU IOAN CUZA" DIN IAŞI**, *BD. CAROL I NR. 11, IAŞI, IS, RO;*
• **EURO SMART DPO S.R.L.**, *STR.SF.LAZĂR, NR.27, BIROU 111, IAŞI, IS, RO*

(72) Inventatori:
• **SOFRONIE ALEXANDRU**, *ŞOS.TUDOR NECULAI, NR.14, IAŞI, IS, RO;*
• **ALBOAIE LENUŢA**, *STR.PROF.IOAN PETRU CULIANU NR.58, IAŞI, IS, RO;*
• **PANU ANDREI**, *STR.FÂNTÂNILOR NR.59, BL.B4, AP.48, IAŞI, IS, RO*

(54) # TARBUS

(57) **Rezumat:**

Invenţia se referă la un dispozitiv, denumit "Tarbus", destinat securizării comunicaţiilor în reţea sau într-o infrastructură fizică de maşini de calcul conectate sau independente care necesită procesare, stocare sau transfer de date în mod securizat/criptat. Dispozitivul conform invenţiei este format din două componente care funcţionează împreună: o componentă hardware şi o componentă software, în care componenta hardware este alcătuită dintr-un mini-computer Raspberry Pi încapsulat într-o cutie securizată de metal prevăzută cu mijloace de disipare a căldurii emise de placa internă, cu închidere securizată, cu protecţie împotriva apei şi a aerului, cu mijloace de conectare WiFi la o reţea de date şi cu posibilitatea de alimentare cu energie electrică şi dintr-un chipset PROM care conţine un identificator unic Tarbus, o sumă de control folosită la verificarea bootării/rebootării şi o serie de biţi care conţine starea actuală a Tarbus-ului, un astfel de bit putând fi "ars" (setat din 0 în 1) o singură dată, iar componenta software este alcătuită dintr-o alicaţie de bootare/ rebootare şi dintr-o aplicaţie de rulare, în care aplicaţia de bootare/rebootare este un program extern care are rolul de a iniţializa sistemul de operare şi de a crea configuraţia iniţială şi care, odată rulat cu succes, nu mai poate rula încă o dată pentru acelaşi Tarbus, iar aplicaţia de rulare oferă, printr-un server HTTP, servicii de comunicaţii securizate între clienţi, eliminând posibilitatea asumării unei identităţi false sau citirea/ modificarea unui mesaj în tranzit.

Revendicări: 1
Figuri: 2

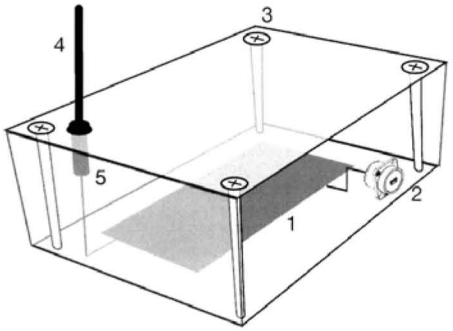

Fig. 1

RO 137269 A2

27

Tarbus

Titlul invenţiei este Tarbus, însemnând: Trust Agent Repository BUS

Domeniul de aplicare al invenţiei este reprezentat de o reţea sau o infrastructură fizică de maşini de calcul conectate sau independente, care necesită procesare, stocare sau transfer de date în mod securizat / criptat.

Toţi algoritmii de criptare bazaţi pe chei (simetrice sau asimetrice) presupun un schimb de informaţii care are loc înainte de stabilirea unui dialog; cu alte cuvinte, doi actori care doresc să comunice securizat fără a se cunoaşte dinainte, trebuie să transmită în mod conceptual nesecurizat o serie de informaţii care să le permită stabilirea unui dialog securizat. Toate soluţiile tehnice cunoscute în acest moment nu rezolvă decât parţial această problemă.

Scopul Tarbus este acela de a pune la dispoziţie o metodă de comunicare securizată chiar de la primul dialog între sisteme software externe, fără posibilitatea asumării unei false identităţi sau citirea / modificarea unui mesaj în tranzit.

Tarbus este format de două componente care funcţionează împreună: o componentă hardware şi o componentă software. Componenta hardware securizată este proiectată pentru a fi uşor instalat şi protejat fizic în acelaşi mod cu un seif tradiţional.

