(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 127992 A0**
(51) **Int.Cl.**
G06F 21/24 (2006.01);
G06Q 90/00 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2012 00424**

(22) Data de depozit: **13.06.2012**

(41) Data publicării cererii:
29.11.2012 BOPI nr. **11/2012**

(71) Solicitant:
• **ISIGN SOLFTWARE SRL**,
STR. VIRGIL MADGEARU NR. 25A, CORP C, AP. 12, SECTOR 1, BUCUREŞTI, B, RO

(72) Inventatori:
• **POPESCU IULIAN VASILE**,
BD. IULIU MANIU NR. 18-20, BL. 15 A+B, SC. 1, AP. 81, SECTOR 6, BUCUREŞTI, B, RO

(54) # SOLUŢIE GENERICĂ DE CONECTARE LA DISPOZITIVE DE CRIPTARE DIGITALĂ

(57) **Rezumat:**

Invenţia se referă la o aplicaţie capabilă să se conecteze la orice tip de dispozitiv de criptare, astfel încât să se realizeze emiterea certificatelor digitale sau marcarea temporală a documentelor. Aplicaţia conform invenţiei comunică cu un computer specializat în activităţi criptografice (**HSM**) (Hardware Security Module) pe care sunt stocate certificate şi chei private ale unei autorităţi de certificare, aplicaţia de certificare (**CA**) (Certification Authority) solicită computerului specializat (**HSM**) semnarea certificatelor numai atunci când acestea sunt validate de către un operator al autorităţii, iar pentru servicii de marcare temporală, după salvarea cererii venite din partea unui client, aplicaţia (**CA**) creează un pachet de marcare temporal, pe care îl va trimite la semnare computerului specializat (**HSM**) de care se conectează.

Revendicări: 1
Figuri: 3

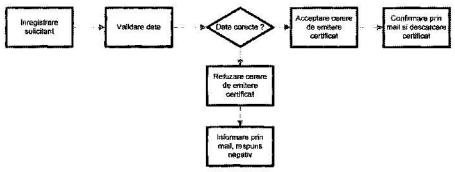

Fig. 1

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 127992 A0

48

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
a 2012 00424
Data depozit 13.06.2012

13.2 DESCRIERE

Titlul invenţiei:

Soluţie generică de conectare la dispozitive de criptare digitală

Domeniul tehnic la care se referă invenţia: tehnologia informaţiei

1. Scopul documentului

Acest document descrie din punct de vedere funcţional şi tehnic modul de conectare la un dispozitiv criptografic, cu utilizarea sa cea mai uzuală şi anume semnătura electronică şi marcarea temporală.

2. Prezentarea procesului

(vezi figura 2.1 de la „DESENE")

Obţinerea unui certificat digital calificat se face în mai multe etape, fiecare etapă având un rol bine determinat şi desfăşurându-se sub responsabilitatea solicitantului, al AI (Autorităţii de înregistrare), sau al AC (Autorităţii de certificare). Fiecare etapă din cele prezentate mai sus, se desfăşoară la rândul său pe mai mulţi paşi.

2.1 Înregistrare solicitant

Înregistrare solicitant este punctul de intrare în sistem şi are rolul de a înregistra o cerere de emitere de certificat calificat. În această etapă se primesc două categorii de informaţii: informaţii online legate de solicitant şi de certificatul dorit şi documentele necesare emiterii certificatului calificat.

Un utilizator trebuie să prezinte AI, următoarele documente:

a) act de identitate (carte de identitate, buletin, paşaport, CUI pentru societăţi comerciale)

b) declaraţie pe proprie răspundere prin care solicitantul îşi expirmă acordul cu condiţiile generale ale ISIGN SOFTWARE privind furnizarea serviciilor de certificare. Formularul acestei declaraţii se poate descărca de pe site-ul ISIGN SOFTWARE:

c) în cazul certificatelor emise pentru instituţii, este necesară şi o împuternicire sau dovadă că solicitantul are dreptul de a semna în numele instituţiei.

Autoritatea de înregistrare are obligaţia de a face copii după documentele originale primite de la solicitant şi le va păstra pe baza metodologiei de arhivare a informaţiilor personale. Aceste metodologii sunt definite în cadrul procedurilor interne de protecţie a informaţiilor cu caracter personal.

În cadrul formularului web sunt cerute, în mai mulţi paşi, informaţii legate de solicitant, instituţia pe care o reprezintă şi despre certificat.

