USIGN - SISTEM AUTONOM DE SEMNĂTURI ELECTRONICE

Cristian JEVERDAN[1*], Elvira DAVID[2], Bogdan GALAȚAN[2], Vlad TROHIN[2]

[1]Departamentul Telecomunicații și Sisteme Electronice, grupa IMTC-221,
Facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei, Chișinău, Rep. Moldova
[2]Departamentul Telecomunicații și Sisteme Electronice, grupa RST-221,
Facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei, Chișinău, Rep. Moldova

*Autorul corespondent: Cristian Jeverdan, cristian.jeverdan@tse.utm.md

Îndrumător/coordonator științific: **DOROGAN Andrei**, dr., l. univ., FET, UTM.

Rezumat. *Usign reprezintă un sistem autonom de semnături electronice, cu scopul principal de a eficientiza și a conferi independență față de alte sisteme de semnături electronice oricărei organizații ce operează cu un volum mare de documente și își dorește să optimizeze cheltuielile, evitând astfel costurile asociate fiecărei semnături. Documentele semnate cu Usign sunt securizate cu cele mai avansate tehnologii criptografice, iar accesul la semnătură este posibil doar cu cunoașterea unei parole unice de către semnatar.*

Cuvinte cheie: *usign, semnătură electronică, tehnologii criptografice, securitate*

Introducere

Proiectul Usign a avut ca obiectiv elaborarea unui sistem informatic software autonom, securizat și flexibil, destinat aplicării semnăturilor digitale pe documente digitale și verificării autenticității acestora de către utilizatorii unei entități economice [1]. Creatorii platformei au urmărit dezvoltarea unui sistem software robust, care să faciliteze emisia automatizată a semnăturilor electronice pentru utilizatorii autorizați, implementarea unui sistem de administrare a certificatelor digitale pentru o gestionare eficientă a semnăturilor, respectarea standardelor tehnice de securitate privind semnătura electronică.

Proiectul a inclus și asigurarea unei verificări facile a autenticității semnăturilor electronice aplicate documentelor PDF, utilizarea tehnicilor criptografice avansate pentru garantarea integrității documentelor și prevenirea falsificării după semnare, facilitarea utilizării semnăturii electronice de pe diverse dispozitive, atât fixe cât și mobile, și oferirea unei interfețe intuitive și ușor de utilizat pentru toți utilizatorii.

Structura sistemului Usign

Sistemul de semnături electronice Usign se distinge prin competitivitate și eficiență, fiind conceput pentru a funcționa independent în cadrul unei entități economice. Este complet autonom și nu depinde de alți furnizori de servicii, precum sistemul guvernamental "Msign". Semnătura este gratuită, semnatarul nefiind obligat să plătească pentru fiecare semnătură în parte și neavând nicio limitare în numărul de documente pe care le poate semna cu semnătura sa aprobată. Un avantaj crucial al sistemului Usign este accesibilitatea acestuia prin intermediul unei pagini web, ceea ce oferă mobilitate sistemului fără a compromite nivelul înalt de securitate.

Structural, Usign este divizat în două componente majore, care, în simbioză, formează sistemul nostru de semnături electronice securizat. Prima parte a platformei este cea pentru utilizatori, fiind cea mai simplă și intuitivă. Aici au acces toți utilizatorii prin intermediul oricărui browser, accesând adresa URL: usign.ddns.net. Utilizatorul are posibilitatea de a alege între două funcții esențiale ale platformei, "Semnează" sau "Verifică", afișate pe pagina principală a site-ului web (fig.1).

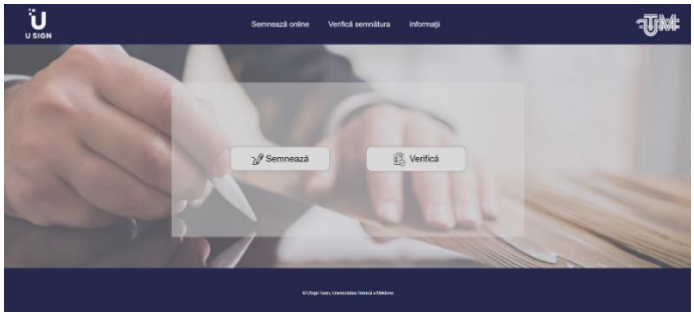


Figura 1. Pagina principală a site-ului web Usign

Accesând butonul "Semnează", utilizatorul va fi redirecționat către o altă pagină, unde îi vor fi propuși 3 pași esențiali și simpli, ce vor rezulta în semnarea fișierului PDF introdus și ulterior va verifica veridicitatea documentului. Primul pas constă în selectarea fișierului PDF ce urmează să fie semnat, al doilea pas presupune alegerea fișierului cu extensia .p12, în care se regăsește certificatul digital cu ajutorul căruia va fi semnat documentul ales, iar al treilea pas implică introducerea parolei unice, cu care va fi posibilă citirea containerului PKCS-12 [2]. După finalizarea acestor pași, utilizatorului îi rămâne doar opțiunea de a accesa butonul "SEMNEAZĂ". Astfel, dacă semnătura este înregistrată în baza de date și parola este corectă, documentul va fi semnat cu succes. Toate aceste etape sunt reprezentate în (fig.2).