Componenta hardware este reprezentată schematic în **Figura 1** de un mini-computer Raspberrry Pi (fig. 1.1), încapsulat într-o cutie securizată (fig. 1.3) de metal (fig. 1.2). Aceasta este concepută în aşa fel încât să rezolve următoarele probleme:

1. Oferă un mod de disipare a căldurii emisă de placa internă (ex: aluminiu);
2. Oferă un mod de închidere securizat (cifru mecanic, cheie, sudare);
3. Oferă protecţie împotriva apei şi a aerului (fig. 1.5 - separator galvanic);
4. Oferă posibilitatea conectării WiFi la o reţea de date (fig. 1.5).
5. Oferă posibilitatea alimentării cu energie electrică (cu protecţia de la punctul 3) - fig. 1.2.

Astfel, componenta hardware rezolvă o serie de probleme de securitate cum ar accesul fizic asupra echipamentului şi minimizarea accidentelor - stocarea cutiei în aproape orice condiţii. Mai mult, datorită consumului redus de energie, se poate asigura cu uşurinţă continuitatea alimentării prin soluţii ieftine tip UPS.

Tot în cadrul componentei hardware este inclus un chipset PROM (Programmable Read Only Memory) care conţine:

- TUID - Tarbus Unique Identifier - reprezentat de o serie pseudo-aleatorie pe 8192 biţi sau 32 de octeţi care reprezintă un identificator unic pentru fiecare Tarbus; astfel se asigură generarea fără coliziuni a unui număr foarte mare de Tarbus (similar cu generarea UUID V4).

Companie

SOCIETATEA COMERCIALĂ EURO SMART DPO S.R.L. IAŞI - ROMÂNIA J22/871/2018

Rector,
Prof. Dr. Tudorel Toader

ROMÂNIA MINISTERUL EDUCAŢIEI UNIVERSITATEA „ALEXANDRU IOAN CUZA" DIN IAŞI

- OSCHK- Operating System Checksum - reprezentat de o sumă de control folosită la verificarea boot/reboot (32 biţi)
- CFLAGS - o serie de biţi care conţine starea actuală a Tarbus; un astfel de bit poate fi "ars" (setat din 0 în 1) o singură dată:

Componenta software este formată din aplicaţia de boot/reboot şi aplicaţia de rulare, astfel:

Aplicaţia de boot/reboot este reprezentată dintr-un program extern care are rolul de a iniţializa sistemul de operare şi a crea configuraţia iniţială. Odată rulată cu succes, aceasta nu mai poate rula încă odată pentru acelaşi Tarbus. Această aplicaţie rulează în mai multe stadii.

Primul stadiu este cel în care aplicaţia rulează pe o maşină de calcul externă şi realizează o imagine care va fi copiată pe un card de memorie folosit de Raspberry Pi. Imaginea rezultată conţine sistemul de operare, aplicaţia de rulare, valoarea TUID şi o serie de opţiuni cu privire la configuraţiile reţelei wifi.

Al doilea stadiu este rulat pe Tarbus, este prezentat în figura 2 şi are ca efecte următoarele acţiuni, ordonate cronologic:

- Se verifică bit-ul CFLAGS-BOOT; dacă este 1, Tarbus semnalează sonor eroarea şi blochează execuţia; dacă este zero, se continuă procesul;
- se calculează suma de control a imaginii de pe card-ul de memorie (sistemul de operare şi aplicaţia de rulare);
- se compară cu valoarea OSCHK
- dacă valorile nu corespund, acest lucru se semnalează sonor şi Tarbus este blocat; dacă valorile corespund, se continuă procesul;
- Se generează o pereche de chei asimetrice principale şi se stochează pe cardul de memorie;
- Se setează un anumit bit (CFLAGS-BOOT) în CFLAGS.
- Procesul se termină cu succes, Tarbus începe procesul de reboot.

Orice încercare de a rula din nou aplicaţia boot/reboot în stadiul 2 nu va avea niciun efect asupra integrităţii datelor.

La orice reboot, Tarbus verifică bit-ul CFLAGS-BOOT. Dacă acesta nu este setat, Tarbus semnalează sonor şi nu permite continuarea. Dacă este setat, se lansează aplicaţia de rulare.