Pas 1: se introduce CNP-ul clientului, sau pentru persoanele care nu sunt cetăţeni români, se introduce codul unic de identificare similar. În funcţie de acest cod, sistemul va verifica dacă clientul mai este deja în baza de date, sau este un client nou. În funcţie de acestă verificare, se va trece la pasul următor.

Pas 2: dacă clientul este un utilizator nou al serviciilor de certificare, atunci în acest pas va trebui să completeze toate datele personale (nume, prenume, adresă, serie şi număr act de identitate, alte

CN-2012-00424--
13 -06- 2012

informații de contact etc). În cazul în care clientul este deja în baza de date, atunci acestuia i se va cere, doar să actualizeze aceste câmpuri, dacă este cazul.

Pas 3: se introduc informațiile legate de certificatul ce se doreşte a fi emis: adresa de email, instituția, funcția şi opțional localitatea şi adresa clientului. Tot în acest pas, prin intermediul unui applet Java semnat, se accesează DCSC-ul (Dispozitiv securizat de creare a semnăturii electronice), care bineînțeles trebuie să fie conectat la calculator. DSCS-ul va genera o pereche de chei care vor fi legate de certificatul ce va fi emis. Cheia publică este împachetată într-un obiect PKCS#10 şi este trimisă odată cu celelalte informații, către server-ul autorității de certificare, unde sunt stocate în baza de date.

Un client nu poate să aibă mai mult de un certificat valid pe acceaşi adresă de email. După ce aceste informații sunt completate utilizatorul va fi înştințat că o să primească un email cu raspunsul pozitiv sau negativ al validării datelor.

2.2 Validare date

Un responsabil cu validarea solicitărilor de certificare, din partea ISIGN SOFTWARE, va trebui să verifice dacă informațiile venite prin formularul web, coincid cu realitatea (documentele primite de către AI). Drepturile de validare a cererilor de certificate sunt date de către responsabilul cu gestiunea autorității de certificare, care poate să creeze conturi noi, să dezactiveze pe cele deja existente, sau să modifice drepturile de acces ale acestora.

a-2012-00424--
13 -06- 2012

Există mai multe tipuri de drepturi pe care un operator le poate avea în sistem: de înregistrare, de revocare, de validare şi de administrare operatori.

Dreptul de administrare a operatorilor îl are doar responsabilul cu gestiunea autorității de certificare.

Ca rezultat al etapei de validare, operatorul responsabil, va trebui să accepte sau să refuze cererea de certificare din partea solicitantului. În cazul unui răspuns negativ, operatorul va trebui să precizeze şi cauza refuzului.

În ambele cazuri, solicitantul va primi pe email răspunsul cererii de certificare. În cazul unui răspuns pozitiv în email va fi trecută şi o adresă URL, de unde se poate descărca certificatul calificat pe un dispozitiv DSCS (Dispozitiv securizat de creare a semnăturii electronice).

2.3 Descărcare certificat

Dacă cererea de certificare a fost validată, atunci solicitantul va primi un mail de confirmare, unde va găsi şi adresa web de unde va putea să descarce acest certificat Descărcarea şi revocarea unui certificat se fac numai pe baza unei parole asociate la certificat. Această parolă a fost introdusă, odată cu informațiile legate de certificat, în etapa de înregistrare.

Descărcarea certificatului se poate face numai pe DCSC-ul care a fost folosit şi în etapa de înregistrare, deoarece, certificatul conține cheia publică a solicitantului, cheie verificată şi la descărcarea certificatului pe dispozitiv.

Conform standardului PKCS#11, dispozitivul securizat este împărțit în „entry-uri", unde se țin cheia publică, cheia privată şi certificatul.

Acest lucru permite, unui utilizator, stocarea mai multor certificate pe un asemenea dispozitiv.

Pentru a permite lucrul cu mai multe certificate pe acelaşi dispozitiv, aplicația autorității de certificare, va salva, în etapa de înregistrare, numele intrării nou create, odată cu perechea de chei.

Numele noii intrări a DSCS-ului este un număr unic, calculat în funcție de momentul de timp în care se face înregistrarea. Acest nume este transmis, odată cu toate informațiile solicitantului, către AC, şi va fi folosit de către aplicația de certificare, în etapa de descărcare a certificatului, pentru a ştii exact unde să fie scris certificatul (în care din intrările DSCS-ului).

Descărcarea certifcatului de pe serverul autorității de certificare şi scrierea lui pe DSCS se face cu ajutorul unui applet Java semnat, care are acces la resursele locale şi care poate să comunice cu dispozitivul de securitate. Acesta este acelaşi applet folosit la etapa de înregistrare, dar care are două funcții diferite în funcție de parametri de intrare dați.

