(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 135951 A2**

(51) Int.Cl.
G06F 21/31 (2013.01);
G06F 21/60 (2013.01);
H04L 9/08 (2006.01);
H04L 9/32 (2006.01);
H04W 12/04 (2009.01);
H04W 12/06 (2009.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00047**

(22) Data de depozit: **12/02/2021**

(41) Data publicării cererii:
30/08/2022 BOPI nr. **8/2022**

(71) Solicitant:
• **UNIVERSITATEA "ALEXANDRU IOAN CUZA" DIN IAŞI**, *BD. CAROL I NR. 11, IAŞI, IS, RO;*
• **ROMSOFT S.R.L.**, *BD.CHIMIEI NR.2 BIS, IAŞI, IS, RO*

(72) Inventatori:
• **MAŞTALERU RAFAEL**, *STR.LUNGA, NR.87, HOLBOCA, IS, RO;*
• **ALBOAIE LENUŢA**, *STR.PROF.IOAN PETRU CULIANU NR.58, IAŞI, IS, RO;*
• **ALBOAIE SÎNICĂ**, *STR.COSTACHE NEGRII NR.39, BL.Z2, AP.36, IAŞI, IS, RO*

(54) # SISTEM DE GESTIUNE AL CHEILOR PRIVATE FORMAT DIN DISPOZITIV DE AUTENTIFICARE ŞI MANAGEMENT CHEI INTEGRAT CU APLICAŢIE DESCENTRALIZATĂ DE TIP SELF SOVEREIGN CLOUD SAFE BOX ENTERPRISE

(57) **Rezumat:**

Invenţia se referă la un sistem informatic de gestiune a cheilor private format dintr-un dispozitiv de autentificare şi management al cheilor integrat cu o aplicaţie descentralizată de tip "self sovereign" care asigură siguranţa şi protecţia datelor confidenţiale. Aplicaţia de tip "self sovereign", conform invenţiei, permite stocarea criptată a informaţiilor secrete offline, în cloud, în timp ce cheile private de acces şi gestiune a informaţiilor sunt stocate offline pe un dispozitiv hardware asemănător unui portofel hardware de criptomonede ce permite autorizarea diferitelor tipuri de tranzacţii.

Revendicări: 1
Figuri: 21

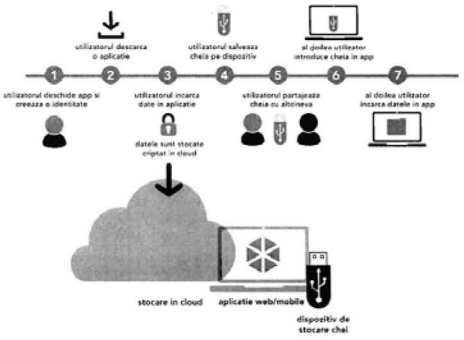

Fig. 1

RO 135951 A2

RO 135951 A2

Sistem de gestiune al cheilor private format din dispozitiv de autentificare şi management chei integrat cu aplicaţie descentralizată de tip s*elf sovereign* Cloud Safe Box Enterprise

Invenţia se referă la un sistem integrat format din aplicaţie *self sovereign* şi dispozitiv de autentificare şi management chei pentru asigurarea securităţii şi protecţia datelor în vederea gestionării şi partajării lor în condiţiile respectării GDPR şi a altor reglementări prin managementul cheilor private, domeniu prioritar de cercetare.

În ultimii ani, dezvoltarea monedelor virtuale a generat dezvoltarea portofelelor prin care utilizatorii pot accesa şi gestiona tranzacţiile cu monede virtuale în platforme de schimb online. Sunt două tipuri de portofele, hardware sau software, care oferă posibilitatea de a stoca şi utiliza monedele virtuale în siguranţă.

Portofelele hardware sunt dispozitive fizice asemănătoare unei unităţi externe care sunt separate de platformele de schimb online şi conţin chei private cu ajutorul cărora pot fi accesate platformele online de schimb valutar. Acestea necesită conectarea la un computer sau dispozitiv online pentru a putea accesa moneda digitală. Siguranţa stocării cheii vine din faptul că cheia privată este stocată pe dispozitivul portofel hardware la care doar utilizatorul are acces şi nu pe serverele online supuse riscurilor cibernetice.

Dezavantajul portofelelor hardware constă în gradul redus de accesibilitate, mai ales în comparaţie cu portofelele software sau de schimb valutar. În cazul în care computerul este supus unui atac cibernetic sau portofelul este pierdut/ furat, nimeni nu îl poate accesa şi transfera monedele fără să vă cunoască cheia privată de acces stocată în portofelul hardware. Pe piaţă există zeci de portofele hardware pentru monede virtuale. Ledger Nano S, este un dispozitiv fără baterii care foloseşte o interfaţă OLED pentru a interacţiona cu utilizatorul, oferind o navigaţie simplă şi un aspect elegant pentru Bitcoin.

TREZOR şi KeepKey, sunt, de asemenea, opţiuni viabile pentru portofelele hardware, ambele oferind securitate completă şi accesibilitate la fel ca orice alt portofel hardware.

Pe măsură ce lumea criptografiei evoluează, apar inovaţii în domeniul stocării cheilor private, cum ar fi cea implementată de Mandala Exchange, care permite utilizatorilor să stocheze şi să securizeze offline nu doar chei private dar şi alte informaţii utile cum ar fi parole şi chiar monede virtuale.

Portofelele software sunt mult mai accesibile şi mai convenabile pentru utilizatori de a schimba şi trimite monede întrucât sunt programe non-fizice descărcate pe computer care permit accesarea monedelor virtuale printr-o parolă.

Companie ROMSOFT SRL J22/1183/2001 IAŞI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

Dezavantajul acestor portofele este că, fiind conectate la internet, rămân susceptibile la orice malware sau virus online. Orice frază de recuperare sau parolă care poate fi vizibilă pe ecran poate fi văzută și înregistrată de un hacker.

Un alt dezavantaj atât la portofelele software cât și cele hardware este că pot fi concepute special pentru anumite monede și nu sunt adaptabile pentru alte tipuri de chei private.

Copay este un portofel software gratuit disponibil doar pentru Bitcoin, spre exemplu, în timp ce Exodus este un portofel gratuit pentru a stoca majoritatea monedelor. Pentru mai multă siguranță există și combinații de hardware și software cum ar fi Electrum care este compatibil cu portofelele hardware Ledger și Trezor.

Cererea de brevet se referă la o metodă de stocare și gestiune a cheilor private, cu ajutorul căreia pot fi protejate datele private și alte informații confidențiale (secrete, parole) împotriva încercărilor de acces neautorizat în momentul stocării lor pe diverse platforme informatice.

Conform noilor reglementări GDPR (Legea 190/2018 privitor la protecția datelor cu caracter personal), date private nu pot fi accesate fără acordul explicit al aparținătorilor.

Pe de alta parte, sunt situații în care există nevoia de partajare a datelor private cu diverși actori în beneficiul aparținătorului de date. Spre exemplu, în cazul datelor medicale, există necesitatea ca un doctor sa poată accesa la un moment dat cat mai multe informații din istoricul medical al pacientului în scopul stabilirii unui diagnostic cât mai corect.

