



certSIGN®



Calea Șerban Vodă 133
Sector 4, 040205
București, România

Tel.: (40)21 311 99 04
Fax: (40)21 311 99 05
e-mail: office@certsign.ro
www.certsign.ro

Continut site SPENS

PRODUSUL: Serviciu de Posta Electronica Nerepudiabila Securizata cu valoare legala - SPENS

Agentul economic contractor: S.C. CERTSIGN S.R.L.

Partenerii proiectului: Universitatea Politehnica Bucuresti si Academia Tehnica Militara

Perioada de realizare a proiectului: 19.08.2008 - 15.07.2011

Finantarea proiectului asigurata din surse de la bugetul de stat: 405.500 [lei]

Echipa de proiect

Coordonatorul proiectului este agentul economic privat S.C. CERTSIGN S.R.L., cu o vasta experienta in domeniul securitatii informatice si a infrastructurilor de certificate digitale, atat in ceea ce priveste latura stiintifica si de cercetare, latura aplicativa si de implementare, dar si latura de furnizare de servicii de certificare si servicii conexe (OCSP, Time Stamp), servicii de personalizare smartcard-uri pentru tahograful digital. Toate serviciile furnizate de catre compania CERTSIGN folosesc sisteme dezvoltate in totalitate in cadrul companiei in departamentul de cercetare-dezvoltare.

Directorul proiectului, Dr. ing. Armand Ropot, este directorul Departamentului de Cercetare - Dezvoltare in cadrul firmei CERTSIGN. El a coordonat din punct de vedere tehnic mai multe proiecte de cercetare-dezvoltare atat in cadrul CERTSIGN, cat si in cadrul companiei UTI Systems, ambele membre ale grupului UTI.

Academia Tehnica Militara este unul dintre partenerii academici in realizarea proiectului. ATM desfășoară o intensă activitate de cercetare stiintifica fiind implicata activ in granturi sau programe nationale ale Ministerului Educatiei, Cercetarii si Inovarii, cum ar fi: ORIZONT, RELANSIN, MENER, CALIST, VIASAN, MATNANTECH, AEROSPATIAL, SECURITATE, CERCETARE DE EXCELENTA.

Universitatea Politehnica Bucuresti, institutie al carei portofoliu in domeniul cercetarii stiintifice o recomanda ca un partener ideal, este cel de al doilea partener academic implicat in realizarea proiectului.

Descrierea serviciului

Vulnerabilitatea postei electronice din punctul de vedere al securitatii, datorată mediului nesigur pe care mesajele il tranziteaza in drumul de la expeditor la destinatar, reprezinta una dintre problemele actuale ale comunicatiei in rețelele de calculatoare. In ultimii ani s-au gasit o serie de solutii la aceasta problema, unele fiind deja adoptate ca standarde, altele fiind inca obiectul unor largi dezbateri in cercurile stiintifice si in grupurile de lucru din

Internet. Prezentul proiect ofera o solutie acestei probleme si propune implementarea unui serviciu de posta electronica securizata nerepudiabila.

Serviciul de posta electronica securizata nerepudiabila cu valoare legala propus (SPENS) realizeaza transpunerea in mediul electronic a unui serviciu clasic de posta si anume corespondenta cu confirmare de primire.

In serviciile clasice de posta dovezile de expediere si receptionare a scrisorilor sunt realizate prin emiterea catre expeditor a recipiselor si a confirmărilor de primire. Recipisa reprezintă dovada că expeditorul a trimis scrisoarea, iar confirmarea de primire reprezinta dovada ca destinatarul a intrat în posesia scrisorii.

Serviciul propus va actiona ca un tert de incredere intre emitentii si destinatarii mesajelor si va implementa mecanisme de nerepudiere pentru mesajele transmise prin posta electronica astfel incat expeditorul sa nu poata nega trimiterea unui mesaj, iar destinatarul sa nu poata nega primirea acestuia.

In plus, serviciul isi propune sa asigure garantarea momentelor trimiterii si primirii mesajelor, arhivarea mesajelor, garantarea autenticitatii, integritatii si confidentialitatii mesajelor folosind metode criptografice avansate, bazate pe infrastructuri cu chei publice (PKI) si certificate digitale.