3. Preambul

În proiectarea sistemului de emitere a certificatelor calificate s-a ținut cont de doi factori foarte importanți: securitatea sistemului, dar şi uşurința şi fiabilitatea în exploatare. Sunt de remarcat câteva din metodele, care combină cei doi factori menționați mai sus: parola de acces pe certificat, sistemul de comunicare prin email şi metodele de

a-2012-00424--
13 -06- 2012

protecție implementate la descărcarea certificatului pe un dispozitiv securizat.

Datorită utilizării unui applet Java pentru comunicarea cu DSCS-ul, va trebui ca pe maşina, pe care se execută etapele de înregistrare şi de descărcare a certificatului, să fie instalată o maşină virtuală Java, cel puțin versiunea JRE 1.5. Acest lucru poate părea o limitare, dar pe de altă parte permite rularea şi sub browsere de internet din altă familie decât Internet Explorer, ca în cazul tehnologiei ActiveX.

Orice browser de internet ar fi folosit, trebuie să fie configurat pentru a permite rularea appleturilor Java semnate digital.

4. Descrierea sistemului informatic

4.1. Introducere

Acest document descrie un sistem de certificare generic folosit de către o autoritate de certificare.

4.2. Infrastructura

(vezi figura 4.1 de la „DESENE")

4.2.1 Router

Routerul este un model LinkSys RV042, care permite două linii de internet de intrare, una principală şi ceea de-a doua de rezervă. Dacă internetul cade pe linia principală, atunci router-ul comută automat pe ceea de-a doua linie.

a 2012-02424--
13 -06- 2012

4.2.2 Firewall

Firewall-ul este o maşină care rulează sistemul de operare Linux, distribuția CentOS v6.2 şi care este configurată să protejeze rețeaua autorității de certificare de accesul neautorizat din afară.

4.2.3 Intrusion Detection System (IDS)

Pentru a monitoriza eventualele încercări de penetrare a sistemului este instalat şi un sistem de detecție a intruziunii, Intrusion Detection System (IDS).

Acesta este tot o maşină Linux, distribuția CentOS v6.2, pe care sunt instalare aplicațiile Snort şi Acid. Logurile sunt vărsate şi raportate dintr-o bază de date MySQL.

Toate logurile generate de IDS vor putea fi consultate de administratorul sistemului din interfață web.

4.2.4 ISSWeb

ISSWeb este un cluster format din două servere, care au rolul de a fi ține aplicația web de generare a certificatelor digitale. Aici este găzduit subdomeniul care conține toate paginile ce țin de Registrul autorității de certificare.

Cele 2 servere ISSWeb1 şi ISSWeb2 îşi fac automat mirroring folosind funcții din cadrul sistemului de operare Windows 2008 Server R2 Enterprise Edition.

Pe aceste servere rulează Apache Tomcat Application Server v5.5.20, care serveşte pagini web pe portul 443 (HTTPS). Acest server va servi atât paginile statice cât şi cele cu conținut activ (Java Server Faces).

4.2.5 ISSDB1

Pentru stocarea informațiilor legate de clienți şi de certificate se foloseşte un o bază de date SQL, gestionată de un server SQL Server 2008 Standard Edition, instalat pe ISSDB1.

4.2.6 ISSDB2

Serverul ISSDB1 are şi el un backup, pentru a respecta un nivel de redundanță ridicat. Baza de date SignTechCA de pe serverul ISSDB1 este replicată pe ISSDB2 în mod continu. În cazul în care serverul ISSDB1 are probleme, ISSDB2, nu numai că va putea să readucă datele din baza de date, dar poate să îi ia locul în mod activ, printr-o simplă comutare a dateleor de conectare la baza de date folosite de ISSWeb.

4.2.7 Hardware Security Module (HSM)

Hardaware Security Module (HSM), este un computer specializat în activități criptografice. Rolul HSM-ului este de a stoca cheile autorităților de certificare din cadrul ISS şi de a semna toate certificatele care sunt emise clienților.

HSM-ul este produs de firma Algorithmic Research din Israel, iar modelul său este PrivateServer v4.