Cele două cerințe sunt contradictorii în sensul ca un medic nu poate accesa istoricul medical al pacientului fără a avea un acord prealabil al acestuia. Chiar dacă pacientul și-a dat acordul unui medic, acel medic nu are voie să trimită datele unui alt medic deoarece încalcă drepturile pacientului.

În realitate însă, pacientul vizitează mai mulți medici pentru tratarea unei afecțiuni. Pacientul poate fi trimis la mai multe spitale și analizele făcute la o clinică nu sunt disponibile la alta clinică. În acest fel, unele analize pot fi repetate și se pierde o mulțime de timp cu completarea și semnarea documentelor de protecție a datelor.

Situații similare cu exemplul expus se regăsesc într-o gama largă de partajare a datelor private, secretelor, unde partajarea în sine atrage și riscul accesului neautorizat.

Soluția implementată în cadrul proiectului PrivateSky și propusă spre brevetare este un sistem informatic unic de stocare a cheilor private care poate fi accesat simplu de aparținătorii de date și persoanele cu care se dorește partajarea datelor secrete, oricând și oriunde, obținând acordul apartinatorului prin metoda partajarii unor chei de acces stocate

Companie

SOCIETATEA COMERCIALĂ C.I.F. R 2760 ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

offline într-un portofel hardware. Sistemul conține așadar o aplicație *wallet* descentralizată care permite generarea și managementul cheilor private pentru diferite tipuri de informații secrete și un dispozitiv hardware de stocare a cheilor private care permit accesarea și gestionarea secretelor.

Realizarea unor platforme unice pentru managementul datelor private reprezintă o problema actuala, pentru care se cauta solutii de implementate ce includ o serie de avantaje și dezavantaje.

Majoritatea soluțiilor sunt nișate pe anumite direcții și nu oferă o soluție generală customizabilă pe nevoia utilizatorului de date secrete.

Revenind la exemplul datelor medicale, există:

- Aplicații de tip *cloud* dezvoltate de marile firme de software ce oferă spații de stocare și aplicații de management al datelor medicale:
    - HealthVault dezvoltat de firma Microsoft, (https://international.healthvault.com/ro/en)
    - Apple Health (https://www.apple.com/ios/health)

Avantaje: sunt aplicații *free*, extrem de flexibile, acceptă dezvoltări ulterioare ale utilizatorilor.
Dezavantaje: sunt orientate pe pacient, este un spațiu de stocare privat și este anevoios pentru doctor să acceseze datele respective.

- Aplicații particularizate de interconectare a bazelor de date medicale: sunt soluții specifice de interconectare, ce oferă posibilitatea transferului automat al datelor medicale. Un exemplu este sistemul Vitalink din Olanda (http://www.ncbi.nlm.nih.gov/pubmed/24804390)

Dezavantaje: sistemele studiate nu oferă o reală protecție a datelor medicale, în principiu se bazează pe un „cerc de încredere" creat între medicii ce utilizează sistemul. Dacă un medic cu drepturi depline în sistem vrea să acceseze și să folosească în mod fraudulos datele medicale din sistem, nu există o barieră reală care să-l împiedice.

Problema pe care o rezolva metoda propusă pentru brevetare se referă la procesul de gestiune a cheilor private în vederea stocării și partajării diferitelor tipuri de date secrete, inclusiv date private, oferind siguranța drepturilor depline aparținătorilor. Aplicația de tip *self sovereign* permite stocarea criptată a informațiilor secrete offline, în *cloud*, în timp ce cheile private de acces și gestiune a informațiilor sunt stocate offline pe un dispozitiv hardware asemănător unui portofel hardware de criptomonede ce permite autorizarea diferitor tipuri de tranzacții.

Invenția prezintă următoarele avantaje:

Companie ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector
Prof. Dr. Tudorel Toader

- Aplicabilitate extinsă: Sistemul de gestionare chei private poate fi folosit pentru o serie de informaţii secrete, parole, chei private şi nu doar monede virtuale. Aplicaţia Cloud Safe Box Enterprise poate fi customizată pentru diferite tipuri de informaţii secrete.
- accesibilitate: orice secret poate fi uşor accesat şi gestionat de oriunde prin intermediul aplicaţiei şi a portofelului.
- Partajare rapidă a datelor între utilizatori. Viteza se datorează faptului că numai cheia trebuie împărtăşită, nu întregul conţinut. Procesul de partajare a informaţiilor secrete (date private) în condiţii de siguranţă este mult mai rapid şi eficient. Acordul accesului la date private conform GDPR se poate face mai rapid, şi în acest fel, nu se mai pierde timp cu citire şi semnare de acorduri la fiecare acord.
- Securitate sporită: prin metoda clasică în care un individ semnează un acord urmând ca interlocutorii să respecte acordul, persoana în cauză nu are niciun control asupra accesării de către diverse persoane a datelor sale. Prin noua metodă, orice acces se face doar prin cheia privată, deci un individ are un control riguros referitor la persoanele care accesează secretele/ datele private.
- Control riguros al persoanelor care au acces la datele secrete proprii: individul poate analiza oricând în aplicaţie persoanele cu care partajează un secret şi poate invalida orice acces pe care îl consideră depăşit sau inoportun.

Dezavantaje:

- Noua metoda presupune că individul are atât un device cu acces online pe care să descarce aplicaţia descentralizată de tip *self sovereign* (web/ mobile) cât şi dispozitivul hardware extern de gestionare a cheilor private. Fără aplicaţia descentralizată de tip *self sovereign* nu poate gestiona secretele.

Prin aplicaţie şi dispozitivul de gestiune chei private, datele pot fi reîncărcate oricând în browser-ul oricărui utilizator care are acces la acele date. În acest fel, aparţinătorul poate partaja datele conştient, evitând riscul accesului neautorizat.

Descriere metodei: etapele procesului de stocare a datelor secrete şi partajarea accesului la acestea este următorul (Fig. 0):

- Utilizatorul îşi creează o identitate prin intermediul aplicaţiei de tip *wallet*, unde îşi poate introduce diferite tipuri de date secrete pe categorii prin intermediul unor aplicaţii *self sovereign* (Fig. 1, Fig. 2)
- Datele sunt stocate în *cloud* (Fig. 0)).

Companie SOCIETATEA COMERCIALĂ C.I.F. RO 14362760 ROMSOFT SRL J22/1183/2001 IAŞI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

- Cheile private de acces la datele secrete sunt stocate pe dispozitivul de gestiune chei private (Fig. 0)
- Datele stocate sunt criptate şi pot fi partajate cu alţi utilizatorii prin acordarea accesului, printr-o cheie privată. (Fig. 0)
- Utilizatorul care are acces la date poate introduce în aplicaţia sa cheia primită şi accesează în acest fel datele private partajate de un alt utilizator. (Fig. 0)
- Dacă aparţinătorul a dat acces doar unui singur utilizator, doar acel utilizator poate accesa datele
- Sistemul construieşte două tipuri de chei private de acces: cheie de citire a informaţiei fără drept de modificare şi cheia cu drept de modificare a informaţiei.