Aplicaţia de rulare este reprezentată de un server HTTP care oferă servicii clienţilor săi astfel: un client necunoscut până în acel moment doreşte conectarea. Accesul la Tarbus poate fi reglat prin mecanisme specifice de acces în reţea (Firewall, Network Isolation, VPN, etc). Orice client care are acces la Tarbus va putea utiliza serviciile sale. Comunicaţia între client şi Tarbus nu se realizează decât pe un canal de comunicaţie în întregime controlat (reţea locală, VPN).

Noul client trebuie să îşi anunţe identitatea (un UUID pe 32 octeţi) către Tarbus. Tarbus va genera o cheie secretă simetrică care conţine informaţii pe baza cărora Tarbus poate determina atât UUID-ul clientului şi TUID-ul. Această cheie nu părăseşte niciodată mediul Tarbus. Cu ajutorul acestei chei simetrice, se generează o pereche de chei asimetrice, partea privată fiind transmisă către client şi ştearsă din Tarbus.

Companie

Rector,
Prof. Dr. Tudorel Toader

ROMÂNIA MINISTERUL EDUCAŢIEI UNIVERSITATEA ALEXANDRU IOAN CUZA DIN IAŞI

În acest moment, clientul este înregistrat în Tarbus şi poate comunica cu alţi clienţi ale aceluiaşi Tarbus.

Reluarea procesului cu acelaşi UUID rezultă într-o eroare.

Revocarea unui client poate fi cerută de acesta. În acest caz, toate datele referitoare la acel client sunt şterse din Tarbus şi procesul poate fi reluat cu acelaşi UUID. Cheile generate vor avea alte valori.

În orice moment, orice client deja înregistrat în Tarbus poate cere o nouă cheie privată temporară. Atributul temporar se poate referi atât la un interval de timp cât şi la un număr specific de accesări. Cheia privată temporară este generată în mod similar cu cea principală, însă va fi automat ştearsă din Tarbus în momentul în care criteriul temporar este îndeplinit.

Comunicarea cu alţi clienţi Tarbus se realizează în două moduri: pseudo-public sau privat. Dacă comunicarea unei informaţii este intenţionată către mulţi clienţi sau clienţi necunoscuţi la momentul criptării, comunicarea se va realiza în mod pseudo-public, în sensul în care orice client înregistrat în Tarbus poate cere cheia de decriptare (cheia publică) aferentă pentru a decripta mesajul şi a autoriza autorul.

Însă autorul poate opta pentru o cheie temporară unde poate specifica UUID-urile clienţilor care pot decripta informaţia, pe lângă criteriul temporar al acesteia. Astfel, chiar dacă informaţia criptată este interceptată de alţi actori, chiar dacă sunt înregistraţi în acelaşi Tarbus, aceştia nu vor putea obţine cheia de decriptare din Tarbus.

Astfel, destinatarul va cere de la Tarbus cheia de decriptare pentru mesajul criptat pe care l-a primit. Tarbus poate răspunde cu cheia publică aferentă sau nu, în funcţie de caracteristicile cheii private folosite la criptarea mesajului.

În anumite cazuri speciale, Tarbus poate fi folosit şi pentru criptarea şi decriptarea mesajelor trimise/primite; aceste cazuri se referă la clienţi care nu pot stoca în mod securizat cheia privată. În acest caz, amândouă cheile sunt stocate în Tarbus (cheia privată nu este ştearsă la momentul generării). Acest lucru este aplicabil şi pentru cheile temporare. Având în vedere că orice comunicaţie între Tarbus şi client este protejată, autorul poate cere Tarbus-ului criptarea mesajului iar destinatarul poate cere decriptarea acestuia, nici unul din aceste procese neavând loc pe calculatorul autorului sau a destinatarului mesajului. Tranzitul informaţiei de la autor la destinatar va conţine astfel un mesaj criptat.

Un client poate de asemenea stoca în Tarbus informaţii criptate cu ajutorul cheii sale private. În orice moment, clientul poate da sau revoca accesul la datele sale pentru alţi clienţi.

Atât generarea cât şi managementul cheilor publice şi private sunt preluate de componenta OpenDSU / PrivateSky. Folosirea Smart Contracts este componenta cheie în asigurarea securităţii software pentru Tarbus.

Fiecare cerere / revocare de chei pentru transmiterea criptată a clienţilor este direct ancorată cu ajutorul sistemul Anchoring Service în Ledger-ul distribuit. Fiecare client dintr-un Tarbus este reprezentat de un agent în sistemul OpenDSU.

