**ROMÂNIA**

**MINISTERUL APĂRĂRII NAŢIONALE**

**ACADEMIA TEHNICĂ MILITARĂ**

**„Ferdinand I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Securitate Tehnologiei Informației**



**Solutie client pentru interogarea si analiza de informatii EUTL**

COORDONATOR ȘTIINȚIFIC: ABSOLVENT:

**Col. Prof. univ. Dr. Ing. Mihai TOGAN Slt. Ing. Alin-Romeo TUDOSE**

Conține \_\_\_\_\_\_\_\_\_\_\_ file Inventariat sub nr. \_\_\_\_\_\_

Poziția din indicator: \_\_\_\_

Termen de păstrare:\_\_\_\_\_

**BUCUREȘTI**

**2023**

PAGINA ALBA

PAGINĂ ALBĂ

PAGINĂ ALBĂ

PAGINĂ ALBĂ

PAGINĂ ALBĂ

# ABSTRACT

# REZUMAT

**Cuprins**

[ABSTRACT 6](#_Toc126503115)

[REZUMAT 7](#_Toc126503116)

[LISTĂ ABREVIERI 10](#_Toc126503117)

[LISTĂ FIGURI 11](#_Toc126503118)

[1. INTRODUCERE 12](#_Toc126503119)

[1.1. Importanța și actualitatea problematicii abordate 12](#_Toc126503120)

[1.2. Scopul și obiectivele proiectului 13](#_Toc126503121)

[1.3. Structura proiectului pe capitole 13](#_Toc126503122)

[2. STADIUL CUNOAȘTERII ÎN DOMENIU 14](#_Toc126503123)

[2.1. Fundamente teoretice 14](#_Toc126503124)

[2.1.1.Semnături și certificate digitale 14](#_Toc126503125)

[2.1.2.Standardul eIDAS 15](#_Toc126503126)

[2.1.3.Liste de Încredere 16](#_Toc126503127)

[2.1.4.Listele de Încredere ale Uniunii Europene (EUTL) 19](#_Toc126503128)

[2.2. Soluții și abordări similare 19](#_Toc126503129)

[2.2.1.Aplicația oficială a Comisiei Europene [6] 19](#_Toc126503130)

[2.2.2.Implementare în Python de către dl. George Gugulea, Director Cercetare și Inovare, CertSIGN [7] 20](#_Toc126503131)

[3. IMPLEMENTAREA APLICAȚIEI 21](#_Toc126503132)

[3.1. Descrierea proiectului 21](#_Toc126503133)

[BIBLIOGRAFIE 22](#_Toc126503134)

# LISTĂ ABREVIERI

|  |  |  |
| --- | --- | --- |
| **Nr. Crt** | **Abreviere** | **Forma completă** |
| 1. | UE | Uniunea Europeană |
| 2. | PKI | Public Key Infrastructure (Infrastructură cu chei publice) |
| 3. | LOTL | List of Trusted Lists (Lista listelor de încredere) |
| 4. | TL | Trusted List (Listă de încredere) |
| 5. | EUTL | European Union Trusted List (Liste de Încredere ale Uniunii Europene) |
| 6. | TLSO | Trusted List Scheme Operator (Operatorul schemei de liste de încredere) |
| 7. | TSP | Trusted Service Provider (Furnizor de servicii criptografice de încredere) |
| 8. | TS | Trusted Service (Serviciu criptografic de încredere) |
| 9. | DSS | Digital Signature Service (Serviciul de semnături digitale), librărie Java oferită de Comisia Europeană |

# LISTĂ FIGURI

[Figura 1 - Structura unei liste de încredere [4] 17](#_Toc126503196)

CAPITOLUL I

# INTRODUCERE

## Importanța și actualitatea problematicii abordate

Nevoia de securitate este o constantă a lumii moderne, în care tot mai multe sarcini umane sunt preluate de către calculator. Informațiile comunicate de sistemele informatice sunt din ce mai sensibile, iar compromiterea acestora poate genera daune foarte mari de ordin financiar în organizațiile civile sau vulnerabilități de securitate națională în organizațiile militare.