Dispozitivul de gestionare a cheilor private funcţionează asemeni unui portofel hardware de criptomonede care stochează cheile private utilizate pentru autorizarea tranzacţiilor în reţeaua blockchain. Principiul de baza este de a separa complet cheile private de orice dispozitiv care poate fi hackuit. Accesarea datelor se face online prin aplicaţie.

Soluţia propusă are la bază un sistem de fişiere distribuit dezvoltat în cadrul proiectului PrivateSky. Spre deosebire de alte sisteme de fişiere distribuite bazate pe reţea (de ex. NFS, GFS, HDFS, etc), partea serverului este restricţionată la un simplu serviciu *cloud*. Informaţiile sunt întotdeauna criptate atunci când sunt stocate. Sistemul de fişiere este disponibil numai pentru entităţile care au acces la o cheie secretă. Fiecare utilizator va avea o viziune diferită asupra sistemului de fişiere în funcţie de permisiunile sale particulare (acces la cheile private potrivite)

Fişierele sunt încărcate în JavaScript sandboxes în mediile corespunzătoare (servere, dispozitive de bord etc.) care pot fi asimilate sub conceptul de portofele digitale.

Conţinutul fişierelor este împărţit în secţiuni, criptate şi stocate în serviciile de stocare compatibile. Fiecare secţiune este criptată cu o cheie separată, salvate offline pe un dispozitiv de autentificare şi gestiune chei. Stocarea asigură că doar proprietarii informaţiei controlează şi pot accesa informaţiile stocate. Nu va fie nevoie de a avea încredere într-un provider central. Datele se pot partaja cu familia, prietenii, colegii, angajatorul, etc.

Descrierea aplicaţiei Cloud Safe Box Enterprise - Interfaţa utilizatorului

La instalarea aplicaţiei CSB Enterprise, se crează un marketplace implicit ce conţine o serie de aplicaţii preinstalate disponibile în cadrul „My applications", accesibilă din meniul din stânga al aplicaţiei. Figurile: 1 „Pagina My Applications - vizualizare listă" şi 2 „Pagina My Applications - vizualizare grilă" arată design-ul implementat pentru această pagină.

Companie SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAŞI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

În partea stângă a paginii „My applications", avem un câmp de căutare pentru aplicații. Cuvintele cheie scrise în acest câmp sunt căutate în numele aplicației dar și în descrierea acesteia. Un exemplu este în Figura 3 „Vizualizare elemente ce conțin cuvântul cheie scris în câmpul de căutare".

Lista de marketplace-uri este disponibilă din meniul din stânga al aplicației. În cadrul acesteia, utilizatorul are posibilitatea de a adăuga alte marketplace-uri folosind butonul plus din dreapta sus, cum este prezentat în figurile 5 și 6. De asemenea, acesta poate șterge din marketplace-uri folosind butonul „Delete" disponibil pentru fiecare marketplace în parte. În această pagină, tipul de vizualizare a marketplace-urilor este la fel ca și în cazul aplicațiilor instalate, în format listă sau grilă, vizualizare ce poate fi schimbată folosind butonul din dreapta sus, de la începutul listei de marketplace-uri.

La crearea unui nou marketplace, inițial, acesta este gol, urmând ca utilizatorii ce împărtășesc acest marketplace, să adauge aplicații în cadrul acestuia. Fiecare aplicație nou adăugată trebuie întâi validată de către un utilizator cu rol de administrator care poate accepta sau respinge adăugarea unei noi aplicații.

Butonul „Plus" din dreapta sus va deschide un meniu cu următoarele opțiuni:

- Submit application - deschide un formular de adăugare a unei noi aplicații cu date minimale inițiale, nume, descriere, o imagine și keySSI-ul aplicației;
- Share marketplace - va deschide un modal cu un QR Code generat cu ajutorul căruia se poate partaja marketplace-ul. Acest QR Code conține informațiile marketplace-ului.
- Manage applications - doar pentru utilizatorii cu drept de admin - va deschide pagina de management a aplicațiilor în așteptarea unei validări.

Tipurile de vizualizare sunt aceleași ca și în pagina My Applications, listă și grilă.

Administratorii marketplace-ului vor avea afișate aplicațiile care sunt în așteptarea validării. Pentru fiecare aplicație, două butoane sunt disponibile, „Accept" și „Deny". La apăsarea acestor butoane, un mesaj de confirmare este afișat.

După ce aplicațiile au fost acceptate, acestea sunt disponibile în marketplace spre a fi instalate de utilizatorii ce doresc utilizarea acesteia.

Figurile 15, 16, 17, 18, 19 și 20 prezintă aplicațiile preinstalate în cadrul CSB Enterprise în forma lor inițială.

Companie SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

REVENDICĂRI

1. Sistem informatic de gestiune al cheilor private format din dispozitiv de autentificare şi management chei integrat cu aplicaţie descentralizată de tip *self sovereign* Cloud Safe Box Enterprise, **caracterizat prin aceea că:** asigură siguranţa şi protecţia datelor confidenţiale conform condiţiilor GDPR şi altor reglementări de securitate a datelor în procesul de gestiune şi partajare a datelor secrete de orice fel prin folosirea aplicaţiilor descentralizate de tip *self sovereign* şi a portofelelor hardware externe.

Companie

Rector,
Prof. Dr. Tudorel Toader

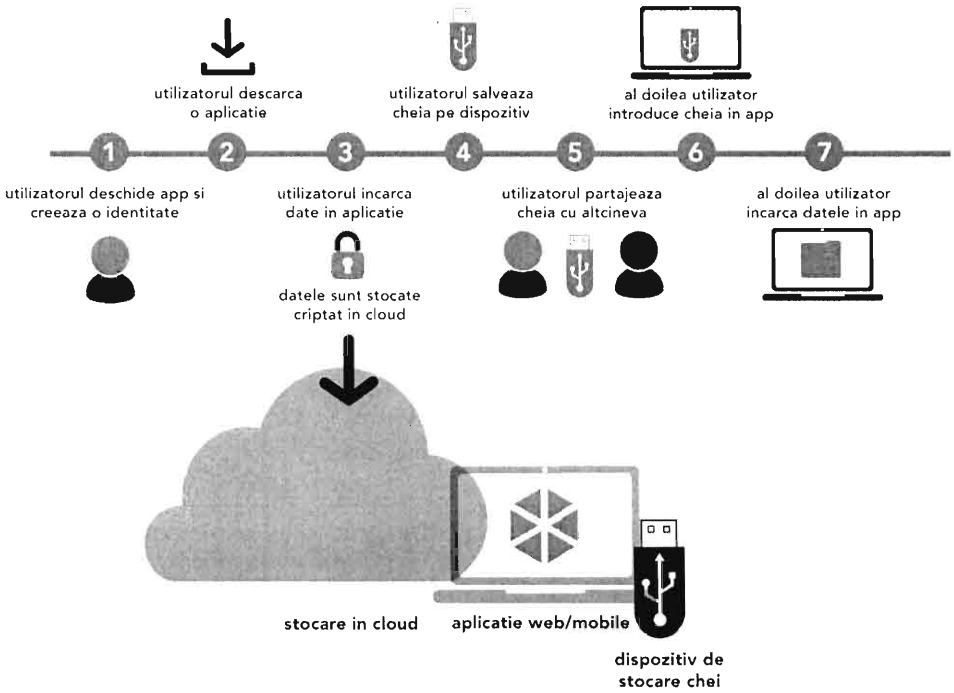

Figura 0: Etapele procesului de stocare a datelor secrete și partajarea accesului la acestea