Mai mult, se poate realiza un Distributed Ledger între diferite entităţi Tarbus, putând astfel interconecta mai multe reţele securizate. Această funcţionalitate poate fi extinsă fără limite, rezolvarea diferitelor Tarbus-uri interconectate cu un protocol bazat pe self certifying

Companie

Rector,
Prof. Dr. Tudorel Toader

DID (Decentralised Identifiers), având în loc de domenii de nume, domenii de chei ce se auto validează cryptographic.

Datorită sumelor de control, software-ul conţinut de Tarbus este garantat identic. Punerea la dispoziţie în mod Open Source a tuturor codurilor sursă permite oricărei părţi interesate să verifice integritatea algoritmilor folosiţi şi calculul şi verificarea independentă (prin propriile metode) ale sumelor de control şi a funcţionării Tarbus.

Securizarea fizică a dispozitivului permite atât izolarea responsabilităţii cât şi garantarea integrităţii acestuia pe parcursul funcţionării. Prin mecanisme simple tip VPN se pot crea structuri de schimb de informaţii complexe şi securizate, inclusiv structuri de tip arbore.

Vom prezenta un prim exemplu care include mai multe use-case-uri în care Tarbus aduce avantajele descrise în document.

Se dau două reţele A şi B distincte, fiecare având instalat câte un Tarbus. Reţeaua A este guvernată de un server având aplicaţia SmartDPO pentru o singură organizaţie, având un Ofiţer DPO Extern, mai mulţi DPO Interni şi utilizatori. Reţeaua B este guvernată de un server SmartDPO care are mai multe organizaţii, unele dintre ele având Ofiţer DPO Intern şi toate având acelaşi DPO Extern.

Ofiţerul DPO extern A începe lucrul la un nou şablon în reţeaua A. Pe parcursul dezvoltării şablonului, ofiţerul DPO A sesizează o greşeală şi doreşte refacerea stării şablonului cu câteva iteraţii în urmă. Acest lucru este realizat facil, pentru că la fiecare modificare, conţinutul şablonului este salvat (notarizat) cu ajutorul Tarbus, astfel încât recuperarea unei versiuni anterioare este nu numai facilă ci are şi garanţia integrităţii datelor.

Un ofiţer DPO intern A foloseşte şablonul pus la dispoziţie de ofiţerul DPO extern A pentru a crea un document în organizaţia A. Acest document la rândul său este salvat în mod criptat la fiecare modificare. Astfel, atât ofiţerul DPO Extern A cât şi cel intern A pot urmări evoluţia documentului (gradul de completare, modificările aduse la fiecare pas, timpii şi utilizatorii care au realizat fiecare modificare).

Ofiţerul DPO Extern A decide că şablonul creat este necesar şi în reţeaua B. Fără Tarbus, transmiterea şablonului între cele două reţele în mod total securizat ar fi imposibilă fără o configuraţie prealabilă. Însă Tarbus poate iniţia această conexiune atât dintr-un sens cât şi din cel invers: ofiţerul DPO Extern A poate oferi şablonul către ofiţerul DPO extern B sau, în sens invers, ofiţerul DPO extern B poate cere şablonul ofiţerului DPO extern A. În ambele cazuri, cele două Tarbus-uri pot iniţia conexiunea şi asigura transportul datelor în mod securizat între cele două reţele.

La nivelul reţelei B, ofiţerul DPO extern alege să pună la dispoziţie în mod selectiv şablonul primit. Astfel, numai organizaţiile selectate vor putea avea acces la şablon, acest lucru rezultând în urma selectării destinatarilor (organizaţiilor), numai cei selectaţi având cheile de decriptare a şablonului.

La un moment următor, ofiţerul DPO extern A realizează modificări asupra şablonului şi înştiinţează ofiţerul DPO extern B de modificarea conţinutului şablonului. Ofiţerul DPO extern B alege aducerea la zi a conţinutului şablonului. Astfel, sistemul are la dispoziţie nu

Companie

Rector,
Prof. Dr. Tudorel Toader

ROMÂNIA
MINISTERUL EDUCAŢIEI
UNIVERSITATEA „ALEXANDRU IOAN CUZA" DIN IAŞI

numai garanţia integrităţii datelor şi transmiterea acestora securizat, ci şi un puternic sistem criptat de versionare, securizat din punct de vedere al accesului.