Pentru prevenirea scurgerilor de informații, sau modificarea ilicită a documentelor de importanță crescută, au fost adoptate pe scară largă servicii criptografice care au scopul de a ascunde datele transmise între două entități, precum și de a garanta integritatea și autenticitatea acestora, folosind mecanisme criptografice precum criptarea, semnăturile digitale și certificatele digitale.

Desigur, în utilizarea certificatelor și a semnăturilor digitale apare o mare întrebare. Cum putem avea încredere că un certificat este valid, și că entitatea care deține acel certificat este cine spune că este? Pentru a rezolva acest impediment, au fost implementate scheme de certificate diferite, precum Web of Trust, sau PKI.

În implementarea schemei PKI, certificatele digitale sunt emise și gestionate de către terțe părți specializate, care sunt marcate ca puncte de încredere în sistemul folosit. Cu alte cuvinte, nu se rezolvă complet problema încrederii, deoarece trebuie să avem încredere *„oarbă”* în acele terțe părți.

Așadar, pentru a aduce un plus de securitate schemei, a fost introdusă componenta legislativă în cadrul schemelor de securitate, de către un corp autorizat de reglementare, și anume Comisia Europeană. Aceasta certifică furnizorii de servicii de securitate care oferă servicii conforme cu standardul eIDAS, din spațiul Uniunii Europene, precum și al Spațiului Economic European.

## Scopul și obiectivele proiectului

Proiectul își propune realizarea unei soluții software ce va realiza extragerea informațiilor din Lista listelor de încredere (LOTL), emisă de Comisia Europeană, precum și a celor din fiecare listă de încredere (TL), emise de entitățile autorizate din fiecare stat membru UE, numiți și operatori ai schemei de liste de încredere (TLSO), și prezentarea acestora către utilizatori. Printre datele prezentate se pot regăsi : lista țărilor participante, furnizorii autorizați de servicii criptografice (TSP) ce își desfășoară activitatea într-o anumită țară, și serviciile criptografice (TS) puse la dispoziția publicului de către un furnizor, împreună cu tot istoricul de certificare al acestuia.

În plus, aplicația software realizată va pune la dispoziția utilizatorilor opțiunile de validare a semnăturilor și a certificatelor digitale, furnizând informații despre nivelul lor de calificare, statutul de validare, precum și alte informații specifice acestora.

## Structura proiectului pe capitole

În capitolul II se definesc noțiunile teoretice necesare pentru înțelegerea funcționării infrastructurii bazate pe liste de încredere, explicând ce reprezintă standardul eIDAS, listele de încredere, precum și noțiuni criptografice de bază.

Capitolul III descrie organizarea aplicației pe componente, și prezintă succint modul de lucru și implementarea fiecăreia dintre acestea, făcând și o parcurgere rapidă a funcționalităților aplicației din punctul de vedere al utilizatorului.

Capitolul IV prezintă rezultatele și comportamentul aplicației, precum și o lista de puncte slabe ale acesteia.

Capitolul V descrie îmbunătățirile ce pot fi aduse aplicației, utilitatea adusă de către aceasta și concluziile proprii legate de dezvoltarea aplicației.

CAPITOLUL II

# STADIUL CUNOAȘTERII ÎN DOMENIU

## Fundamente teoretice

Operațiile criptografice ce se pot efectua asupra datelor sunt de mai multe tipuri, printre ele regăsindu-se criptarea, semnarea, hash-uirea și marcarea temporală a datelor.

### Semnături și certificate digitale

O semnătură digitală este o schemă matematică folosită pentru a demonstra autenticitatea mesajelor sau documentelor digitale. O semnătură digitală validă oferă destinatarului o bază solidă pentru a crede că mesajul a fost creat de către un expeditor cunoscut (autentificare), să fie sigur că expeditorul nu poate nega că a trimis mesajul (non-repudiere), și că mesajul nu a fost modificat pe parcurs (integritate) [1].

O schemă de semnătură digitală este formată din 3 algoritmi:

* Un algoritm de generare a cheilor care alege o cheie privată uniform aleatoare⁠ dintr-un set de chei private posibile. Algoritmul produce la ieșire cheia privată împreună cu o cheie publică corespunzătoare.
* Un algoritm de semnare care, atunci când i se prezintă un mesaj și o cheie privată, produce o semnătură.
* Un algoritm de verificare a semnăturii care, primind mesajul, cheia publică și semnătura, poate accepta sau respinge mesajul în raport cu autenticitatea sa.