Comunicarea cu acest dispozitiv se face folosind stanradrul PKCS#11. Pentru aceasta serverul ISSCAServer comunica direct pe un cablu UTP dedicat, izolând astfel HSM-ul de restul rețelei. (vezi figura 4.2 Hardware Security Module de la „DESENE")

În tabelul de mai jos se găsesc specificațiile tehnice ale HSM-ul de la Algorithmic Research utilizat pentru testarea aplicației:

2012-00424--
13 -06- 2012

Caracteristică	Valoare
Algoritm asimetric de criptare	RSA (320-4096 bits)
Algoritm simetric de criptare	DES, Triple-DES, AES
Standarde de securitate	FIPS 140-1 Level 3 FIPS 140-2 level 3* FCC Subpart B Class B EN 55022 Class B for AC
Stocare sigură a cheilor	Da
Conectivitate	TCP/IP Ethernet LU6.2 Token Ring LU6.2 SDLC
API criptografic	PKCS#11 MS CAPI JCA
Dimensiuni fizice	W 48.3cm; D 44.7cm; H 17.8cm 6U Rack mountable Greutate: 15KG
Moduri de autentificare	Smart Card (Windows only) USB Token (Windows only) Software Key (Windows, Linux, HP, AIX and Solaris)
Performanță	450 RSA Signatures pe secundă (1024 bit) 5500 Symmetric Transactions pe secundă
Funcții HASH	SHA-1, SHA-256, SHA-512 ISO-Hashing ARDFP

Management de la distanță	Da
Sisteme de operare clienți	MS Windows 2000, XP, 2003 Server Sun/ Solaris HP-UX, AIX, Linux OS/2 STRATUS/VOS Tandem MVSOS390

4.2.8 Domanin Controller

Pentru a asigura funcționarea serverelor ISSWeb în cluster şi pentru o mai uşoară administrare s-a implementat un domeniu pentru autoritatea de certificare. Domeniul este *isign.ro*. Calculatorul de Domain Controller are numai această funcție.

5. Problema de rezolvat

Pentru a asigura funcționarea sistemului este necesară comunicarea cu dispozitivul Hardware Signing Module, producătorul acestuia nu oferă o soluție concretă, ci doar aplicații în baza cărora să se dezvolte software ajutător de către utilizatori, în funcție de platforma utilizată şi tipul de utilizare indicat (HSM având mai multe utilizări potențiale, de exemplu, gestionarea PIN cardurilor bancare).

În acest sens, este nevoie de o aplicație capabilă să se conecteze la orice tip de dispozitiv de criptare, pentru a nu mai fi dependent de platformă sau producător.

Pentru emiterea certificatelor digitale, aplicatia va trebui sa comunice cu un HSM pe care sunt stocate certificatele si cheiele private ale autoritatii de certificare si subautoritatile sale. Aplicatia de certificare,

numita si CA (Certification Authority) va trebui sa ceara HSM-ului semnarea certificatelor numai atunci cand acestea sunt validate de catre un operator al autoritatii.

Pentru servicii de marcare temporală, după salvarea cererii venite din partea clientului, aplicatia va crea un pachet de marcare temporal, pe care il va trimite la semnare HSM-umului de care se conecteaza.

Comunicația cu HSM-ul se realizeaza pe baza standardului PKCS#11.

6. Soluția

Soluția aleasă este una independentă de sistemul de operare, bazată pe Java care include pachete ce trebuiesc instalate neapărat pe sistemul local (necesită să existeța funcțională a unei maşini virtuale Java), acolo unde are loc accesul securizat la certificatele digitale.

Codul aplicației de conectare poate fi folosit de sine stătător, cu propria interfața grafică, sau integrat în alte aplicații, prin care se prelucrează datele care necesită fie semnarea digitală prin intermediul unui certificat digital, fie marcarea temporală pentru dovedirea datei certe de elaborare a documentelor. Totul este scris în Java, având avantajele rulării pe orice sistem de operare, existenței unor unelte performante pentru prelucrare XML-PDF şi al securității lucrului cu certificate digitale.

Interfetele specifice criptografiei sunt bazate pe furnizori, permitand multiple implementari interoperabile. Unii furnizori pot efectua operatii criptografice in software; altii pot realiza operații pe un token hardware (de exemplu pe dispozitive smartcard).

a-2012-00474--
13 -06- 2012
37

Platforma Java include furnizori predefinitipentru cei mai utilizati algoritmi criptografici, incluzand algoritmii RSA si DSA de semnatura, algoritmii de criptare DES, AES si ARCFOUR, si algoritmii de hash MD5 si SHA-1. Acesti furnizori implementeaza algoritmii criptografici in cod Java. Infrastructura de chei publice (PKI) este un termen folosit pentru un framework care permite un schimb de informatii securizat bazat pe arhitectura de chei publice (se folosesc algoritmi de chei asimetrice in locul sau laolalta cu algoritmii de chei simetrice). Permite persoanelor/organizatiilor sa utilizeze cetificatele digitale si ofera mijloace de verificare a autenticitatii certificatelor. Platforma Java incude suport pentru certificate digitale X.509 si pentru CRL-uri.