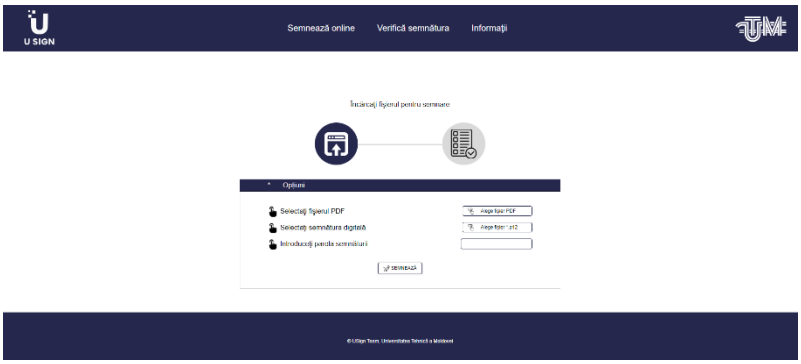
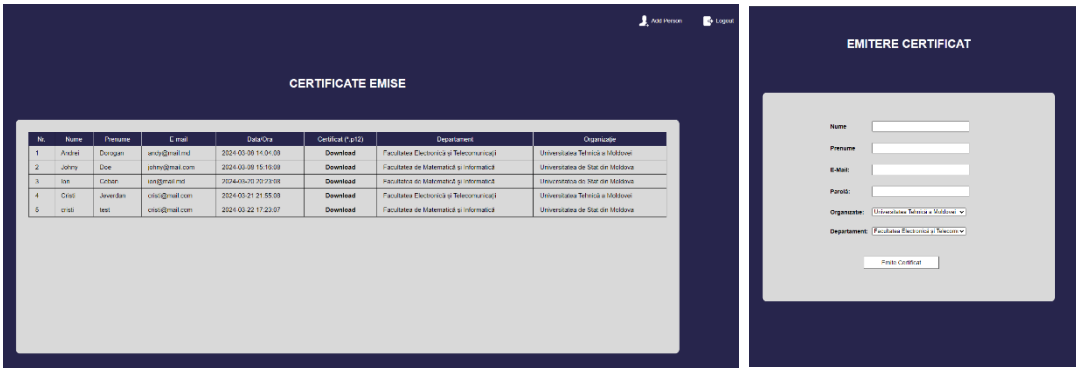


Figura 2. Pagina pentru semnarea documentului

A doua parte a platformei este secțiunea de administrare, accesibilă doar utilizatorilor cu privilegii speciale prin intermediul adresei URL: usign.ddns.net/admin. Aici se găsește lista certificatelor emise destinate utilizatorilor sistemului. Pentru acces, se introduc numele utilizatorului și parola. După autentificarea persoanei cu acces privilegiat, interfața de administrare afișează un tabel cu certificatele emise. Acesta conține informații precum numele, prenumele, adresa de email, departamentul și organizația persoanei pentru care a fost emis certificatul, precum și data și ora emiterii acestuia. Administratorul are posibilitatea de a descărca certificatul în format p12 (fig.3, a).

Prin apăsarea butonului "Add Person", administratorul este redirecționat către pagina cu formularul destinat emiterii certificatului. Aici se completează informațiile referitoare la nume, prenume, email, departament și organizație. Pentru crearea certificatului, este necesară introducerea unei parole unice pentru utilizator, care va fi folosită pentru semnarea documentelor PDF. După completarea datelor, administratorul validează emiterea certificatului. În decurs de 1 minut, certificatul poate fi descărcat și distribuit persoanei căreia i-a fost emis (fig.3, b).



a) b)

Figura 3. a) Pagina cu certificatele emise; b) Formular pentru emiterea certificatului

Standardul PKCS12

PCKS12 este unul dintre standardele din familia Public-Key Cryptography Standards (PKCS). Este un fișier de tip container criptat, unde se păstrează cheia privată, cheia publică și certificatul utilizatorului, care conține informație despre autoritatea eminentă a certificatului. Acest fișier este folosit pentru semnarea documentelor PDF. Stochează și transportă securizat cheia privată, care este partea componentă a certificatului utilizatorului. Semnătura digitală este obținută prin folosirea cheii private a platformei sursă. Verificarea semnăturii se realizează prin utilizarea cheii publice a destinatarului pe platformă. Cheia privată se află doar la utilizator și este utilizată înainte de semnarea informațiilor personale. Usign folosește algoritmul de criptare RSA-SHA256.