Certificatele digitale folosite în infrastructura PKI, conțin informații despre deținător, printre care și cheia publică, care poate fi folosită pentru validarea semnăturilor emise de către acesta. Rolul principal al certificatelor, încă de la apariția acestora a fost să asigure apartenența cheii publice unei anumite entități.

### Standardul eIDAS

eIDAS (electronic IDentification, Authentication and trust Services) reprezintă un set de reglementări europene asupra serviciilor criptografice folosite pentru tranzacții electronice în piața unică europeană [2]. Mai exact, acesta reglementează semnăturile electronice, tranzacțiile electronice și procesele de încorporare a acestora pentru a oferi un mod sigur pentru utilizatori să desfășoare activități online, precum transferuri de fonduri sau servicii. Atât semnatarul, cât și recipientul pot avea mai multă încredere și securitate. În loc să se bazeze pe metode tradiționale, precum poșta, sau întâlnirile față în față pentru a schimba documente fizice, acum pot folosi tranzacții la distanță.

eIDAS a creat standarde pentru semnături și sigilii electronice, certificate digitale calificate, timestamp-uri și alte mecanisme de autentificare prin care tranzacțiile electronice au aceeași calitate legală precum tranzacțiile fizice, semnate pe hârtie [3]. Acesta a fost implementat în iulie 2015, și toate statele membre EU sunt obligate să recunoască legal semnăturile electronice care respecta standardele eIDAS.

Obiectivele eIDAS sunt să împingă spre inovație. Respectând regulile impuse de eIDAS, organizațiile pot să atingă un nivel mult mai mare de securitate informatică. În plus, eIDAS se focusează pe interoperabilitate și transparență, astfel încât statele membre trebuie să creeze un framework comun care va recunoaște identități electronice (eIDs) din alte state membre, și să poată să asigure autenticitatea si securitatea acestora, și să întocmească TL-uri ce specifică serviciile acreditate care pot fi folosite în acest framework.

eIDAS impune ca toate semnăturile electronice calificate să aibă aceeași valoare ca o semnătură olografă.

Serviciile de încredere acoperite de eIDAS sunt următoarele:

* Semnături avansate și calificate asociate persoanelor fizice și juridice;
* Sigilii avansate și calificate asociate persoanelor juridice;
* Validare calificată pentru semnături și sigilii electronice calificate;
* Conservare calificată pentru semnături și sigilii electronice calificate;
* Marcare temporală;
* Servicii de poștă electronică;
* Autentificarea website-urilor;

### Liste de Încredere

Listele de încredere sunt liste care oferă informații despre statusul serviciului de încredere oferit de un furnizor de servicii de încredere, precum și despre istoricul acestuia, în conformitate cu cerințele aplicabile și legislația în vigoare.

Așadar, TL-urile fac posibil pentru orice entitate să determine dacă un serviciu de încredere operează în prezent, sau a operat într-un moment de timp din trecut, în conformitate cu cerințele aplicabile. Pentru a îndeplini această cerință, TL-urile trebuie să includă informații care să poată stabili dacă un furnizor de servicii de încredere este, sau a fost, cunoscut de către autoritatea care emite lista de încredere. Deci, TL-urile trebuie să conțină atât statusul curent al serviciului, cât și istoricul acestora.

Fiecare stat membru al UE își emite propria TL. Pentru a putea verifica statusul oricărui serviciu de încredere, și a oferi acces către toate listele de încredere, Comisia Europeană emite o listă centralizată ce specifică locațiile (URI-ul) unde sunt publicate toate listele de încredere. Această listă centralizată este denumită Lista Listelor de Încredere, și este publicată atât în clar, cât și în format XML pentru procesare automată de programe.

LOTL are un rol foarte important, pe lângă localizarea fiecărui TL. Fiecare stat membru își semnează lista de încredere în momentul publicării de către operatorul schemei de încredere, iar certificatul necesar validării acestei semnături este inclus în LOTL, după notificarea Comisiei Europene. Autenticitatea și integritatea formatului XML al LOTL este asigurată de o semnătură electronică calificată sau de un sigiliu electronic calificat, efectuate cu un certificat calificat care poate fi autentificat și beneficiază de încredere prin una din publicațiile Jurnalului Oficial al Uniunii Europene.