Pentru asigurarea valorii legale a serviciului, implicit a mesajelor vehiculate prin intermediul acestuia, vor fi implementate toate prevederile legii Semnaturii Electronice (2001), legii Prelucrării Datelor cu Caracter Personal si Protectiei Vietii Private in Sectorul Comunicatiilor Electronice (2004), Legii Marcii Temporale (2004) si Legii Arhivarii Electronice (2007) cat si a normelor de aplicare corespunzatoare.

Caracteristicile serviciului

Principalele caracteristici ale serviciului deriva din urmatoarele cerinte de business care stau la baza proiectarii sistemului, si anume:

- Garantarea **non-repudierii trimiterii mesajului** de catre expeditor, prin:
 - generarea de dovezi de expediere a mesajelor de catre furnizorul serviciului
 - transferul dovezii de expediere catre partile implicate
 - stocarea de catre furnizorul serviciului a dovezilor de expediere a mesajelor
 - obtinerea dovezilor de la furnizorul serviciului de catre partile implicate
 - furnizarea de mecanisme de verificare a dovezilor de catre furnizorul serviciului
- Garantarea **momentului trimiterii** mesajului prin marcarea temporala a dovezii de expediere
- Garantarea **non-repudierii primirii mesajului** de catre destinatar, prin:
 - generarea de dovezi de primire a mesajelor
 - transferul dovezii de primire catre partile implicate
 - stocarea de catre furnizorul serviciului a dovezilor de primire a mesajelor
 - obtinerea dovezilor de primire de la furnizorul serviciului de catre părțile implicate
 - furnizarea de mecanisme de verificare a dovezilor de catre furnizorul serviciului
- Garantarea **momentului primirii** mesajului prin marcarea temporala a dovezii de primire

- Garantarea **identificării sigure a expeditorului** mesajului pe baza de certificat digital X.509 v3
- Garantarea **identificării sigure a destinatarului** mesajului pe baza de certificat digital X.509 v3
- Garantarea **integrității mesajelor** schimbate între utilizatorii sistemului
- Garantarea **autenticității mesajelor** schimbate între utilizatorii sistemului
- Asigurarea **confidențialității mesajelor** schimbate între utilizatorii sistemului
- Filtrarea mesajelor nedorite – **anti spam**
- **Arhivarea** electronica a mesajelor
- **Jurnalizare** în vederea auditării complete a funcționării serviciului
- **Arhitectura flexibilă și scalabilă** a sistemului dezvoltat pentru implementarea serviciului

Deoarece furnizorul unui astfel de serviciu de poșta electronică nerepudiabilă securizată cu valoare legală acționează ca un tert de încredere, acesta poate fi privit ca o Autoritate Postală Electronică.

Pentru a putea utiliza serviciul, clienții vor trebui să dispună de un certificat digital emis de către o Autoritate de Certificare agreată de către furnizorul serviciului de poșta electronică și să se înregistreze ca și client al serviciului. Înregistrarea utilizatorilor se va realiza prin intermediul unei interfețe web pe conexiune SSL (server side) pentru a asigura confidențialitatea datelor personale ale acestora. Procedura de înregistrare permite accesarea interfețelor de înregistrare ale Autorităților de Certificare agreate de către Autoritatea Postală Electronică, pentru a permite utilizatorilor obținerea facilă a certificatelor digitale necesare.

Mod de utilizarea a serviciului

Serviciul va funcționa după cum urmează:

- I. În cazul în care va folosi interfața web oferită de autoritatea postală electronică, utilizatorul se va autentifica la serviciu folosind certificatul său digital și va compune mesajul într-un mod similar serviciilor web-mail consacrate: yahoo, hotmail, gmail, etc. O altă posibilitate va consta în folosirea unui client clasic de e-mail (Outlook) pentru care va fi instalat în prealabil un plug-in oferit de către furnizorul serviciului.
- II. Mesajul va fi încapsulat într-un mod specific serviciului, semnat digital folosind certificatul digital al expeditorului, după care, în loc să fie trimis direct destinatarului va fi trimis autorității postale electronice, cu informațiile necesare pentru ca aceasta să-l poată trimite la destinatar. Pentru asigurarea confidențialității, mesajul va putea fi criptat.
- III. Autoritatea Postală Electronică va verifica semnătura digitală asociată mesajului primit și structura acestuia. Vor fi acceptate doar mesajele de la expeditori înregistrați în sistem. Primirea mesajului va fi înregistrată într-un jurnal împreună cu marca temporală asociată, garantându-se astfel momentul primirii.
- IV. Expeditorul va fi notificat printr-un e-mail de confirmare ce va conține recipisa de expediție, semnată digital și marcată temporal, asupra înregistrării mesajului de către autoritatea postală electronică.