Pentru semnarea unui document, sistemul software calculează un rezumat al conținutului PDF, adică un hash, și apoi criptează rezumatul cu ajutorul cheii private a utilizatorului care semnează, formând astfel semnătura digitală. Această semnătură digitală este atașată la conținutul fișierului PDF. În faza verificării semnăturii, sistemul software formează un hash din conținutul primar al PDF-ului (fără semnătură), decriptează semnătura digitală din conținutul fișierului încărcat folosind cheia publică și obține un alt hash. Dacă cele două hash-uri obținute sunt identice, semnătura este considerată validă.

Avantajele implementării semnăturii electronice

Semnăturile electronice sunt o componentă esențială a securității cibernetice, oferind o modalitate de a verifica autenticitatea și integritatea mesajelor sau documentelor digitale. Ele joacă un rol crucial în consolidarea securității cibernetice prin asigurarea integrității datelor, verificarea autenticității expeditorului, nerepudierea și protecția datelor.

Autentificare: Semnăturile electronice leagă identitatea unei persoane de un mesaj sau document, garantând că acesta provine de la sursa revendicată. Aceasta este o formă sigură de identificare, similară cu o semnătură scrisă de mână pe un document fizic.

Integritate: Semnăturile electronice garantează că conținutul unui mesaj sau document nu a fost modificat în timpul transmiterii. Dacă conținutul este modificat după aplicarea semnăturii electronice, semnătura devine invalidă, alertând destinatarul că datele pot fi compromise.

Nerepudiere: Semnăturile electronice oferă o modalitate de a dovedi că un mesaj sau document a fost trimis sau aprobat de către expeditor. Odată ce o semnătură electronică este aplicată, expeditorul nu poate nega ulterior că a trimis mesajul sau a aprobat documentul. Acest lucru este deosebit de important pentru contractele și acordurile electronice sensibile.

Protecția datelor: Semnăturile electronice contribuie la protejarea informațiilor sensibile împotriva accesului neautorizat, modificării sau falsificării. Ele stabilesc încrederea în comunicațiile digitale prin verificarea autenticității și integrității schimbului de date.

În plus față de consolidarea securității cibernetice, semnăturile electronice aduc o serie de beneficii suplimentare:

- *Eficientizarea activității:* Semnăturile electronice reduc semnificativ utilizarea documentelor fizice, accelerând fluxurile de lucru și optimizând procesele interne. Aceasta duce la o îmbunătățire a eficienței operaționale și a productivității.
- *Promovarea sustenabilității:* Prin reducerea semnificativă a consumului de hârtie, semnăturile electronice contribuie la diminuarea indirectă a amprentei de carbon. Acest lucru este în concordanță cu obiectivele de dezvoltare durabilă și de protecție a mediului.
- *Creșterea productivității:* Semnătura electronică este mobilă și poate fi utilizată pe diferite platforme, sporind viteza de procesare a documentelor. Îmbunătățește comunicarea internă și externă și eliberează timp prețios al angajaților pentru alte sarcini importante.
- *Beneficii financiare:* Semnăturile electronice ajută la reducerea costurilor operaționale ale entităților economice prin optimizarea resurselor umane. De asemenea, ele pot crește satisfacția utilizatorilor, ceea ce poate duce la o creștere a loialității clienților și a rentabilității.

Concluzii

Eliminând dependența de alte sisteme de semnături electronice, Usign oferă organizațiilor independența necesară pentru a funcționa la capacitate maximă. Accelerând fluxurile de lucru și optimizând procesele interne, acest sistem contribuie la reducerea semnificativă a consumului de hârtie, promovând astfel sustenabilitatea și diminuând amprenta de carbon. Sistemul dat nu doar îmbunătățește eficiența și optimizează procesele, ci și îmbunătățește comunicarea internă și externă, eliberând timp valoros al angajaților pentru alte sarcini critice. Semnăturile electronice aplicate prin Usign sunt absolut gratuite, reducând astfel costurile operaționale ale organizațiilor. În plus, documentele semnate cu Usign sunt securizate folosind tehnologii avansate criptografice, asigurând autenticitatea și integritatea mesajelor sau documentelor digitale.

Usign reprezintă mai mult decât un simplu sistem de semnături electronice. El este un instrument puternic care transformă modul în care organizațiile gestionează și securizează documentele lor. Interfața sa intuitivă face ca procesul de semnare a documentelor să fie rapid și simplu, chiar și pentru cei neinițiați în tehnologie, făcându-l util pentru organizațiile de toate dimensiunile, de la întreprinderile mici până la corporațiile mari. Adoptarea și implementarea Usign pot aduce beneficii semnificative pentru orice organizație interesată să își îmbunătățească eficiența, sustenabilitatea, productivitatea și securitatea proceselor sale.

Referințe

[1] https://www.ibm.com/docs/en/ibm-mq/9.1?topic=tls-digital-signatures-in-ssltls (Definiția semnăturii digitale).
[2] https://ru.wikipedia.org/wiki/PKCS12 (Definiția containerului PKCS-12).
[3] https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/ (Definiția certificatului SSL).