Listele de încredere conțin 4 componente cu rolul de a:

* Oferi informații despre schema de emitere;
* Identifica furnizorii de servicii de încredere recunoscuți;
* Identifica serviciile oferite de către fiecare furnizor de servicii, tipul și statusul curent al acestora;
* Indica, pentru fiecare serviciu, istoricul statusului.

Structura detaliată se poate observa în Fig. 1, mai jos:

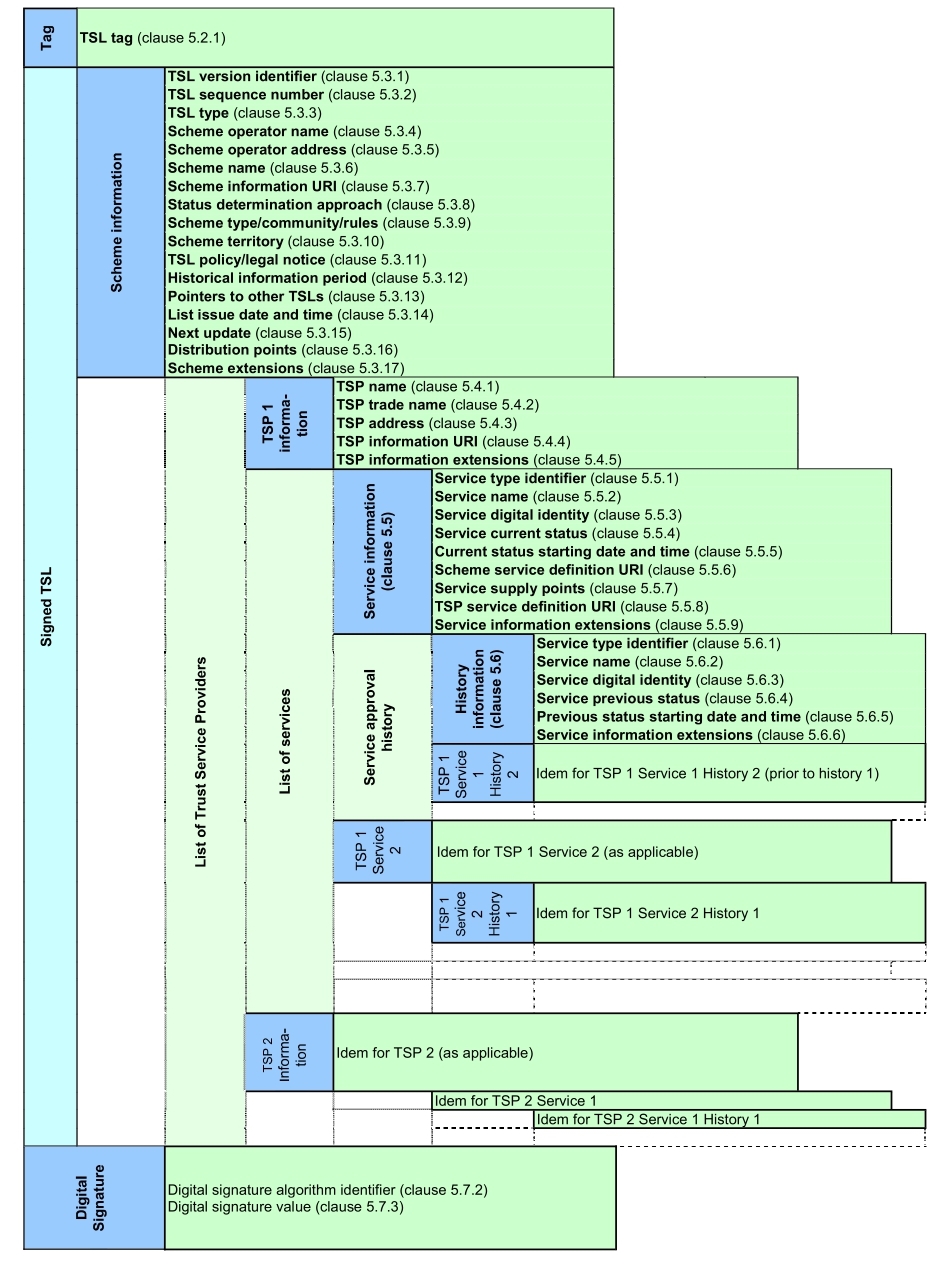


Figura 1 - Structura unei liste de încredere [4]

