**ROMÂNIA**

**MINISTERUL APĂRĂRII NAŢIONALE**

**ACADEMIA TEHNICĂ MILITARĂ**

**„Ferdinand I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Securitatea Tehnologiei Informației**



**Solutie client pentru interogarea și analiza de informații 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**

# ABSTRACT

# REZUMAT

**Cuprins**

[ABSTRACT 1](#_Toc126688364)

[REZUMAT 2](#_Toc126688365)

[LISTĂ ABREVIERI 5](#_Toc126688366)

[LISTĂ FIGURI 6](#_Toc126688367)

[1. INTRODUCERE 7](#_Toc126688368)

[1.1. Importanța și actualitatea problematicii abordate 7](#_Toc126688369)

[1.2. Scopul și obiectivele proiectului 8](#_Toc126688370)

[1.3. Structura proiectului pe capitole 8](#_Toc126688371)

[2. STADIUL CUNOAȘTERII ÎN DOMENIU 9](#_Toc126688372)

[2.1. Fundamente teoretice 9](#_Toc126688373)

[2.1.1. Semnături și certificate digitale 9](#_Toc126688374)

[2.1.2. Standardul eIDAS 10](#_Toc126688375)

[2.1.3. Liste de Încredere 11](#_Toc126688376)

[2.1.4. Listele de Încredere ale Uniunii Europene (EUTL) 14](#_Toc126688377)

[2.2. Soluții și abordări similare 14](#_Toc126688378)

[2.2.1. Aplicația oficială a Comisiei Europene [6] 14](#_Toc126688379)

[2.2.2. Implementarea dl. George Gugulea, Director Cercetare și Inovare, CertSIGN [7] 15](#_Toc126688380)

[3. IMPLEMENTAREA APLICAȚIEI 16](#_Toc126688381)

[3.1. Descrierea proiectului 16](#_Toc126688382)

[3.2. Componenta de extragere 17](#_Toc126688383)

[3.2.1. Validarea și extragerea informațiilor din LOTL 18](#_Toc126688384)

[3.2.2. Validarea și extragerea informațiilor din TL 20](#_Toc126688385)

[3.2.3. Tratarea cererilor de la componenta UI 21](#_Toc126688386)

[3.3. Componenta de validare 21](#_Toc126688387)

[3.3.1. Validarea certificatelor 22](#_Toc126688388)

[3.3.2. Validarea semnăturilor 23](#_Toc126688389)

[3.4. Componenta UI 24](#_Toc126688390)

[3.4.1. Afișarea informațiilor extrase din LOTL. 26](#_Toc126688391)

[3.4.2. Afișarea informațiilor extrase dintr-un TL 27](#_Toc126688392)

[3.4.3. Afișarea informațiilor despre un furnizor de servicii criptografice 29](#_Toc126688393)

[3.4.4. Afișarea informațiilor unui serviciu criptografic 30](#_Toc126688394)

[BIBLIOGRAFIE 32](#_Toc126688395)

# 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 |
| 10. | MVC | Model-View-Controller |

# LISTĂ FIGURI

[Figura 1 - Structura unei liste de încredere [4] 13](#_Toc126688396)

[Figura 2 - Interacțiunea componentelor 16](#_Toc126688397)

[Figura 3 - Reprezentare JSON a structurii obținute în memoria cache 20](#_Toc126688398)

[Figura 4 - Informațiile obținute în urma validării unui certificat 23](#_Toc126688399)

[Figura 5 - Informațiile obținute în urma validării unei semnături 24](#_Toc126688400)

[Figura 6 - Diagrama de secvență pentru afișarea LOTL 26](#_Toc126688401)

[Figura 7 - Prezentare informații LOTL 27](#_Toc126688402)

[Figura 8 - Diagrama de secvență pentru afișarea TL 28](#_Toc126688403)

[Figura 9 - Prezentare informații TL aferent statului român 29](#_Toc126688404)

[Figura 10 - Prezentare informații furnizor de servicii criptografice (Ex.: CertSIGN) 30](#_Toc126688405)

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 și 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:

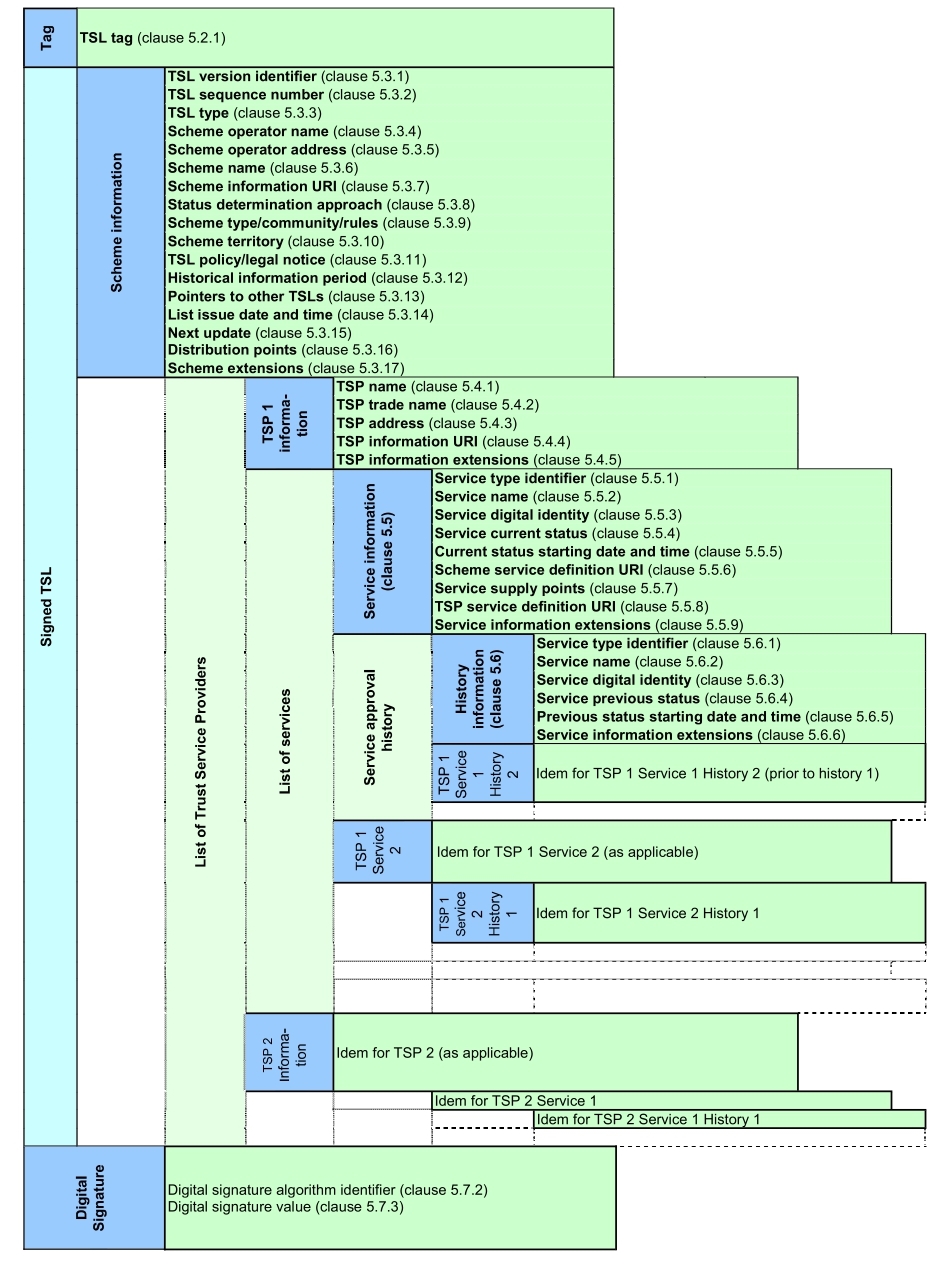


Figura 1 - Structura unei liste de încredere [4]

### 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:

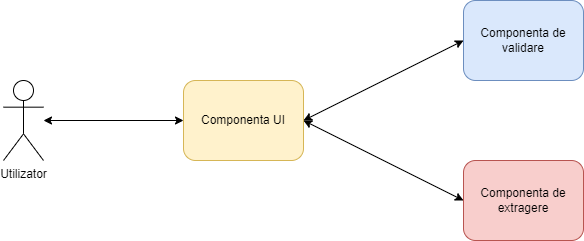


Figura 2 - Interacțiunea componentelor

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

## Componenta de extragere

Componenta de extragere este reprezentată de un serviciu REST. Cerințele funcționale ale 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 [10]. 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. Proiectul DSS este o librărie open-source, care are ca scop implementarea standardelor pentru crearea, augmentarea și validarea semnăturilor avansate, în conformitate cu legislația europeană și cu standardul eIDAS [8].

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.

Comunicarea dintre serviciul REST și componenta UI este securizată folosind TLS, accesul către serviciu fiind permis doar prin protocolul HTTPS.

### 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.

Pentru a putea fi încărcate informațiile prezente în LOTL, se vor parcurge următoarele 3 etape:

* Încărcarea informațiilor necesare claselor interne DSS;
* Descărcarea LOTL în format XML, și validarea semnăturii digitale folosind DSS;
* Parcurgerea documentului XML, și încărcarea în memorie a informațiilor.

#### Încărcarea informațiilor necesare claselor interne DSS

Pentru inițializarea claselor interne DSS este necesară efectuarea configurării conform documentației DSS. Odată configurată, librăria pune la dispoziție clase specializate pentru a efectua validarea și încărcarea automată a informațiilor necesare validării semnăturilor, printre care se numără și certificatele folosite la semnarea LOTL, sau a altor TL. Această inițializare are loc într-un thread separat de cel principal, pentru a nu impacta negativ experiența utilizatorilor și se execută periodic la un interval de timp configurabil..

#### Descărcarea LOTL în format XML și validarea semnăturii digitale

Locația exactă a LOTL este publică, putând fi accesată de pe pagina oficială a Comisiei Europene (<https://commission.europa.eu/index_ro>), sau în mod direct, la adresa <https://ec.europa.eu/tools/lotl/eu-lotl.xml>. Aici se găsește documentul în format XML, având aplicat, pentru asigurarea integrității, o semnătură în format XAdES.

Odată încărcate informațiile necesare DSS, putem efectua validarea semnăturii. Acest lucru se produce într-un thread separat, pentru a nu impacta negativ experiența utilizatorilor. Validarea semnăturii asupra listei se face respectând procedurile descrise în ETSI TS 119 615 [5], iar rezultatul validării, împreună cu orice alte mesaje de informare este păstrat în memoria cache, unde se vor popula și informațiile prezente in LOTL, pentru a putea fi înmânate componentei UI.

#### Parcurgerea documentului XML și încărcarea în memorie a informațiilor

Parcurgerea documentului XML are loc în același thread de execuție ca validarea semnăturii, pentru a păstra accesul la documentul deja validat. Extracția informațiilor se execută folosind modelul DOM pentru XML, structura listei fiind deja cunoscută, conform standardului ETSI TS 119 612 [4]. În final, obținem un obiect Java ce va fi adăugat în memoria cache împreună cu informațiile obținute în urma validării sale.