Technologia OpenDSU / Tarbus este folosită nu numai în cazul comunicării între diferite organizaţii. Astfel, un client al organizaţiei A face o cerere prin care doreşte, conform GDPR, să i se şteargă toate datele personale din sistem. Conform legii, datele trebuie şterse sau anonimizate într-un mod în care nu se pot recupera datele originale. Cu ajutorul Tarbus, ştergerea cheilor folosite la decriptarea informaţiilor despre acel client atrage după sine imposibilitatea citirii acelor date, cu toate că acestea rămân stocate în sistem, putând fi folosite în continuare doar ca date statistice: chiar dacă identitatea şi detaliile personale ale clientului sunt în continuare inaccesibile, pot fi extrase informaţii cu privire la activitatea clientului (de exemplu numărul de intrări/ieşiri, date şi agregări de date financiare, numărul de contracte încheiate, etc).

Un al doilea exemplu, mai generic, este prezentat cu ajutorul unei instituţii (Spital) care interacţionează atât cu populaţia (Pacienţi) cât şi cu alte instituţii (Evidenţa Populaţiei, Poliţie). Toate instituţiile au acces la un Tarbus Privat.

Spitalul mai are instalat un Tarbus care este expus public către Internet. Orice pacient poate să se identifice în Tarbus Public al Spitalului şi să obţină o cheie privată. Pacientul poate aşadar să stocheze în Tarbus Public al Spitalului dosarul său şi să dea acces către diferite departamente la dosarul său. Comunicarea între Pacient şi Spital este în întregime securizată, atât Pacientul cât şi Spitalul având garanţia identităţii celuilalt.

Pacientul este internat în Spital şi se determină faptul că acesta a trecut printr-un proces care trebuie anunţat la Poliţie. Folosit Tarbus Privat, informaţiile relevante sunt transmise către Poliţie, care foloseşte informaţiile pentru a demara o anchetă. După un anumit timp de la internare, Pacientul decedează. Spitalul va adăuga în dosar informaţiile relevante. Datele statistice sunt extrase şi Spitalul nu mai necesită acces la dosarul Pacientului. Datele rămân însă în Tarbus Public, însă un nou timp de acces (un alt client care să aibă acces la date) nu mai este posibil. La închiderea dosarului, însă, Spitalul trimite cu ajutorul Tarbus-ului privat informaţia despre deces către Evidenţa Populaţiei. Datele Pacientului pot rămâne aşadar în cadrul Evidenţei Populaţiei, această instituţie devenind, practic deţinătorul informaţiei.

Companie

Rector
Prof. Dr. Tudorel Toader

22

REVENDICĂRI

1. Metodă de comunicare securizată, **caracterizat prin aceea că:**
   - protejează comunicarea chiar de la iniţiere (primul dialog) şi astfel nu există posibilitatea asumării unei false identităţi sau citirea / modificarea unui mesaj în tranzit.
   - existenţa unui dispozitiv hardware securizat ce poate fi uşor instalat şi protejat în acelaşi mod cu un seif tradiţional