Figura 1 Pagina My Applications - tip vizualizare listă

Companie

SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

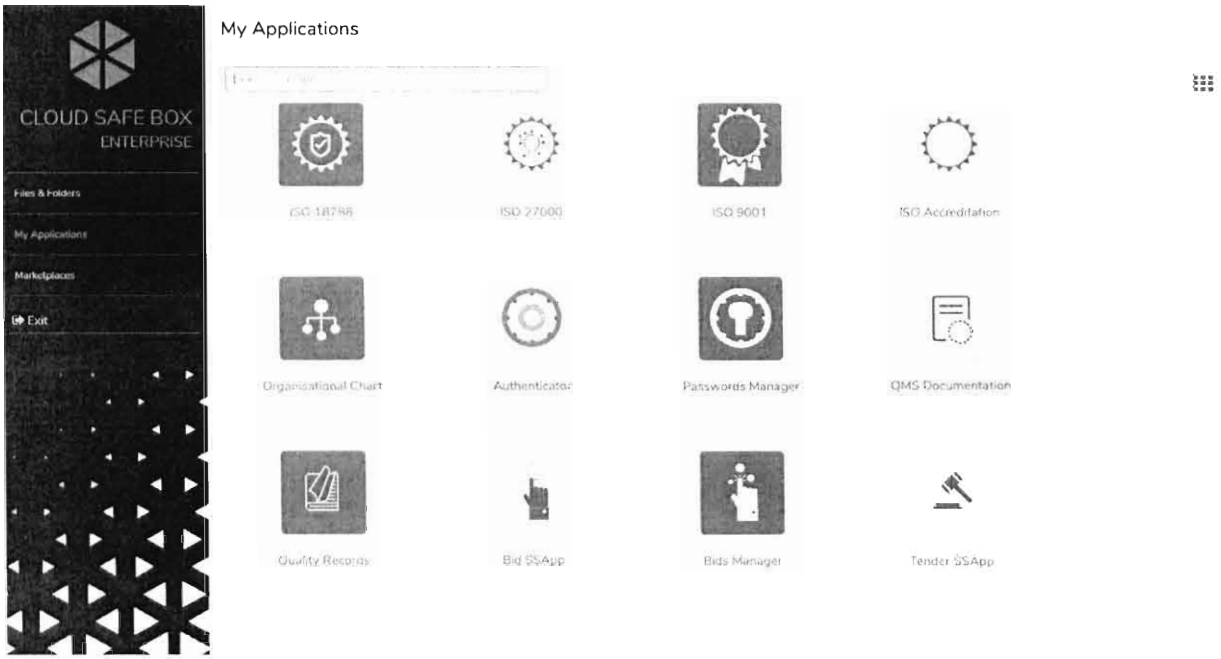

Figura 2 Pagina My Applications - tip vizualizare grilă

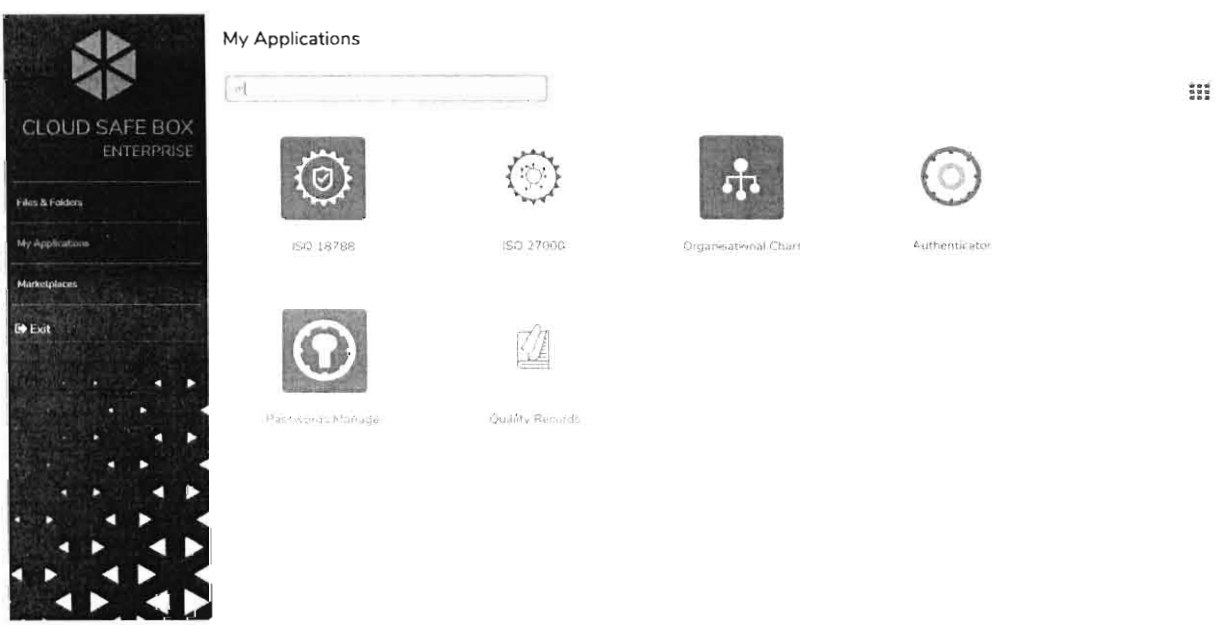

Figura 3 Vizualizare elemente ce conțin cuvântul cheie scris în câmpul pentru căutare

Companie

SOCIETATEA COMERCIALĂ ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA C.I.F. RO 14362760

Rector,
Prof. Dr. Tudorel Toader

Figura 4 Pagina Marketplace Manager în stadiul inițial al aplicației - tip vizualizare listă