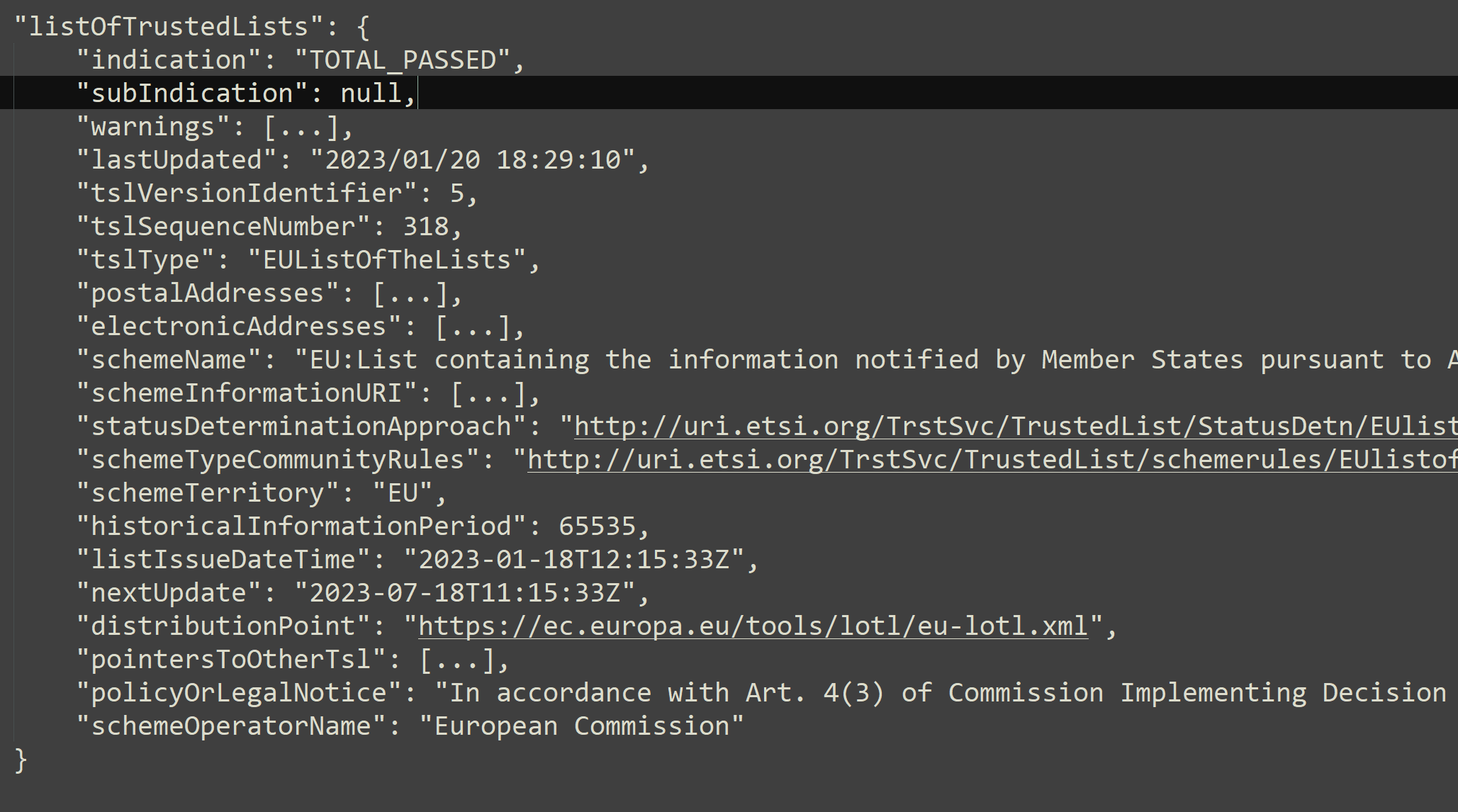


Figura - Reprezentare JSON a structurii obținute în memoria cache

### Validarea și extragerea informațiilor din TL

Pentru efectuarea validării și extragerii informațiilor dintr-o listă de încredere pașii sunt similari cu cei de la punctul anterior. Totuși, față de pasul anterior, nu mai este necesară încărcarea informațiilor necesare DSS, deoarece acest lucru a fost deja executat la validarea LOTL.

Accesarea listei de încredere se face folosind câmpurile extrase anterior din LOTL. În cadrul acesteia, există o listă de *„pointeri”* care definesc locația listelor de încredere pentru fiecare stat membru. Pentru a obține pointerul asociat unui anumit stat, trebuie sa parcurgem lista de pointeri până ajungem la cel care are menționat în cadrul câmpului *SchemeTerritory* codul ISO din 2 litere asociat statului membru dorit. Folosind URL-ul prezent în acel pointer, putem executa în mod asemănător validarea și extragerea informațiilor ca la punctul anterior, rezultând în memoria cache un obiect cu structura asemănătoare celei descrise la Figura 1, având, totuși, adăugate câmpurile ce includ informațiile care reies în urma validării listei de încredere (*„Indication”*, *„SubIndication”* și *„Warnings”* prezente și în Figura 3*)*.

Este important de menționat că, spre deosebire de validarea LOTL care se execută automat la un interval de timp stabilit prin configurarea aplicației, validarea unui TL se execută doar în situația în care un utilizator a cerut accesarea respectivei liste, iar aceasta fie nu se află în memoria cache, fie se află în memorie dar a expirat.

### Tratarea cererilor de la componenta UI

Componenta UI gestionează cererile de la client și le trimite către componenta de extragere în situația în care este necesar. Serviciul REST de extragere a informațiilor va răspunde întotdeauna componentei UI cu informațiile extrase din LOTL, sau din respectivul TL cerut care au fost deja introduse în memoria cache.

## Componenta de validare

Componenta de validare este reprezentată de un JAR. Cerințele funcționale ale acesteia sunt următoarele:

* Primește de la componenta UI un certificat în format PEM, și un timp pentru care să fie afișate informațiile, execută validarea acestuia și returnează rezultatele validării, precum și informații prezente în certificat, și statutul de calificare al acestuia.
* Primește de la componenta UI un document semnat, execută validarea acestuia și returnează rezultatele validării, informațiile despre semnătură precum statutul de calificare, timpul semnării, etc. precum și informațiile despre semnatar.

Aplicația este implementată în Java, folosește, la fel ca serviciul REST, librăria oficială a Comisiei Europene, DSS, și implementează mecanisme din Spring Framework precum Dependency Injection și Inversion of Control.

Deși ar putea funcționa ca un serviciu REST independent, această aplicație este implementată folosind arhitectura client-server bazată pe comunicarea prin sockets [9], componenta de validare fiind serverul, iar componenta UI fiind clientul.

Astfel, componenta UI trimite către componenta de validare comenzile și datele necesare efectuării comenzilor către validator prin intermediul socketurilor de rețea, și așteaptă primirea răspunsului.

Întrucât componenta de validare folosește librăria DSS, este necesară efectuarea pașilor de configurare și încărcare a informațiilor în cache-ul intern librăriei, la fel ca la componenta de extragere. Așadar, prima etapă din ciclul de viață al componentei de validare este verificarea și stocarea informațiilor necesare validării de semnături și certificate în cadrul memoriei cache DSS. Acest lucru se întâmpla la fiecare conexiune nouă cu un client, pentru a asigura actualitatea datelor de validare, integritatea și consistența rezultatelor validării.

### Validarea certificatelor

Pentru efectuarea validării, componenta de validare primește de la componenta UI certificatul ce se dorește a fi validat. De asemenea, se poate selecta un anumit moment de timp pentru care să fie efectuate validările, în situația în care vrem să aflăm starea certificatului în acel moment.