Clasele asociate cu PKI-urisunt localizate in pachetele java.security si java.security.cert.

Platforma Java permite o stocare persistentă a cheilor si a certificatelor via depozitelor de certificate si chei. Mai exact, clasa java.security.KeyStore reprezinta un depozit de chei, permitand stocarea cheilor criptografice si/sau a certificatelor digitale de tip trusted (pentru a fi utilizate ulterior in validarea cu ajutorul certificatelor), cat si clasa java.security.CertStore care reprezinta un depozit de certificate. Un CertStore poate stoca si certificate.

Furnizorul SunPKCS11 include o implementare KeyStore PKCS11. Acest lucru inseamna ca certificatele si cheile pastrate intr-un hardware securizat (spre exemplu intr-un smartcard) pot fi accesate si utilizate de aplicatiile Java via API-ului KeyStore. Ca o observatie cheile din smartcard-uri nu le este permis sa parasesca dispozitivul. In aceste cazuri obiectul java.security.Key returnat de API-ul KeyStore ar putea fi o simpla referinta la cheie (acest lucru insemnand ca nu contine explicit

cheia). Acest obiect de tip Key ar pute fi folosit numai pentru a realiza operatii criptografice numai asupra dispozitivului unde este pastrata cheia.

Platforma Java include de asemenea un depozit de certificate de tip LDAP (pentru a accesa certificatele stocate intr-un director LDAP) cat si un depozit de certificate in-memory de tip Collection (pentru certificatele dintr-un obiect java.util.Collection).

Aplicația integrată posedă următoarele caracteristici:

a) Pentru partea de emitere certificate digfitale:

Aplicatia de emitere a certificatelor calificate trebuie sa respecte normele legii semnaturii electronice 455/2001, normele de aplicare ale acesteia, precum si standardele referite de aceste documente:

C1: aplicatia este pe o platforma web.

C2: aplicatia permite inscrierea clientilor pentru obtinerea de certificate calificate.

C3: păstrează un numenclator de client, identificarea unica facandu-se dupa codul numeric personal sau similarul sau pentru cetateni straini.

C4: aplicatia permite cautarea si afisarea informatiilor legate de certificatele emise si starea acestora.

C5: aplicatia lucrează cu o baza de date tip SQL in care va stoca certificatele calificate emise si toate detaliile necesare (attribute, stare, data emiterii, data expirarii, data revocarii etc).

2-2012-00424--
13 -06- 2012

C6: aplicatia permite validarea de catre un operator al autoritatii, datele inscrise pentru obtinerea unui certificate, avand in fata documentele furnizate de catre client.

C7: un operator al autoritatii de certificare poate refuza o cerere venita din partea unui client, doar pe baza unui motiv pe care il va mentiona in aplicatie.

C8: Validarea datelor clientului de catre un operator va duce automat la generarea certificatului calificat si semnarea acestuia de catre autoritate folosind un dispozitiv HSM (Hardware Security Module).

C9: Fiecare certificate are o serie unica formata din un cod unic al autoritatii si un numar de ordine al certificatului generat in registrul certificatelor.

C10: De asemenea certificatul calificat respecta atributele cerute de catre legea semnaturii electronice si normele de aplicare ale acesteia prin standardele referite.

C11: Se vor trece sub forma de atribute informatii ca numele posesorului, orasul, organizatia si functia sa, acolo unde este cazul.

C12: Aplicatia comunică cu un HSM pe care sunt stocate certificatele si cheiele private ale autoritatii de certificare si subautoritatile sale. Aplicatia de certificare, numita si CA (Certification Authority), cere HSM-ului semnarea certificatelor numai atunci cand acestea sunt validate de catre un operator al autoritatii.

0-2012-00424--
13 -06- 2012

C13: Orice client are posibilitatea, pe baza unui cont si a unei parole, sa revoce certificatul, in cazul in care acesta a fost compromise.

C14: Revocarea este disponibila la orice ora, si de pe orice platform hardware si software.

C15: De asemenea revocarea este posibila si de catre un operator al autoritatii, pe baza unei cereri venite din partea clientului.

C16: Sistemul permite managementul operatorilor si al nivelului de acces al acestora in cadrul sau. Trebuie sa se faca diferenta clara intre operatorii care pot valida certificate, anula certificate sau cei care administreaza conturile sistemului.