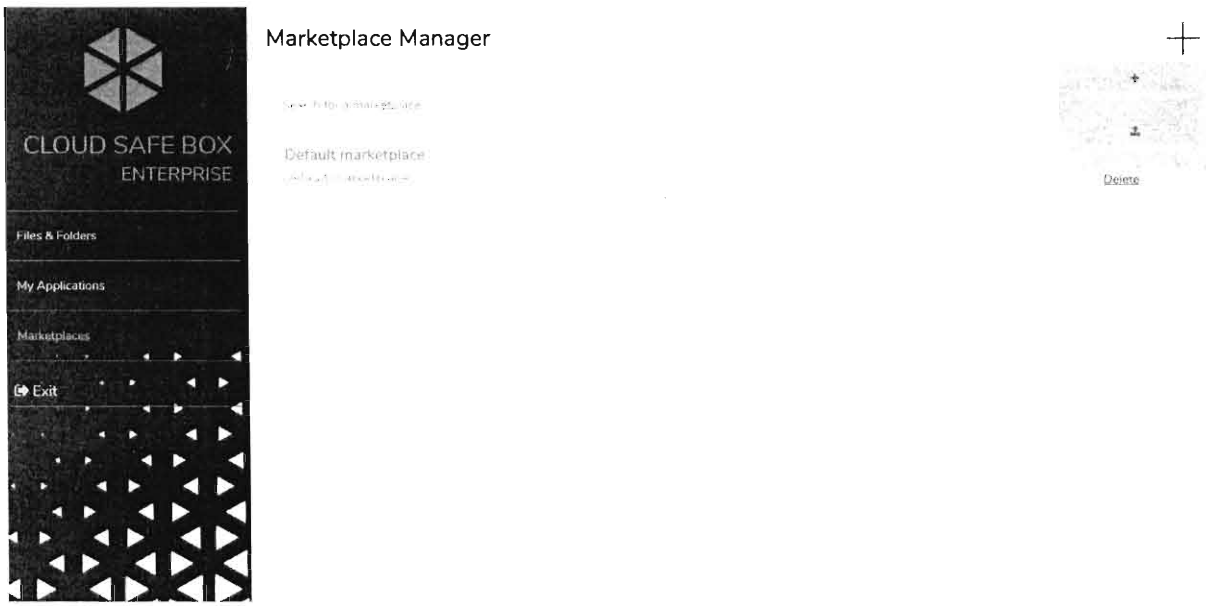

Figura 5 Pagina Marketplace Manager - meniul de adăugare este deschis; opțiunile de adăugare sunt: 1. Submit Marketplace, opțiune ce crează un marketplace nou; 2. Import marketplace, opțiune ce crează un marketplace pe baza de keySSI.

Companie

SOCIETATEA COMERCIALĂ ROMSOFT SRL C.I.F. RO14362760 J22/1183/2001 IAȘI, ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

Figura 6 Formularul de adăugare a unui marketplace nou.