Folosind informațiile stocate în cache-ul DSS, și clasele specifice librăriei pentru validarea certificatelor digitale, se execută validarea și se extrag informațiile dorite.

Răspunsul care va fi trimis către componenta UI este un șir de caractere ce conține un obiect JSON, reprezentând informații precum rezultatul validării, perioada de valabilitate, posesorul certificatului, utilizările autorizate pentru cheia privată asociată certificatului, nivelul de calificare atât la momentul emiterii certificatului, cât și la momentul validării, dar și statutul revocării, pentru fiecare dintre certificatele prezente în lanțul de certificare aferent certificatului de validat.

Informațiile prezente pentru fiecare certificat din lanțul de certificare arată de forma:

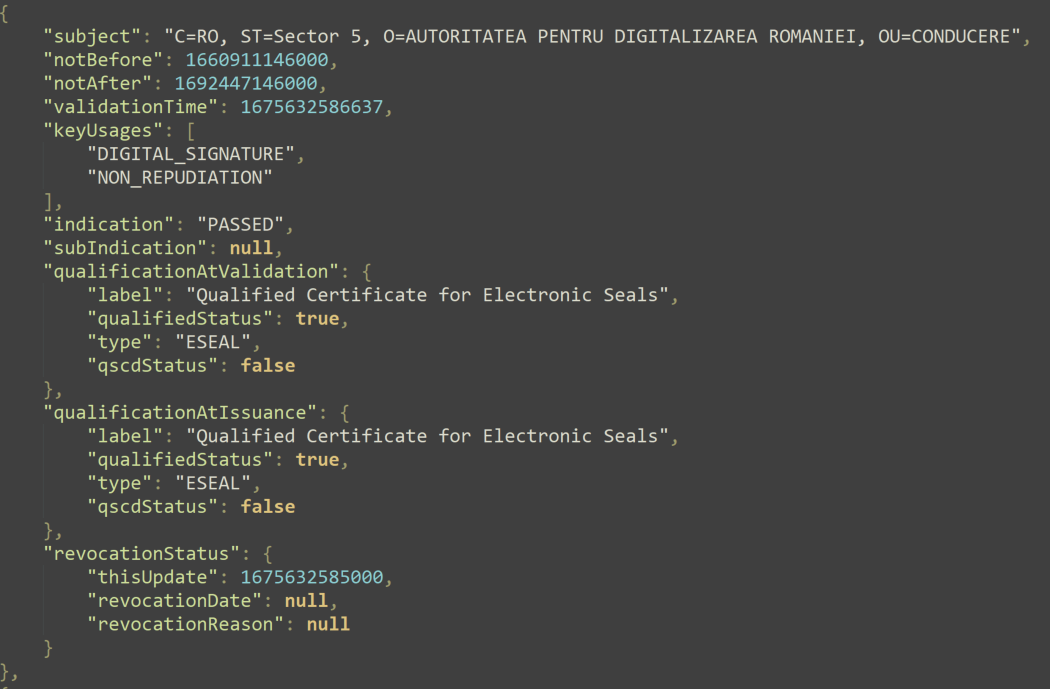


Figura - Informațiile obținute în urma validării unui certificat

### Validarea semnăturilor

Pentru efectuarea validării, componenta de validare primește de la componenta UI documentul conținând semnătura atașată ce se dorește a fi validată. Folosind informațiile stocate în cache-ul DSS, și clasele specifice librăriei pentru validarea semnăturilor digitale, se execută validarea și se extrag informațiile dorite.

Răspunsul care va fi trimis către componenta UI este un șir de caractere ce conține un obiect JSON, reprezentând informații precum politica abordată pentru validarea semnăturii, numărul de semnături valide, dar și numărul total de semnături prezente, iar pentru fiecare semnătură, se specifică timpul semnăturii, formatul semnăturii, semnatarul, rezultatul validării, nivelul de calificare al semnăturii, și o listă ce conține numele posesorilor de certificate ce se află pe lanțul de certificare al certificatului semnatarului.

Un exemplu de răspuns pentru validarea unei semnături poate fi văzut în figura de mai jos:

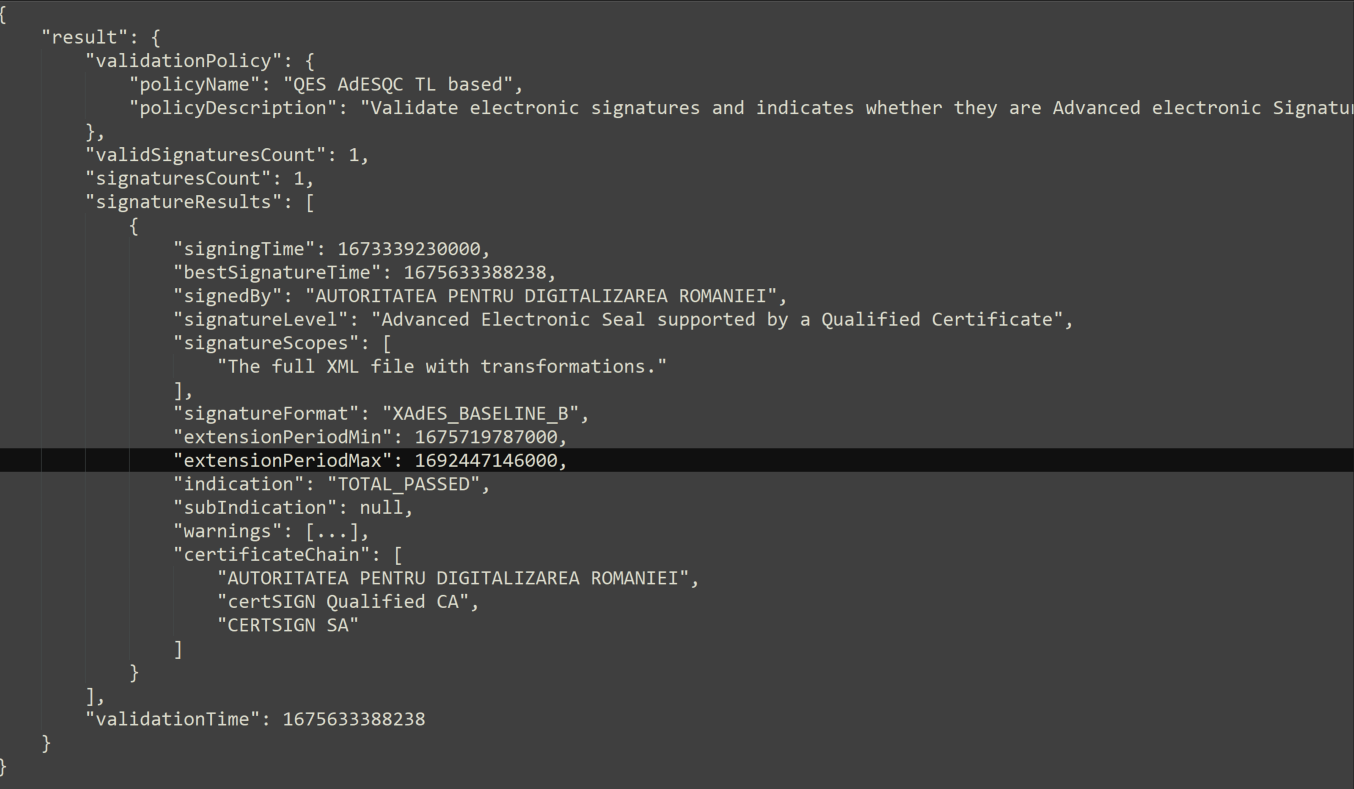


Figura - Informațiile obținute în urma validării unei semnături

## 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.

Serverul web este implementat folosind Java și SpringBoot Framework pentru partea de backend, împreună cu Thymeleaf și Bootstrap pentru partea de frontend, fiind implementat pe arhitectura MVC. Arhitectura MVC este o paradigmă de programare software utilizată, de obicei, în dezvoltarea aplicațiilor ce oferă interfețe cu utilizatorul. MVC, după cum se poate deduce din nume, implică 3 componente: Model, View, și Controller.

Modelul este componenta principală a arhitecturii și reprezintă structura internă a datelor acesteia. Modelul implementează în mod direct logica și regulile de utilizare ale aplicației. De obicei, un model este reprezentat de un tabel în baza de date a aplicației. View-ul este componenta de interfață cu utilizatorul, precum o pagină web, interfața grafică a unei aplicații, etc.. Controllerul este componenta care mediază interacțiunile dintre View și Model. Acesta primește input de la utilizatori prin intermediul View-ului, și le convertește în comenzi de executat pentru Model.

Fiind componenta care mediază interacțiunea dintre utilizator și componentele de validare și extragere, interfața web, primind cereri de la utilizator, trimite mai departe, către cele două componente, comenzile necesare pentru afișarea răspunsului.

Componenta UI va îndeplini următoarele cerințe funcționale:

* Afișează lista cu toate listele de încredere obținute prin parcurgerea LOTL;
* Afișează lista furnizorilor de servicii criptografice de încredere pentru un stat membru, precum și informații prezente în lista de încredere a respectivului stat;
* Afișează lista serviciilor criptografice de încredere pentru un anumit furnizor grupate în funcție de tipul acestora, precum și informații despre respectivul furnizor;
* Afișează informații despre un anumit serviciu criptografic de încredere, precum status, perioada de validitate a statusului, istoric, certificatele digitale deținute, etc.;
* Afișează informații despre starea istorică a unui anumit serviciu criptografic de încredere, precum status, perioada de început a statusului, informații despre certificatele digitale deținute, etc.
* Primește de la client un certificat ce se vrea a fi validat, și, opțional, un moment de timp pentru care se dorește obținerea rezultatului, și afișează rezultatele validării;
* Primește de la client un document semnat ce se vrea a fi validat, și afișează rezultatele validării.

### Afișarea informațiilor extrase din LOTL.

Pentru vizualizarea informațiilor extrase din LOTL, componenta UI trimite către serviciul REST o cerere pentru acestea. Serviciul REST primește cererea, și trimite înapoi către componenta UI informațiile prezente în memoria cache, deja extrase.

Diagrama de secvență a acestui scenariu poate fi observată mai jos:

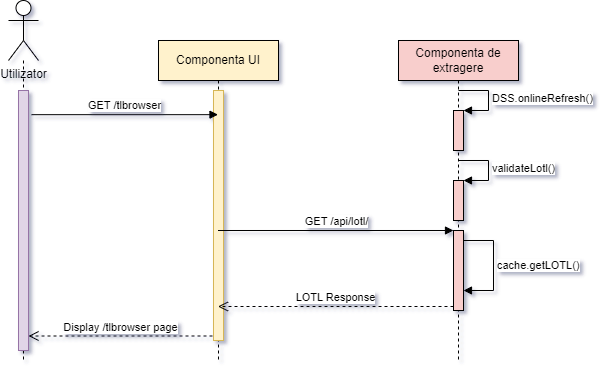


Figura - Diagrama de secvență pentru afișarea LOTL

Informațiile extrase din LOTL reprezintă, de fapt, pointeri către listele de încredere ale statelor membre UE, așa cum este specificat în ETSI TS 119 612 [4], precum și informații despre operatorul LOTL, Comisia Europeană. Fiecare pointer descrie locația listei de încredere a unui stat membru, și este prezentat în pagină conform imaginii de mai jos:



Figura - Prezentare informații LOTL

Printr-un click pe numele statului sau pe drapelul respectiv, putem accesa pagina cu informațiile extrase din TL-ul statului.

În partea de jos a paginii putem regăsi informații legate de LOTL, precum data emiterii, data următoarei emiteri, numele și adresa operatorului, tipul listei de încredere, etc.

Este important de menționat faptul că orice atenționare obținută în urma validării LOTL este accesibil prin intermediul meniului extensibil, prezent în poza de mai sus, făcând click pe butonul galben cu semnul de atenționare.

### Afișarea informațiilor extrase dintr-un TL

Pentru vizualizarea informațiilor extrase dintr-un TL, componenta UI trimite către serviciul REST cererea împreună cu codul ISO-2 al statului dorit. Serviciul REST primește cererea și răspunde cu informațiile prezente în memoria cache.