C17: aplicatia va treui sa genereze periodic pentru autoritatea de certificare si pentru orice subautoritate a acesteia, la un interval setabil de timp pentru fieecare in pate (ex: 12 ore), o lista a certificatelor revocate – CRL (Certification Revocation List), utilizand standardele cerute de lege. Fisierele CRL vor fi semnate de HSM cu certificatele autoritatii parinte pentru fiecare CRL in parte. Dupa semnare fisierele CRL vor fi stocate in baza de date, dar si pe server-ul web astfel incat fisierul sa poata fi consultat de clientii umane din pagina web, dar si automat de catre aplicatiile software.

C18: La introducerea datelor de catre client, sau de catre un operator al autoritatii, cu scopul obtinerii unui certificate, adresa de email a clientului este validată prin trimiterea unui email cu un anumit link web, pe care clientul va trebui sa il acceseze. Prin acesarea acestui link aplicatia va primi confirmarea ca adresa de

email exista si este active. Daca trece un anumit timp, setabil de catre administratorul sisitemului, cererea de validare a emailul va trebui sa expire, pentru a nu fi utilizata in alte scopuri.

C19: Dupa finalizarea procesului de inscriere a unui client, acesta va primi alt email prin care este informat ca cererea lui de emitere a unui certificate a fost inregistrata cu succes si ca aceasta va fi verificata de catre un operator al autoritatii.

C20: Daca cererea de emitere a unui certificate calificat este respinsa de catre operator, atunci clientul primeste un email de informare prin care sa se precizeze si motivul pentru care cererea sa a fost respinsa. Motivul transmis prin email este textul pe care operatorul il introduce in sistem la respingerea unei cereri de certificare.

C21: Dupa validarea unui certificat, de catre operatorul autoritatii, clientul va primi un email de informare ca cererea sa a fost aprobata si va avea si o adresa URL de unde va putea sa descarce certificatul generat de catre autoritate. Descarcarea unui certificate se face pe un dispozitiv de securitate de tip token sau smart-card. Comunicarea cu dispozitivele de securitate se face folosind standardul PKCS#11. La descarcarea certificatului se cere clientului sa introduca o parola, pe care a specificat-o in procesul de inscriere. De asemenea aplicatia va face si o verificare ca dispozitivul securizat pe care este descarcat certificatul calificat sa fie acelasi cu cel folosit la generarea perechii de chei din procesul de inscriere.

C22: La revocarea unui certificat se trimite automat un email pe adresa de email a clientului, prin care este informat de aceasta actiune.

C23: Toate aceste emailuri, pe care aplicatia le transmite clientilor, sunt modificabile de catre un administrator, prin editarea unor template-uri ale acestora.

C24: La revocarea unui certificate se va genera imediat si lista de certificate revocate CRL, care va include noul certificate revocat.

C25: Certificatele care au expirat, conform perioadei de valabilitate, nu vor mai fi trecute in listele CRL.

C26: Paginile in care este nevoie de acces la dispozitivul securizat al clientului contin un obiect ActiveX sau Java Applet semnate digital, pentru a avea acces la resursele locale ale calculatorului clientului.

C27: Aplicatia este complet functionala si optimizata cel putin pentru platform Internet Explorer 6 sau versiuni mai noi.

C28: Toate actiunile operatorilor in aplicatie vor trebui sa fie auditate si se vor pastra in baza de date, permitand astfel analiza acestora in cazul unor anumite contestatii. Actiunile logate vor include: inscrierea unui client, validarea sau respingerea unei cereri de certificare, revocarea unui certificate, generarea fisierelor CRL. Pentru fiecare actiune sistemul va trebui sa stocheze in baza de date un cod al actiunii, un identificator al operatorului responsabil, data si ora exacta a actiunii, si o lista de parametrii ai actiunii respective, acolo unde este cazul.

S-2012-00424--
13 -06- 2012

C29: De asemenea, aplicatia va trebui sa scrie in fisiere de tip log, toate erorile sau orice alte informartii care ar putea sa intereseze pe administratorii sistemului. In fisierele de tip log este obligatorie precizarea orei exacte.

C30: Accesul la zonele critice ale aplicatiei, cum ar fi modulul de administrare sau cel de validare cereri de certificare, va trebui sa fie limitat pe baza de IP al clientului care incearca sa se conecteze. Numai daca IP-ul acestuia este unul de incredere se va trece la pasul in care este ceruta parola de acces.

b) Pentru partea de marcare digitală:

Aplicatia de emitere a certificatelor calificate trebuie sa respecte normele legii marcii temporal 451/2004, normele de aplicare ale acesteia, precum si standardele referite de aceste documente:

C1: aplicatia este pe o platforma web.