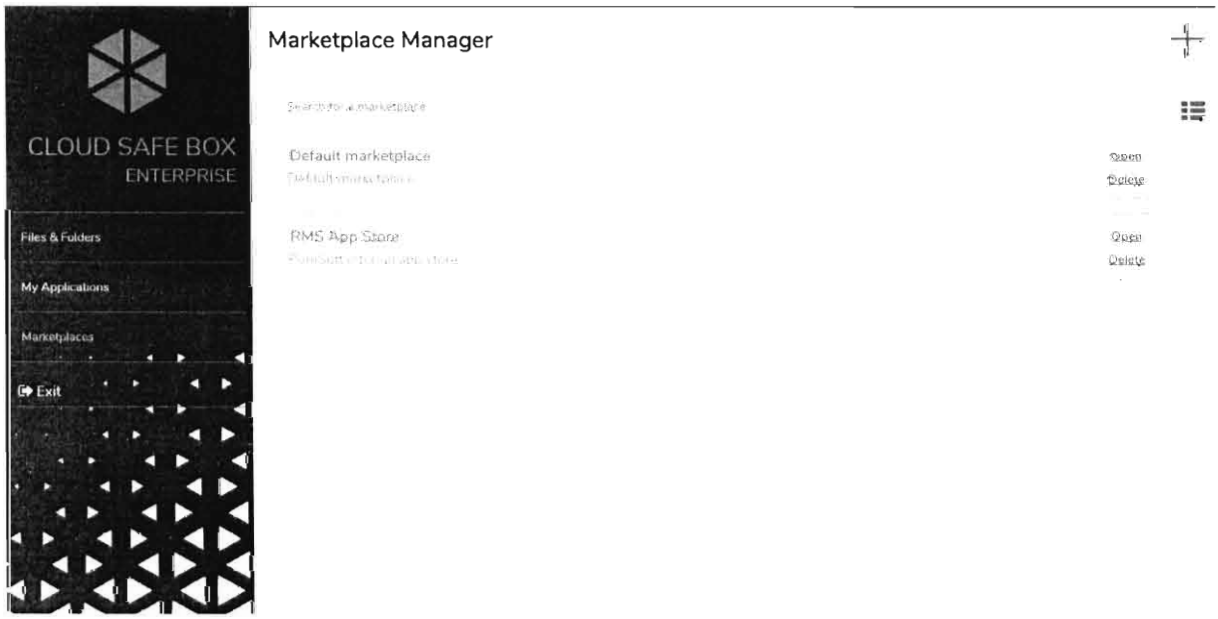

Figura 7 Pagina Marketplace Manager după adăugarea unui marketplace nou

Companie

Rector,
Prof. Dr. Tudorel Toader

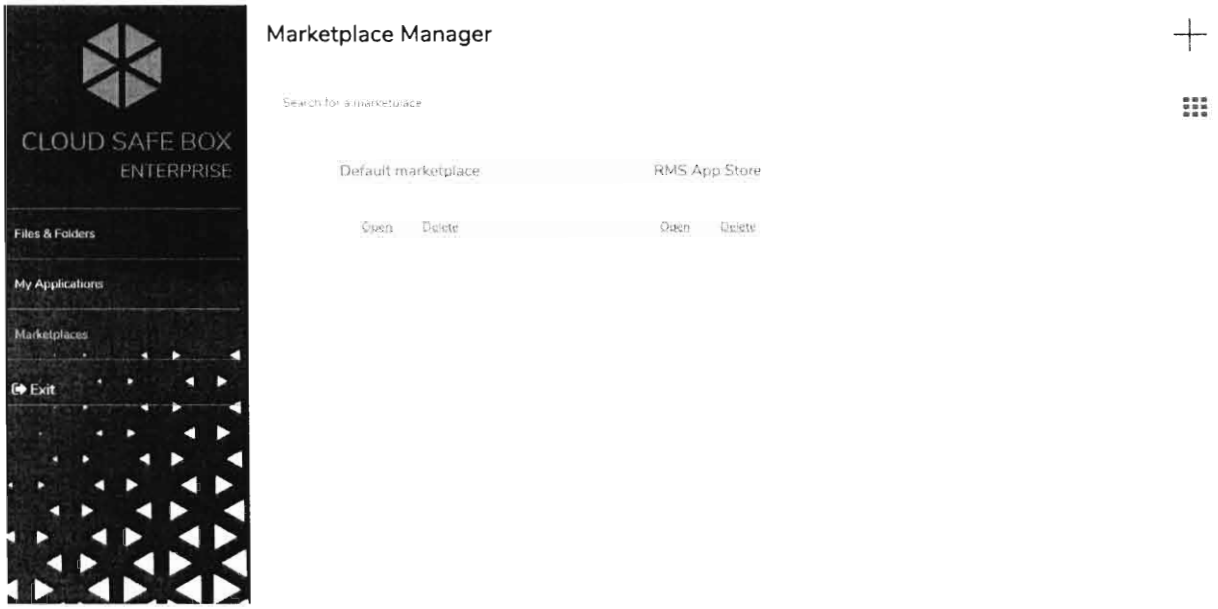

Figura 8 Pagina Marketplace Manager - tip vizualizare grilă

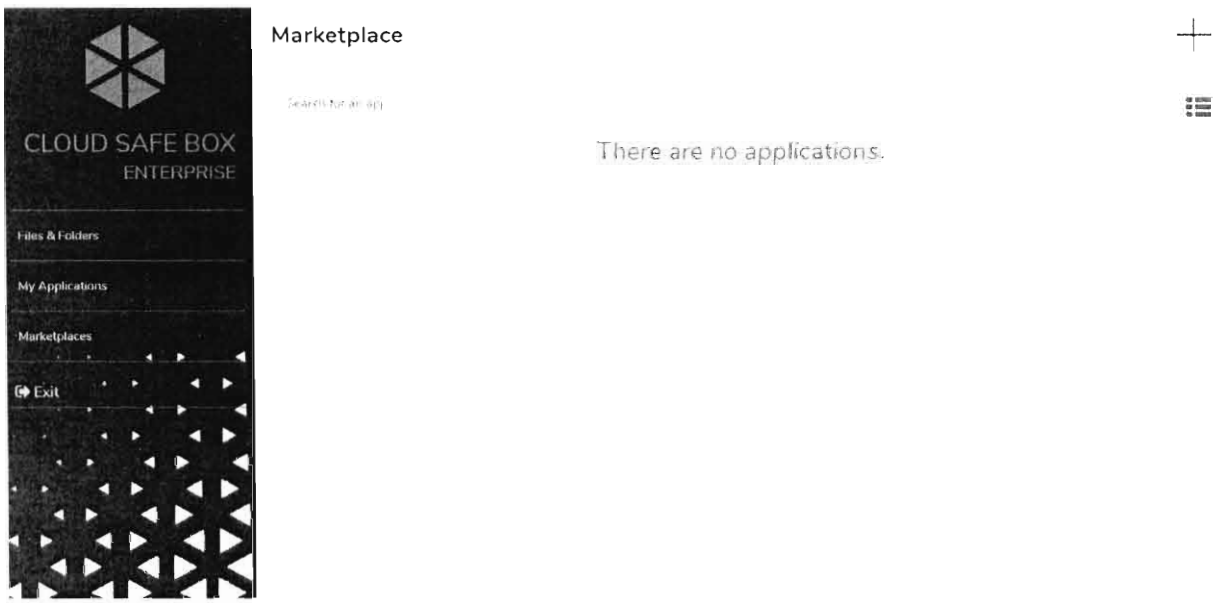

Figura 9 Pagina principală a unei instanțe de marketplace nou

Companie

SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

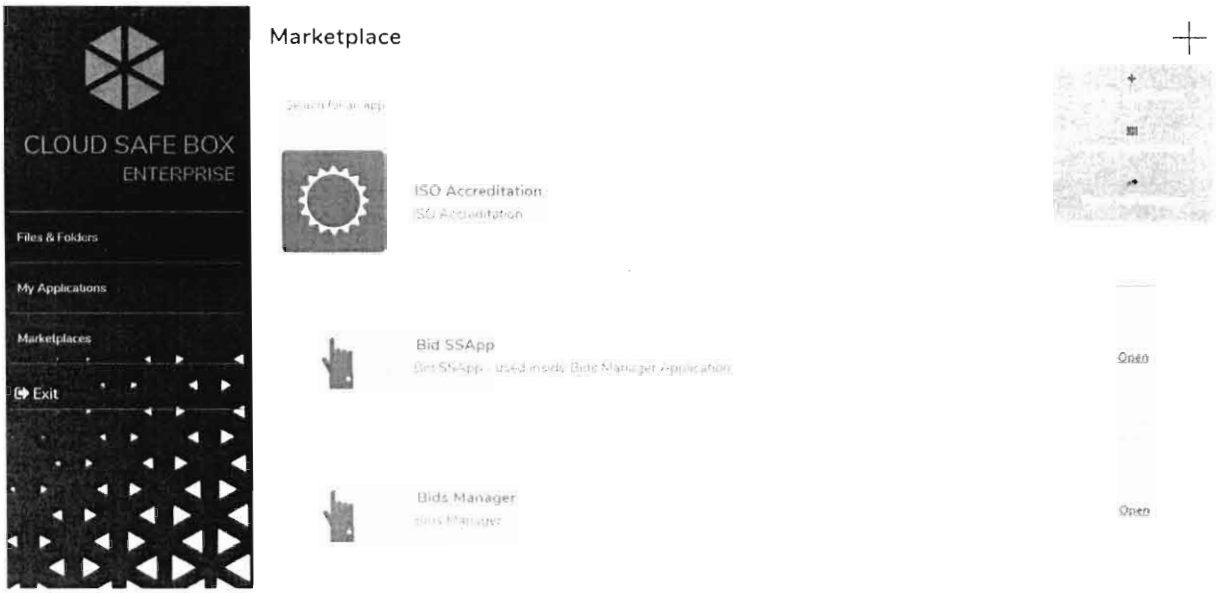

Figura 10 Pagina principală a unei instanțe de marketplace - meniul de adăugare este deschis

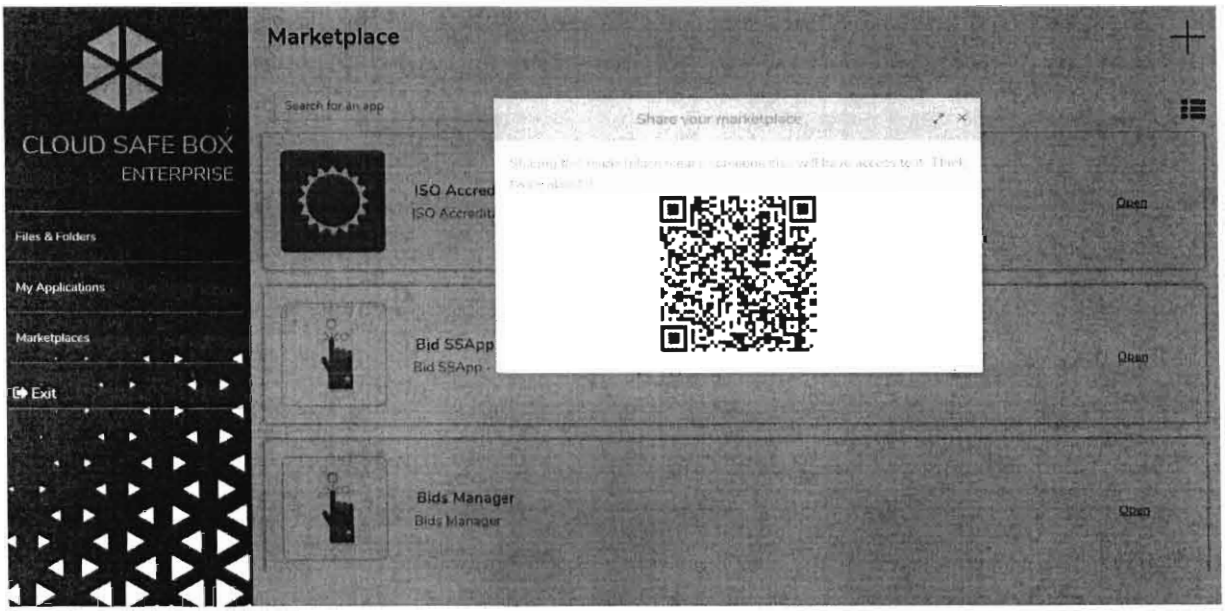

Figura 11 QR Code generat pentru opțiunea de partajare a unei aplicații din cadrul unui marketplace