Diagrama de secvență a acestui scenariu poate fi observată mai jos:

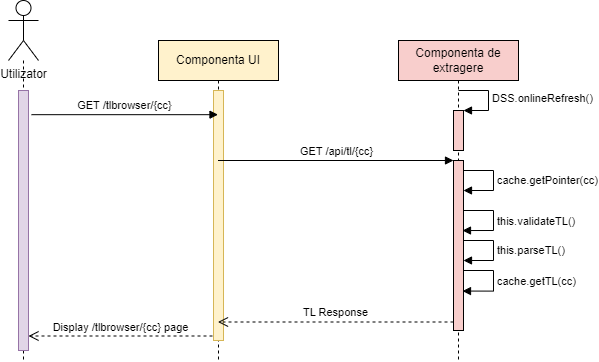


Figura - Diagrama de secvență pentru afișarea TL

Un lucru important de amintit, pentru diagrama prezentată mai sus, este că pașii *validateTL()* și *parseTL()* se execută doar în cazul în care lista de încredere nu a mai fost parcursă, sau informațiile prezente în cache au expirat. Așadar, este posibilă observarea unor diferențe de performanță între prima accesare și a doua accesare a aceleiași liste de încredere.

Astfel, serverul web, primind de la serviciul REST lista cu furnizorii de încredere, o prezintă către utilizator în forma următoare:

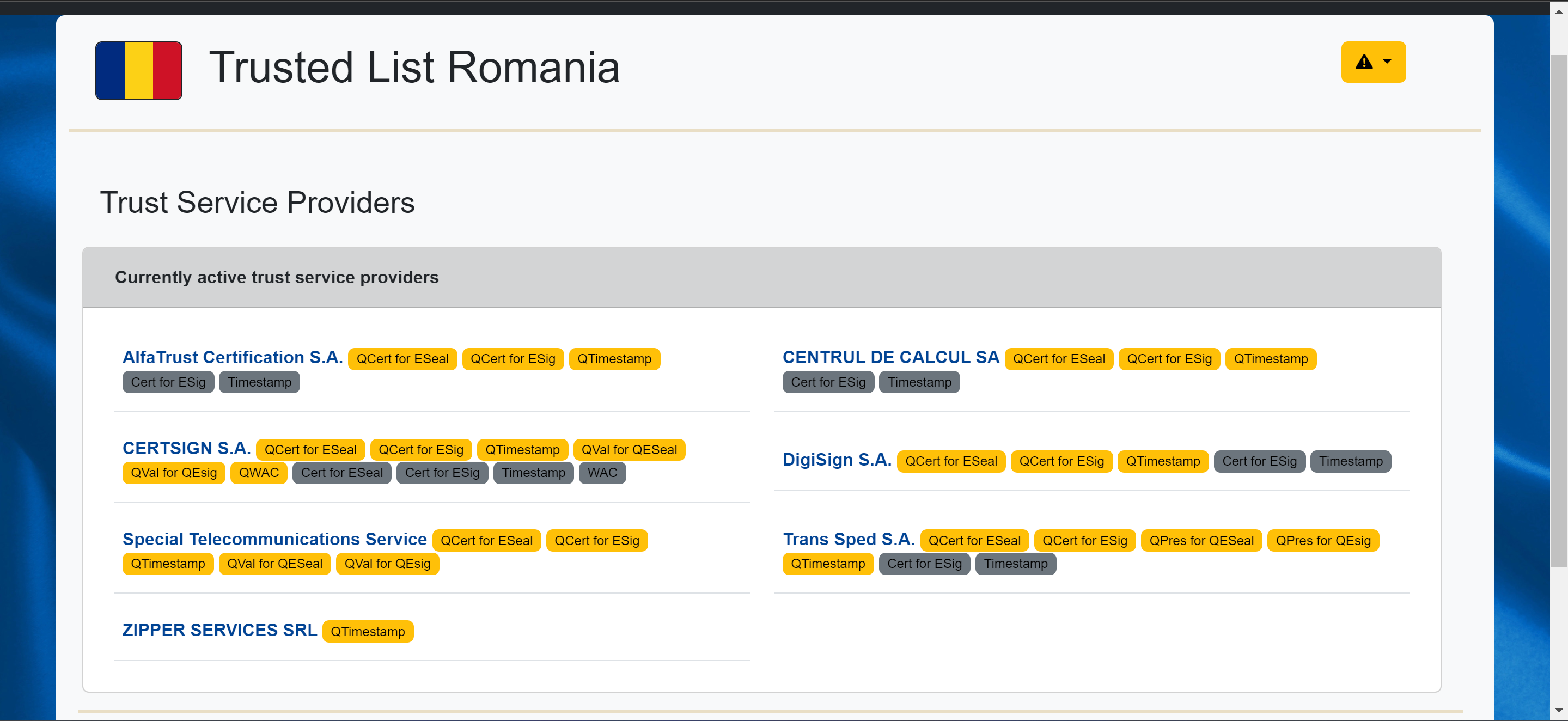


Figura - Prezentare informații TL aferent statului român

Furnizorii sunt separați în furnizori cu servicii active la momentul curent, și furnizori fără servicii active, prin două meniuri colapsabile. Pentru utilizatorii cu servicii active, sunt afișate și tipurile de servicii pe care le oferă. Putem accesa informațiile despre orice furnizor de aici, făcând click pe numele acestuia.

De asemenea, putem regăsi în partea de jos a paginii informațiile legate de lista de încredere a statului, precum operatorul listei de încredere, numărul de secvență al acesteia, data emiterii, data următoarei emiteri, etc.

### Afișarea informațiilor despre un furnizor de servicii criptografice

Pentru afișarea informațiilor despre un furnizor de servicii criptografice de încredere, componenta UI trimite către serviciul REST cererea pentru lista de încredere asociate statului în care furnizorul își execută activitatea. Astfel, odată primit răspunsul, componenta UI selectează informațiile asociate furnizorului din lista de încredere, fiind apoi expuse către utilizator.

Rapiditatea răspunsului este asigurată de procesul de cache-uire a memoriei, astfel încât validarea semnăturii aplicate asupra listei de încredere, și extragerea informației se execută doar în cazul în care informațiile valide nu există în cache.

Comunicația între serverul web și serviciul rest este identică cu cea de la punctul 3.4.2, diferența fiind informația extrasă efectiv din răspunsul serverului.