C2: aplicatia lucrează cu o baza de date tip SQL in care va stoca marcile temporale emise si toate detaliile necesare (atribute, stare, data emiterii etc).

C3: Aplicatia gestionează o lista de clienti. Fiecare client va avea un cont de acces (username si parola), dar si o descriere a unui abonament de servicii. Prin abonament se intelege un numar de marcari temporal incluse, costul unei marcari peste cele incluse in abonament etc.

C4: Aplicatia va astepta sa primeasca cereri din partea aplicatiilor clientilor, cereri de marcare temporala in formatul impus de standardele referite de cadrul legislative.

C5: Daca clientul care cere semnarea nu cont sau nu este unul valid, atunci aplicatia va opri procesul de emitere al marcii temporal.

C6: Dupa receptionarea cererii de marcare, aplicatia va stoca informatiile venite de la client (data si ora, nume client, codul HASH al informatiilor care trebuiesc marcate temporal, IP-ul masinii prin care clientul s-a conectat).

C7: Dupa salvarea cererii venite din partea clientului, aplicatia crează un pachet de marcara temporal, pe care il va trimite la semnare HSM-umului de care se conecteaza. Comunicatia cu HSM-ul se realizeaza pe baza standardului PKCS#11.

C8: HSM-ul semneaza setul de date folosind certificatul si cheia private create special pentru marca temporal. Aplicatia va trimite inapoi clientului un raspuns cu o marca temporala in formatul cerut de standardele tehnice impuse de lege.

C9: Fiecare marca temporal va avea o serie unica de identificare formata din codul autoritatii de marcare temporala si un numar de ordine in registrul marcilor emise.

C10: Raspunsul catre un client poate sa fie sub forma unor coduri de eroare, acolo unde este cazul.

C11: Dupa trimiterea raspunsului catre client, aplicatia va salva in baza de date acest raspuns cu toti parametri necesari.

C12: Aplicatia genereaza, la cerearea unui operator al autoritatii, registrul marcilor temporal emise.

O-2012-00424--
13 -06- 2012

C13: De asemenea, marca temporala respectă atributele cerute de catre legea marcii temporale si normele de aplicare ale acesteia prin standardele referite.

C14: Sistemul permite managementul operatorilor si al nivelului de acces al acestora in cadrul sau

C15: Interfata cu utilizatorii funcționează cel putin pe navigatoarele Mozila Firefox 6 si Internet Explorer 6.

C16: Fiecare client va putea accesa o pagina web din cadrul aplicatiei, iar pe baza unui username si a unei parole, va putea sa intre in contul sau, unde sunt prezentate informatii legate de numar marcilor temporal emise pentru contul current, si toate detaliile acestora.

C17: Separat, trebuie luata in calcul dezvoltarea unui sistem integrat cu aplicatia de plata online a abonamentelor de catre clienti.

C18: Aplicatia scrie in fisiere de tip log, toate erorile sau orice alte informartii care ar putea sa intereseze pe administratorii sistemului. In fisierele de tip log este obligatorie precizarea orei exacte.

a-2012-00424--
13 -06- 2012

13.3 REVENDICĂRI

Prin prezenta dorim protejarea proprietății intelectuale pentru:

Soluție generică de conectare la dispozitive de criptare digitală

o aplicație capabilă să se conecteze la orice tip de dispozitiv de criptare, pentru a nu mai fi dependent de platformă sau producător astfel încât să se realizeze emiterea certificatelor digitale sau marcarea temporală a documentelor, conform descrierii acesteia depusă la actula cerere cu titlul „DESCRIERE".