### Listele de Încredere ale Uniunii Europene (EUTL)

EUTL constituie liste publice de peste 200 de furnizori de servicii de încredere, activi sau care și-au sistat activitatea, care sunt în mod specific acreditați să ofere servicii de încredere în conformitate cu standardul UE eIDAS. Acești furnizori oferă certificate digitale pentru identificare, servicii de marcare temporală, ce pot fi folosiți pentru a crea semnături electronice calificate. Conform standardului eIDAS, doar semnăturile calificate sunt, în mod legal, echivalente cu semnăturile olografe, și sunt singurele semnături recunoscute în tranzacții între două state membre ale Uniunii Europene.

## Soluții și abordări similare

### Aplicația oficială a Comisiei Europene [6]

O soluție deja implementată o putem găsi pe site-ul oficial al Comisiei Europene: <https://esignature.ec.europa.eu/efda/tl-browser>. Aplicația web pune la dispoziție utilizatorului o formă interpretabilă a LOTL-ului, de unde se poate accesa TL-ul fiecărui stat membru. Accesând lista oricărui stat membru, ne sunt prezentate informații suplimentare despre furnizorii de servicii de încredere care își desfășoară activitatea în statul respectiv, serviciile pe care le oferă, informații de identificare, incluzând certificatele digitale ale fiecărui serviciu, precum și statusul curent și istoricul statusului de acreditare pentru fiecare dintre aceste servicii.

Validarea LOTL-ului, și a fiecărui TL este făcută de către un serviciu REST separat, independent de accesarea paginilor de către utilizator. La accesarea paginilor, serviciul REST livrează utilizatorului în browser informațiile dorite.

### Implementarea dl. George Gugulea, Director Cercetare și Inovare, CertSIGN [7]

Aplicația este un utilitar în linie de comandă, scris in Python ce oferă 3 funcționalități:

* Descărcarea și validarea listelor de încredere;
* Extragerea din fiecare TL a certificatelor fiecărui furnizor de servicii de încredere;
* Extragerea, pentru fiecare furnizor, a serviciilor oferite, precum și statusul curent și istoricul statusului acestora.

Aplicația este disponibilă pe site-ul : <https://github.com/authone/eutl-parser>.

CAPITOLUL III

# IMPLEMENTAREA APLICAȚIEI

## Descrierea proiectului

Împărțind cerința proiectului în subprobleme ce pot fi rezolvate mai ușor, putem distinge următoarele 3 direcții de dezvoltare:

* Componenta UI – cu rolul de a pune informațiile cerute într-o formă prezentabilă, și de afișa utilizatorului;
* Componenta de extragere – cu rolul de a valida și a extrage informațiile din TL/LOTL și, mai apoi, să le trimită către componenta UI.
* Componenta de validare – cu rolul de a valida semnăturile sau certificatele oferite de utilizator.

Astfel, utilizatorul interacționează doar cu componenta UI, către care face cereri, iar componenta UI, în funcție de cererile utilizatorului, le trimite către componenta de extragere sau componenta de validare, în funcție de tipul cererii, preia răspunsurile de la acestea, și le afișează utilizatorului.

Interacțiunile dintre componente și utilizator pot fi observate în diagrama de mai jos:

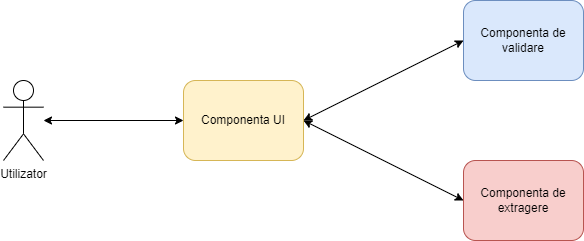


Figura 2 - Interacțiunea componentelor

Cele 3 componente vor fi scrise în limbajul de programare Java.