- V. Serviciul va trimite un e-mail de notificare prin care il va anunta pe destinatar ca a primit un mesaj si ca poate sa-l ridice accesand autoritatea postala electronica.
- VI. Destinatarul se va conecta la interfata web a autoritatii postale electronice folosind o conexiune securizata https si se va autentifica cu certificatul sau digital.
- VII. Pentru a prelua mesajulul destinatarului i se va cere sa semneze digital o recipisa de primire care va identifica in mod unic mesajul. Semnatura acestei recipise de primire va fi marcata temporal pentru a identifica momentul in care a fost primit mesajul. Dupa ce va semna de primire, destinatarul va putea accesa oricand mesajul folosind interfata web a autoritatii postale electronice, il va putea redirectiona spre casuta lui postala, etc.
- VIII. Recipisa de primire semnata digital de catre destinatar si marcata temporal va fi inregistrata in sistem si, in acelasi timp, va fi trimisa prin e-mail expeditorului.

In orice moment, expeditorul va putea verifica daca un mesaj a fost primit de destinatarul sau si momentul de timp la care acesta a fost accesat.

In procedura de autentificare a utilizatorilor, autoritatea postala electronica va verifica starea certificatului fiecarui utilizator care cere permisiunea de acces prin conectarea la un serviciu OCSP (On-line Certificate Status Protocol) care deserveste autoritatile de certificare agreeate de catre autoritatea postala electronica.

Serviciul va permite stocarea criptata a mesajelor garantand astfel confidentialitatea corespondentei electronice. Fiecare utilizator va dispune atat de o cutie postala, cat si de o agenda, ambele configurabile. Expeditorul va putea verifica in ce stare se afla mesajele trimise, iar destinatarul isi va putea descarca mesajele accesand cutia postala personala pe conexiune SSL cu dubla autentificare.

Obiectivele proiectului de cercetare

I. Obiectivul principal al proiectului il constituie proiectarea, dezvoltarea, testarea, implementarea si punerea in functiune a unui serviciu de posta electronica securizata nerepudiabila cu valoare legala. Acest serviciu va realiza transpunerea in mediul electronic a unui serviciu clasic de posta, si anume corespondenta cu confirmare de primire. Serviciul va implementa mecanismul de non-repudiere pentru mesajele transmise prin posta electronica. Scopul este de a garanta faptul ca un e-mail a fost transmis de catre expeditor si a fost primit de catre destinatar fara a mai putea fi negat ulterior acest lucru. In plus, serviciul asigura autenticitatea, integritatea, confidentialitatea si datarea exacta a mesajelor transmise prin posta electronica si ofera si posibilitatea de arhivare a acestora.

II. Furnizorul unui astfel de serviciu poate fi privit ca o Autoritate Postala Electronica. In acest sens, un alt obiectiv este auditarea si acreditarea serviciului oferit.

III. De asemenea, un alt obiectiv il constituie diseminarea rezultatelor cercetarii si prezentarea serviciului oferit prin scrierea de articole si publicarea acestora in reviste de specialitate, prin participarea la conferinte stiintifice nationale si internationale, prin organizarea de workshop-uri si prin publicarea pe site-ul web al CERTSIGN.

Etapele proiectului

Conform planului de realizare, proiectarea, dezvoltarea, testarea, implementarea si punerea in functiune a serviciului de posta electronica securizata nerepudiabila cu valoare legala, cat si raportarea efectelor economice obtinute, se vor desfasura in 5 etape pe parcursul a 34 de luni.