Companie

SOCIETATEA COMERCIALĂ ROMSOFT SRL C.I.F. RO 14362760 J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

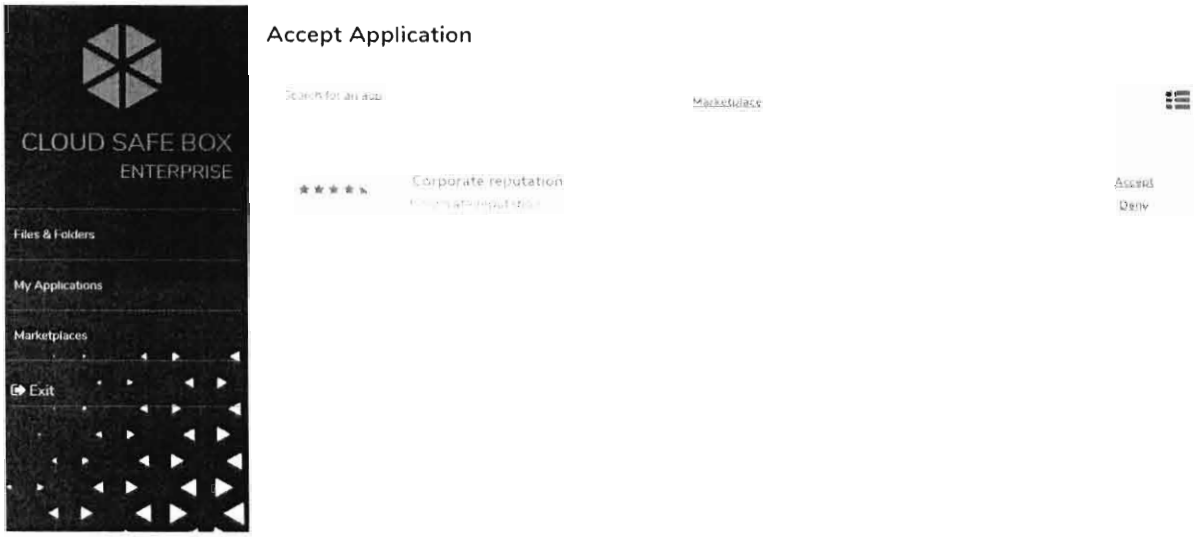

Figura 12 Pagina de management al aplicațiilor noi adaugate în marketplace

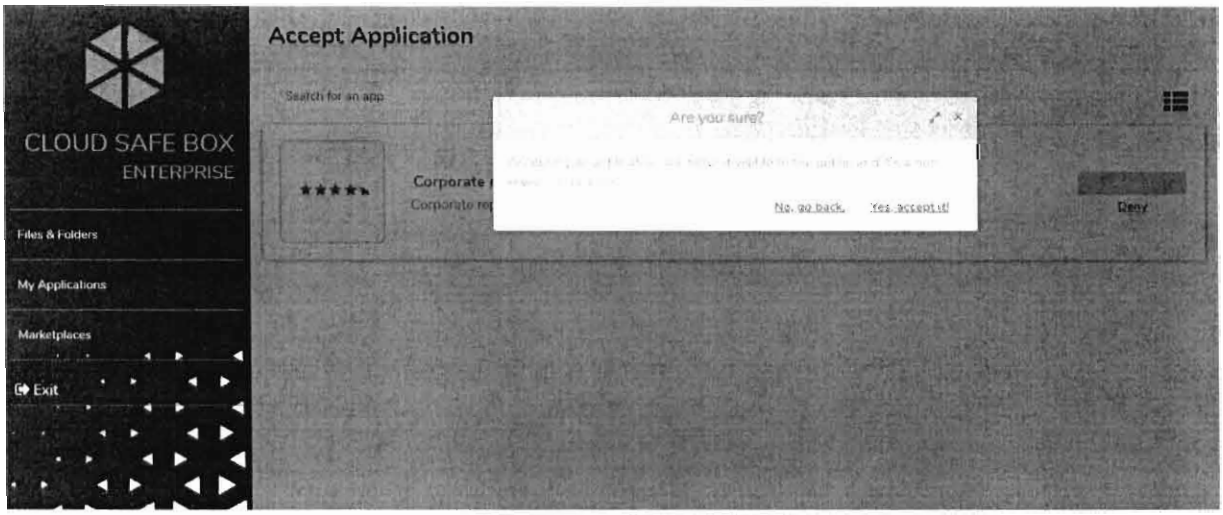

Figura 13 Mesaj de confirmare afișat pentru acțiunile luate asupra aplicațiilor noi adăugate

Companie

SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

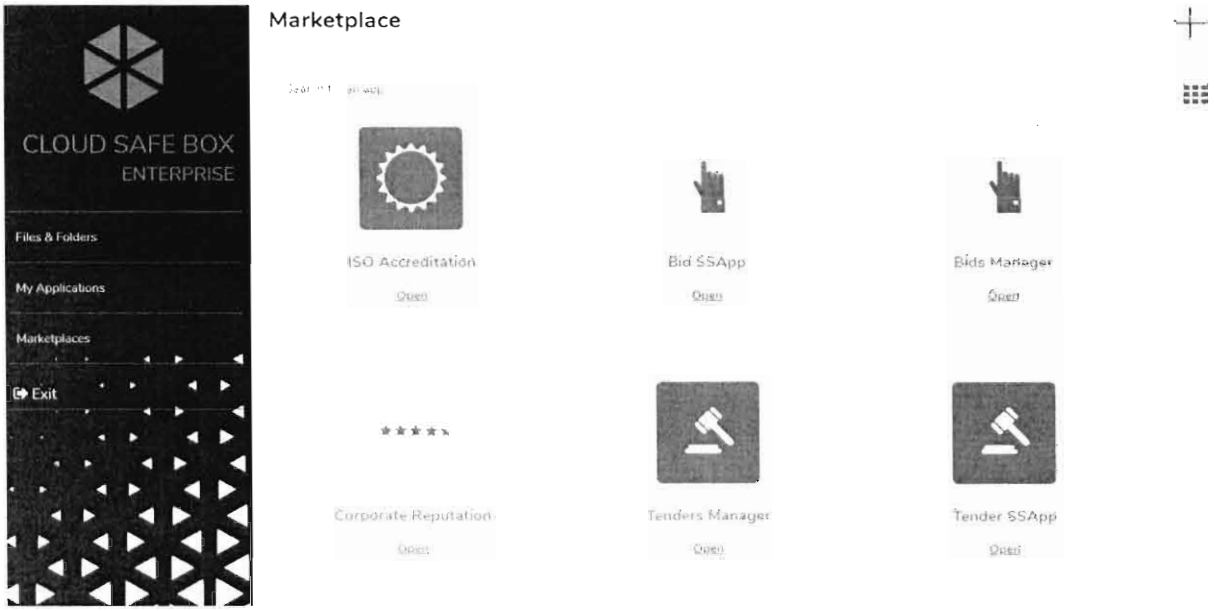

Figura 14 Pagina principală a unui marketplace după ce noua aplicație a fost acceptată