Companie

Rector
Prof. Dr. Tudorel Toader

21

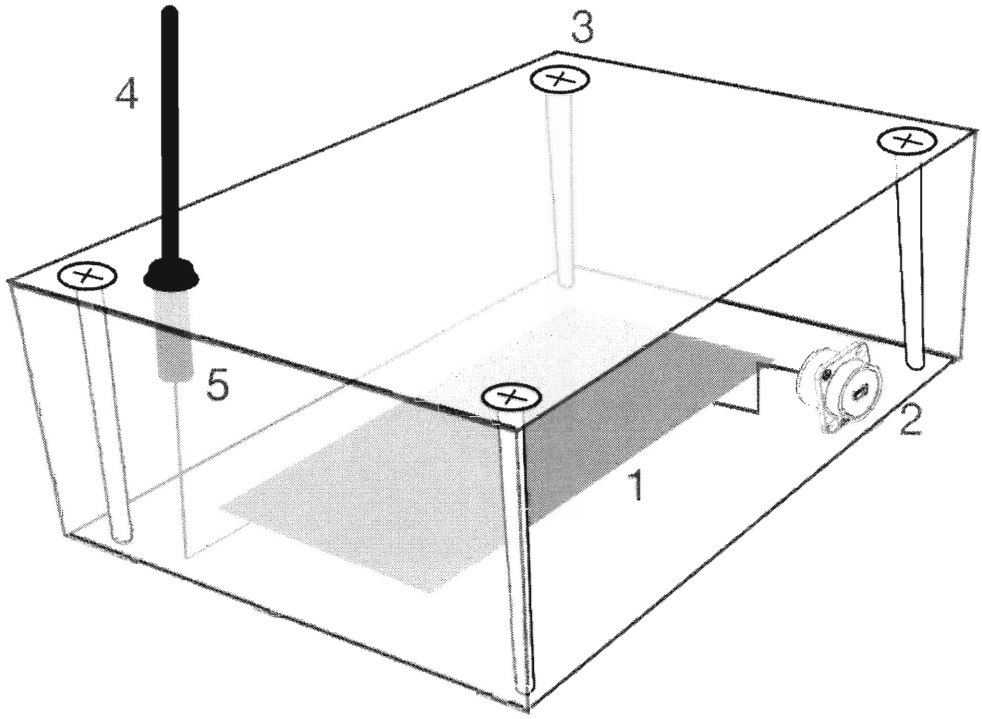

Figura. 1. Prezentare schematică hardware

1 - placă Raspberry PI; 2 - conector MiniUSB de alimentare cu energie electrică; 3- şuruburi sudate sau sigilate, cutie metal (aluminiu) pentru disiparea căldurii; 4 - antenă Wireless; 5 - separator (izolator) galvanic antenă;

Companie

Rector,
Prof. Dr. Tudorel Toader

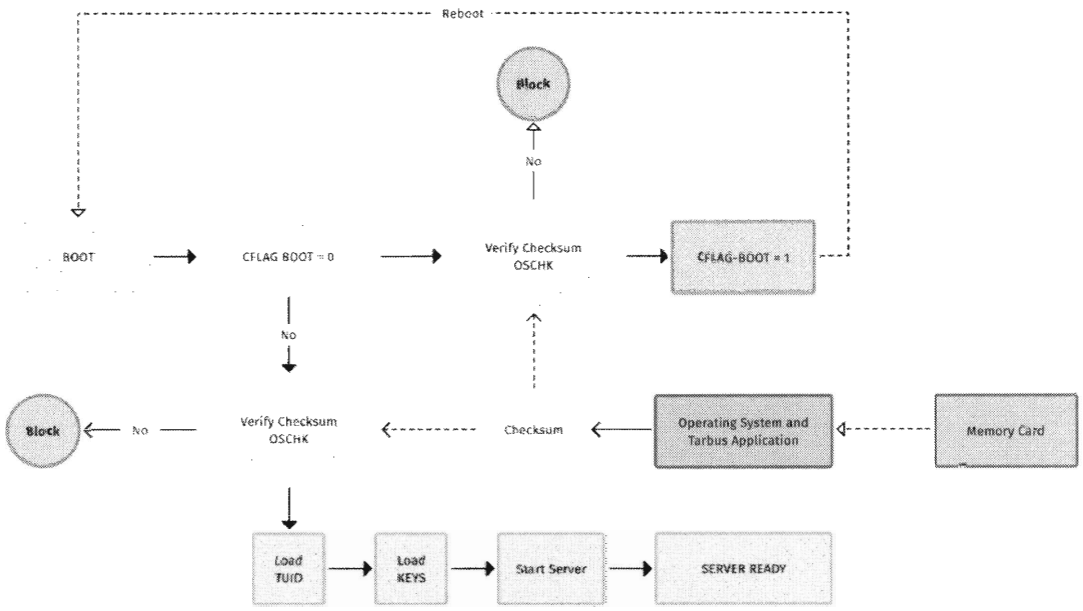

Figura 2. Procesul de boot și verificarea integrității datelor

Galben: *inițierea procesului de Boot*;
Roșu: *semnalizare sonoră (beeps) și blocare execuție*;
Verde: *proces normal de inițializare și rulare*;
Albastru: *setare ("ardere") PROM*;
Violet: *date introduse de pe suport extern pe MemoryCard*;
Romb Gri: *decizie*; Oval gri: *calculare Checksum (SHA256)*.

Companie

Rector,
Prof. Dr. Tudorel Toader