Stadiul actual al proiectului

Stadiul proiectului in momentul de fata este urmatorul:

- **Etapa 1, si anume *Analiza preliminara de sistem a fost finalizata pe data de 30.10.2008.***

Etapa 1 a continut activitatea A I.1: *Analiza preliminara a proceselor ce definesc sistemul*, activitate la care au participat toti cei 3 membri ai consorțiului

- **Etapa 2, si anume *Analiza finala de sistem a fost finalizata pe data de 21.02.2009.***

Etapa 2 contine urmatoarele 4 activitati:

- SubActivitatea A II.1: Analiza proceselor ce definesc sistemul – activitate finalizata pe 15.01.2009 de catre toti cei 3 membri ai consorțiului;
- Activitatea A II.2: Definirea subsistemelor/modulelor componente - activitate finalizata pe 31.01.2009 de catre CERTSIGN, coordonatorul consorțiului;
- Activitatea A II.3: Definirea tehnologiilor folosite pentru realizarea subsistemelor/modulelor - activitate finalizata pe 15.02.2009 de catre CERTSIGN, coordonatorul consorțiului;
- Activitatea A II.4: Studiu de fezabilitate a sistemului - activitate coordonata de catre CERTSIGN, coordonatorul consorțiului, si realizata de catre S.C. E-SECURITY CONSULT S.R.L. - activitate finalizata pe 19.02.2009.

- **Etapa 3, si anume *Proiectarea, realizarea si testarea sistemului a fost finalizata in data de 15.06.2010.***

Etapa 3 contine urmatoarele 12 activitati:

- Activitatea A III.1: Stabilirea cerintelor pentru modelul experimental-documentul de prezentare a rezultatelor este “Caietul de sarcini pentru modelul experimental”;
- Activitatea A III.2: Proiectarea de detaliu a modulelor sistemului si a interfetelor dintre acestea- rezultatul acestei activitati il reprezinta “Proiectarea de detaliu a subsistemelor: SDD, DBDD”
- Activitatea A III.3: Proiectarea testarii sistemului -documentul de prezentare a rezultatelor este “Planul de testare si descrierea testelor sistemului si a subsistemelor: STP, STD”
- Activitatea A III.4: Dezvoltarea si testarea modulelor software ale sistemului - rezultatul acestei activitati il reprezinta “Totalitatea modulelor software ale sistemului, testate”
- Activitatea A III.5: Integrarea modulelor software in sistemul experimental –rezultatul acestei activitati il reprezinta “Modelul experimental”

- Activitatea A III.6: Elaborarea documentatiei de implementare, punere in functiune, administrare si utilizare a serviciului - rezultatul acestei activitati il reprezinta “Manualele de instalare, configurare, administrare si utilizare a sistemului”
 - Activitatea A III.7: Testarea functionala, de performanta si de securitate a modelului experimental si corectarea eventualelor probleme. Acceptanta interna -documentul de prezentare a rezultatelor este “Raport de testare sistem (STR)”
 - Activitatea A III.8: Transferul tehnologic. Diseminarea rezultatelor in cadrul unor workshopuri- documentul de prezentare a rezultatelor este “ Procesul verbal de transfer tehnologic si Ordinul de organizare al serviciului. Workshop de prezentare a sistemului experimental”
 - Activitatea A III.9: Lansarea publica a serviciului-rezultatul acestei activitati il reprezinta “Serviciul operational pentru public”
 - Activitatea A III.10: Mediatizarea serviciului si diseminarea rezultatelor-rezultatul acestei activitati il reprezinta “Activitatile de marketing, comunicari stiintifice si workshopuri”
 - Activitatea A III.11: Auditarea si acreditarea serviciului-rezultatul acestei activitati il reprezinta “Raportul de audit si certificatul de acreditare”
 - Activitatea A III.12: Inregistrarea drepturilor de autor la ORDA. Introducerea în Registrul special de evidență a rezultatelor activităților de cercetare – dezvoltare- rezultatul acestei activitati il reprezinta “Certificat ORDA. Extras din Registrul special de evidență a rezultatelor activităților de cercetare – dezvoltare”
- ***Etapa 4 - Raportarea efectelor economice obținute de către agentul economic beneficiar, ca urmare a utilizării serviciului este în derulare, data estimată de finalizare fiind 15.07.2011***