Figura 15 Conținutul paginii principale a aplicației ISO 27000 Information security management systems - instanță nouă de aplicație

Companie

SOCIETATEA COMERCIALĂ C.I.F. RO14362760 ROMSOFT SRL J22/1183/2001 IAȘI, ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

Figura 16 Conținutul paginii principale a aplicației ISO 9001 Quality Manager - instanță nouă de aplicație

Figura 17 Conținutul paginii principale a aplicației Authenticator - instanță nouă de aplicație

Companie

SOCIETATEA COMERCIALĂ ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA C.I.F. RO 14362760

Rector,
Prof. Dr. Tudorel Toader

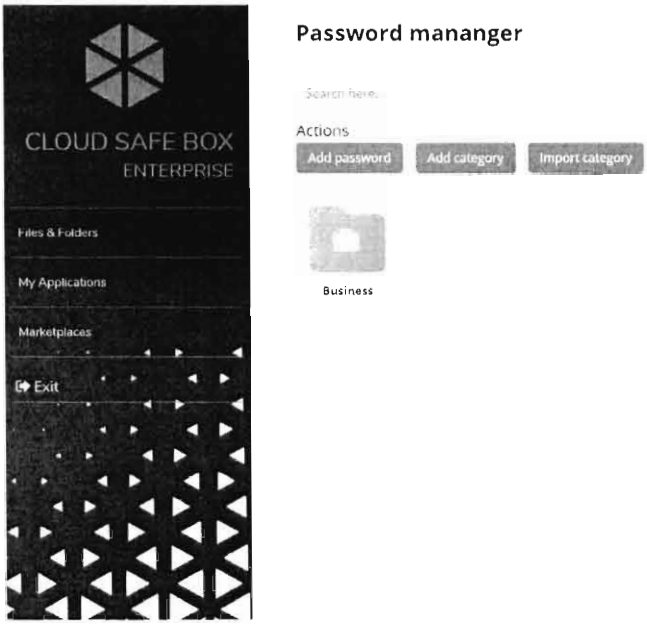

Figura 18 Conținutul paginii principale a aplicației Password Manager - instanță nouă de aplicație

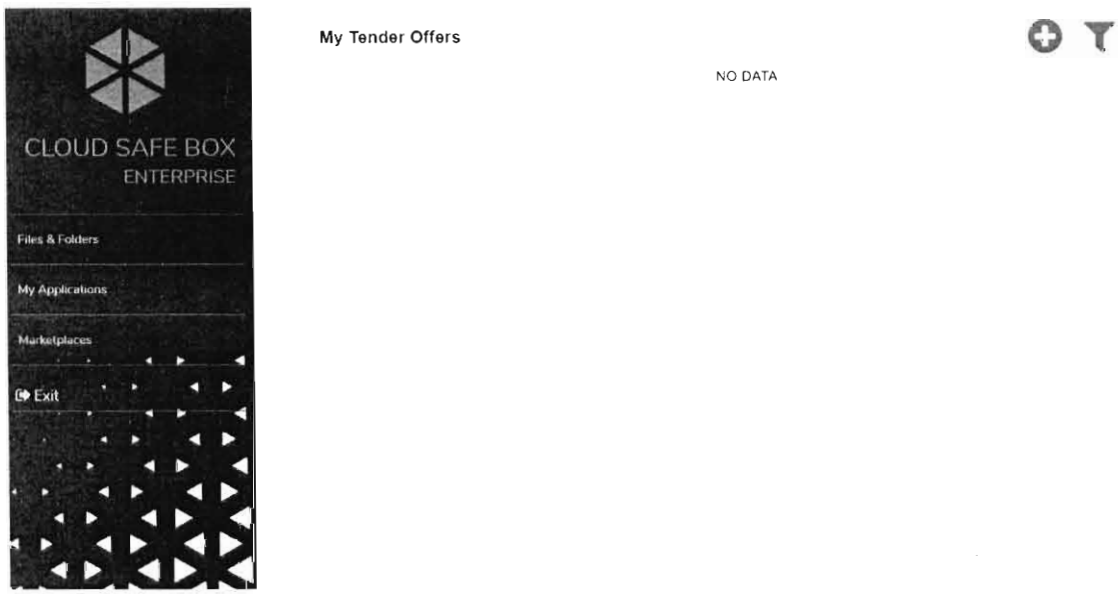

Figura 19 Conținutul paginii principale a aplicației Tenders Manager - instanță nouă de aplicație

Companie

SOCIETATEA COMERCIALĂ ROMSOFT SRL J22/1183/2001 IAȘI-ROMÂNIA

Rector,
Prof. Dr. Tudorel Toader

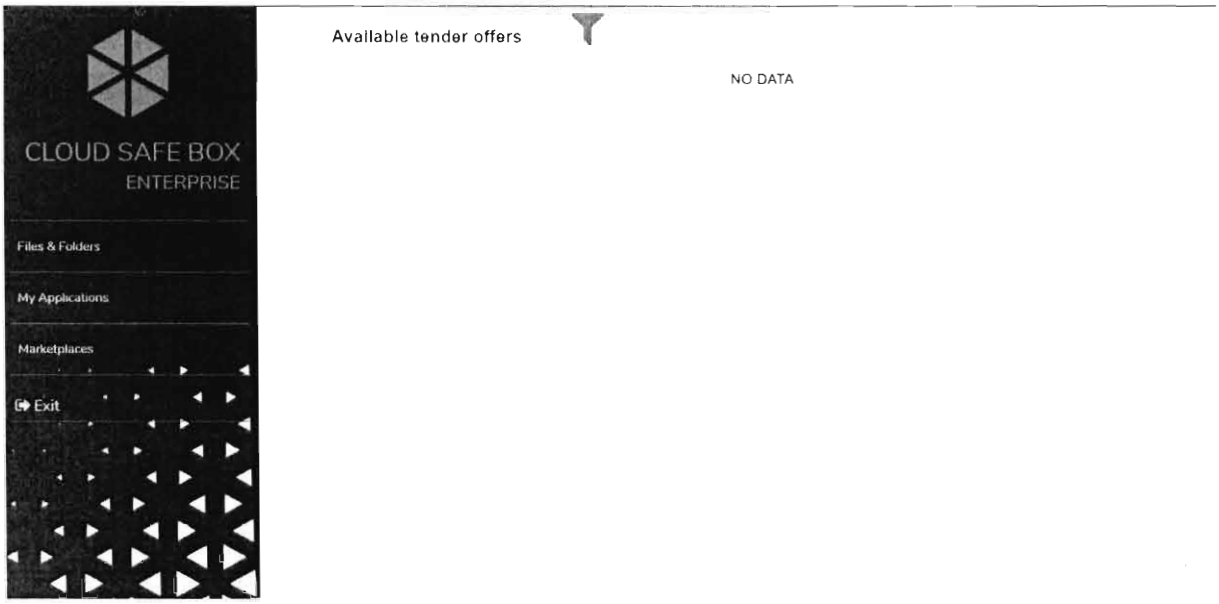

Figura 20 Conținutul paginii principale a aplicației Bids Manager - instanță nouă de aplicație

Companie

Rector,
Prof. Dr. Tudorel Toader