## Componenta de extragere

Componenta de extragere este reprezentată de un serviciu REST. Cerințele acestei componente sunt următoarele:

* Accesează periodic serverul de resurse al Comisiei Europene, folosind URL-ul oficial pentru accesarea LOTL-ului, pentru a obține documentul în format XML, execută validarea semnăturii asupra acestuia, extrage informațiile prezente în LOTL, și le adaugă în memoria cache internă, împreună cu rezultatul validării, precum și alte indicații;
* Accesează serverul fiecărui TLSO la cerere, folosind URL-ul extras din LOTL, pentru a obține documentul ce conține TL-ul cerut în format XML, execută validarea semnăturii asupra acestuia, extrage prezente in TL, și le adaugă în memoria cache internă, împreuna cu rezultatul validării, precum și alte indicații;
* Primește de la componenta UI cereri pentru LOTL, și transmite ca răspuns informațiile prezente în memoria cache.
* Primește de la componenta UI cereri pentru TL-ul asociat unui stat membru, și transmite ca răspuns informațiile acestuia prezente în memoria cache.

Serviciul REST implementat este scris în Java, folosind SpringBoot Framework. De asemenea, din cauza complexității și rigurozității necesare validării semnăturilor prezente în cadrul LOTL și al oricărei TL aferente statelor membre, Comisia Europeană a implementat o librărie ce facilitează validarea semnăturilor digitale. Librăria este numită Digital Signature Service (DSS), și a fost folosită atât în cadrul componentei de extragere, cât și în cadrul componentei de validare.

Toate informațiile extrase atât prin parcurgerea LOTL, cât și a oricărui TL, sunt introduse în memoria cache internă aplicației. Practic, serviciul REST trimite către componenta UI rezultatele aflate numai și numai în memoria cache, și niciodată rezultate obținute direct. Mecanismul de cache-uire a datelor se asigură ca nu apar probleme de tipul accesului concurențial la date, folosind mecanisme de sincronizare (mutex), și, odată ce datele au fost introduse în memorie, acestea au un timp de expirare de 10 minute. După expirarea datelor, la următoarea accesare, acestea sunt marcate ca fiind invalide, iar procesul de extragere este reluat.

### Validarea și extragerea informațiilor din LOTL

LOTL este lista oficială ce conține adresele web pentru accesarea tuturor celorlalte liste de încredere asociate fiecărui stat membru. Aceasta listă este emisă de către Comisia Europeană, o dată la maxim 6 luni, și este semnată digital pentru a proteja datele prezente.

## Componenta UI

Deoarece dezvoltarea aplicațiilor web ia o amploare din ce în ce mai mare, și datorită mai multor considerente precum independența față de platforma utilizată, ușurința de accesare, etc., am decis că este oportună implementarea unei interfețe web pentru componenta UI.

# BIBLIOGRAFIE

1. Wikipedia, Semnătură Digitală, Accesibil: <https://ro.wikipedia.org/wiki/Semnătură_digitală>, Accesat la 01.02.2023 10:00.
2. Wikipedia, eIDAS, Accesibil: <https://en.wikipedia.org/wiki/EIDAS>, Accesat la 01.02.2023 11:00.
3. Turner, Dawn M. "eIDAS from Directive to Regulation - Legal Aspects". Accesibil: <https://www.cryptomathic.com/news-events/blog/eidas-from-directive-to-regulation-legal-aspects>, Accesat la 01.02.2023 18:00.
4. ETSI TS 119 612, *„Electronic Signatures and Infrastructures (ESI); Trusted Lists”,* Accesibil: , <https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf> , Accesat la 01.02.2023 20:00.
5. ETSI TS 119 615, *„Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists”*, Accesibil: <https://www.etsi.org/deliver/etsi_ts/119600_119699/119615/01.01.01_60/ts_119615v010101p.pdf>, Accesat la 01.02.2023 20:00.
6. European Commission, eIDAS Dashboard, Accesibil: <https://esignature.ec.europa.eu/efda/tl-browser>, Accesat la: 06.12.2022 10:00.
7. Github Project, *„EUTL-Parser”*, George Gugulea, CertSIGN S.A., Accesibil: <https://github.com/authone/eutl-parser>, Accesat la 07.12.2022 10:00.