a-2012-00424--
13 -06- 2012

13.4 DESENE

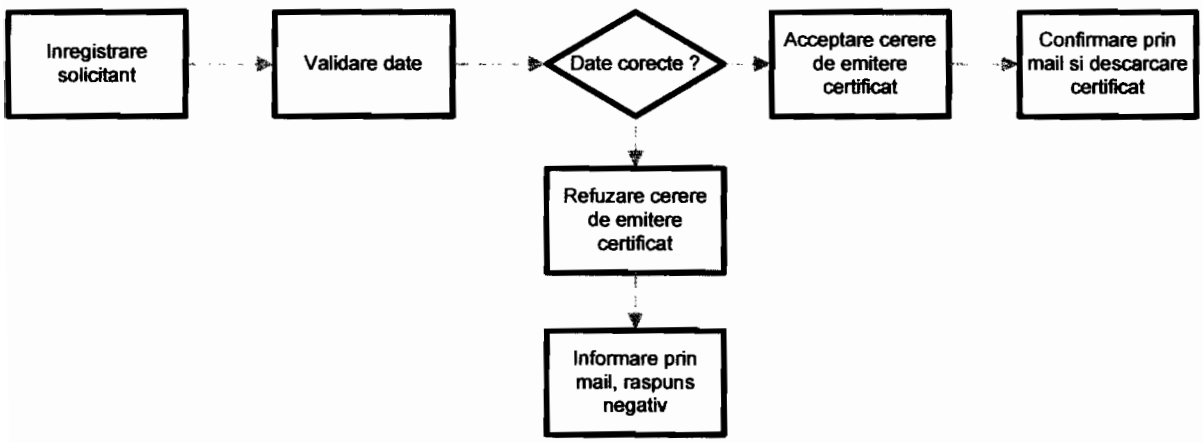

Figura 2.1 Procesul de emitere certificate calificate

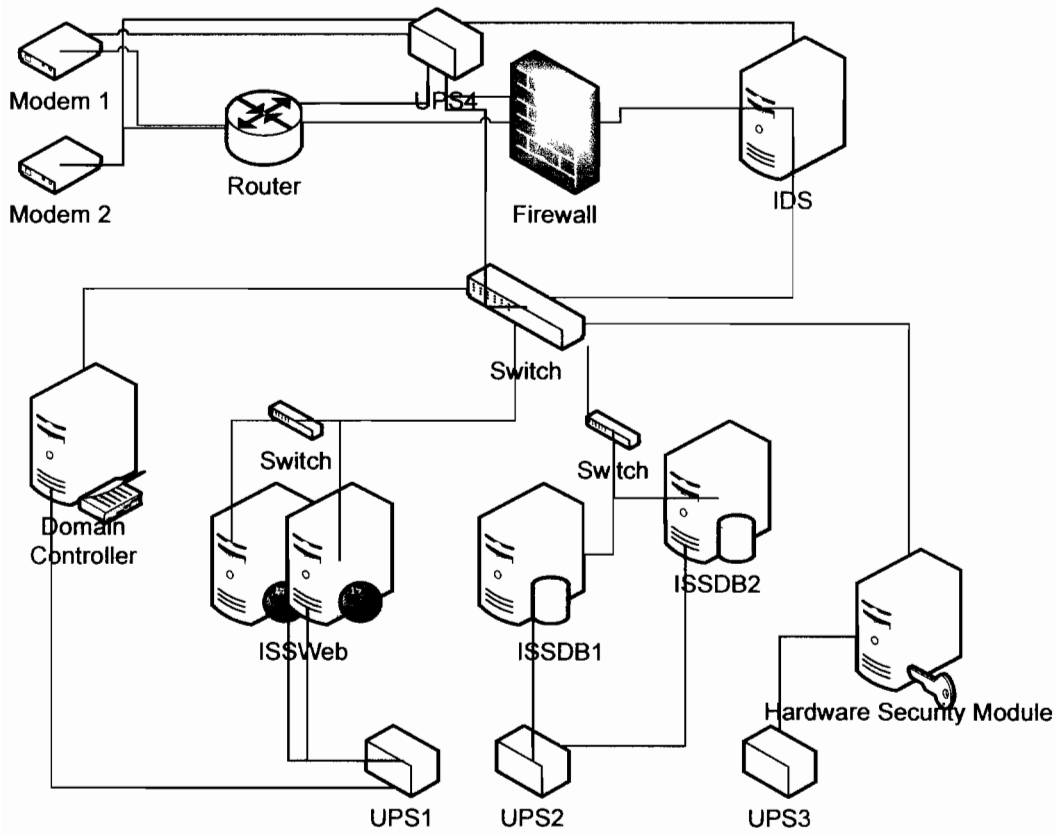

Figura 4.2 Infrastructura autorității de certificare ISS

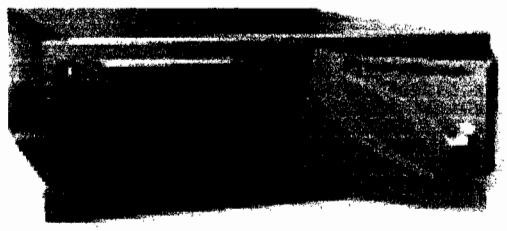

Figura 4.2 Hardware Security Module