Accesând pagina unui furnizor de servicii, utilizatorului îi va fi prezentat următorul ecran:

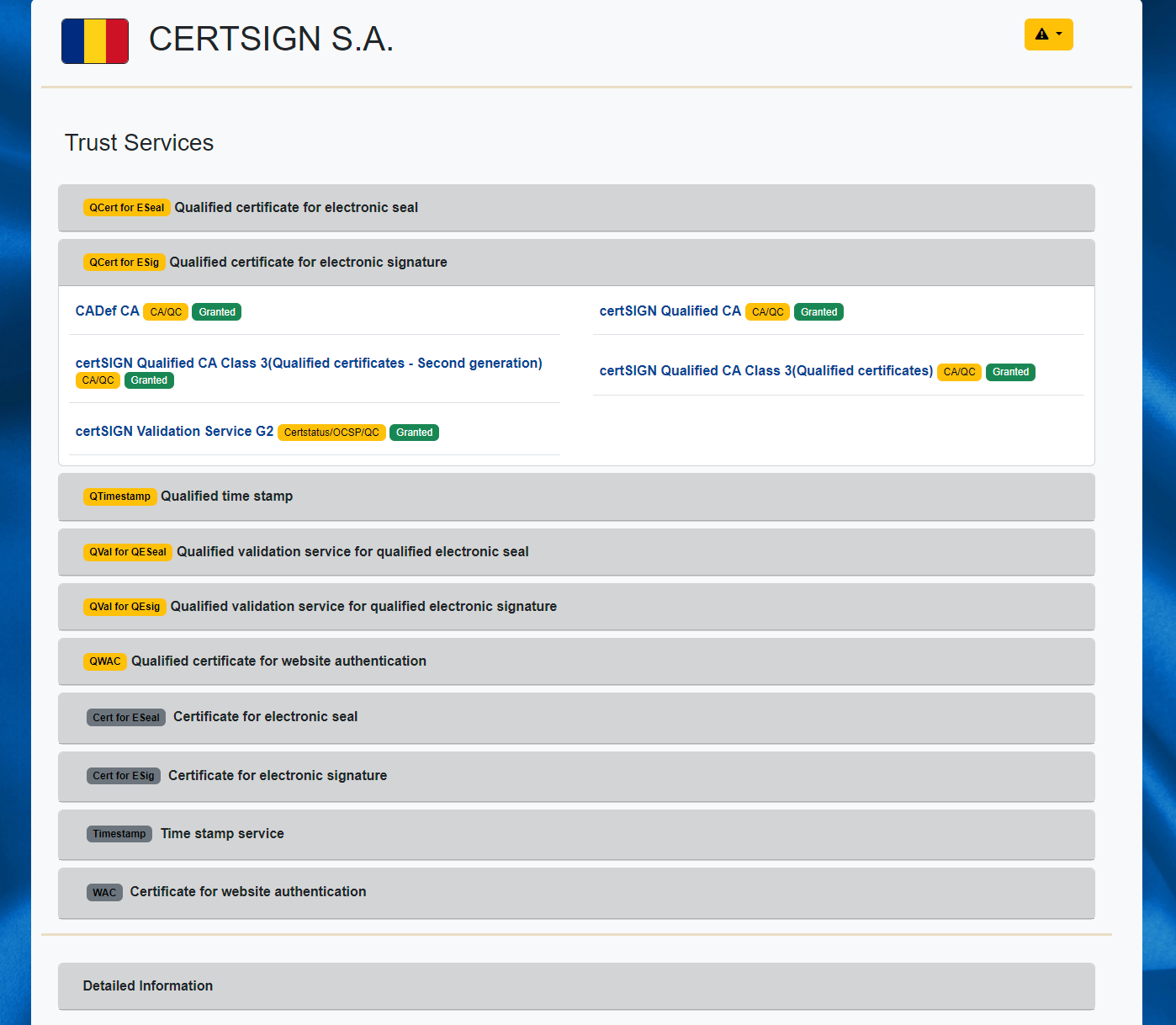


Figura - Prezentare informații furnizor de servicii criptografice (Ex.: CertSIGN)

În pagină putem vedea toate serviciile criptografice aferente furnizorului dorit, grupate în funcție de tipul de serviciu, și statutul calificării acestora. În urma expandării fiecărui grup se poate vedea tipul detaliat al serviciilor, împreună cu statutul de acreditare al acestuia. De asemenea, în partea de jos a paginii, accesând tab-ul *„Detailed Information”*, sunt afișate informațiile despre furnizor, precum numele, adrese, adrese de e-mail, etc..

### Afișarea informațiilor unui serviciu criptografic

La fel ca la punctul 3.4.3, componenta UI primește de la serviciul REST lista de încredere asociată statului membru în care furnizorul își execută activitatea, de unde extrage informația serviciului criptografic dorit.

Comunicația între serverul web și serviciul REST este identică cu cea din Figura 8, cu excepția faptului că diferă cererea utilizatorului către componenta UI, iar răspunsul returnat de UI către utilizator conține doar informațiile serviciului criptografic cerut.

Informațiile despre serviciul criptografic sunt prezentate utilizatorului conform imaginii de mai jos:

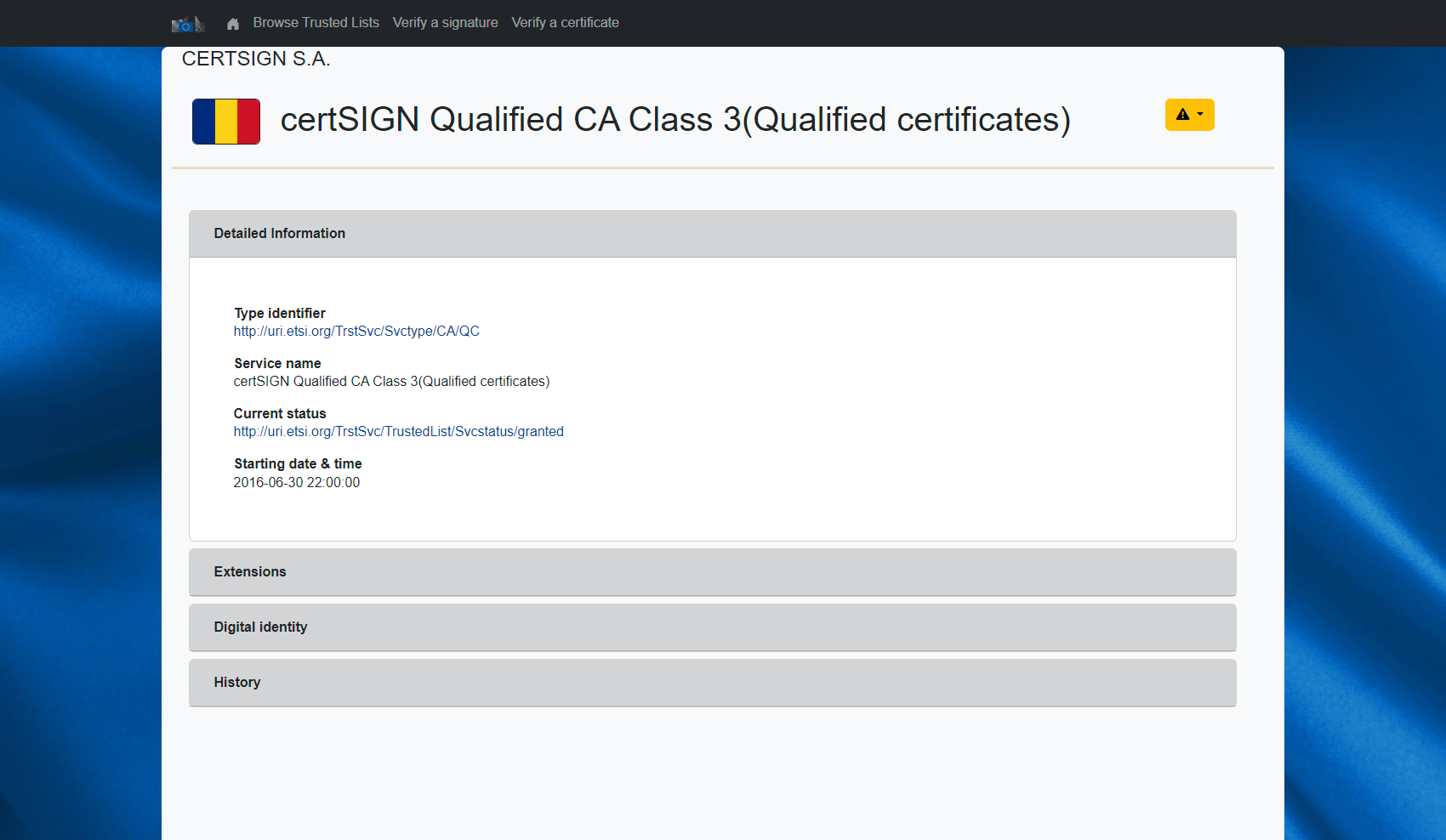


Figura - Prezentare informații serviciu criptografic (Ex.: CertSIGN Qualified CA Class 3)

În pagină putem vedea toate informațiile despre serviciul respectiv, printre care putem identifica tipul serviciului, numele acestuia, statusul de acreditare, precum și data de început a acestuia. De asemenea, putem vedea extensiile serviciului accesând tab-ul *„Extensions”*.

Avem acces și la informațiile incluse în certificatele declarate ale serviciului, prezente în lista de încredere a statului, accesând tab-ul *„Digital identity”*.

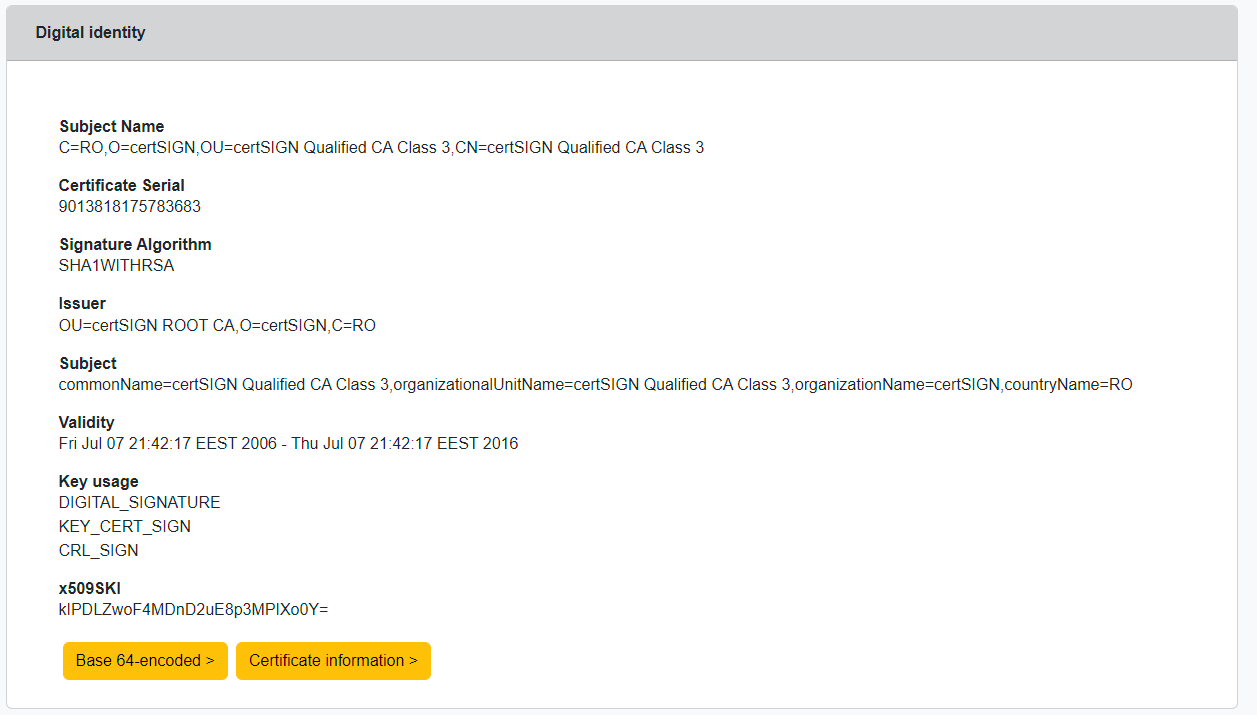


Figura - Prezentare informații certificate serviciu

De asemenea, putem accesa și certificatul în mod direct, în format PEM, făcând click pe butonul *„Base 64-encoded”*, sau pe informațiile extrase din certificat, făcând click pe butonul *„Certificate information”*.

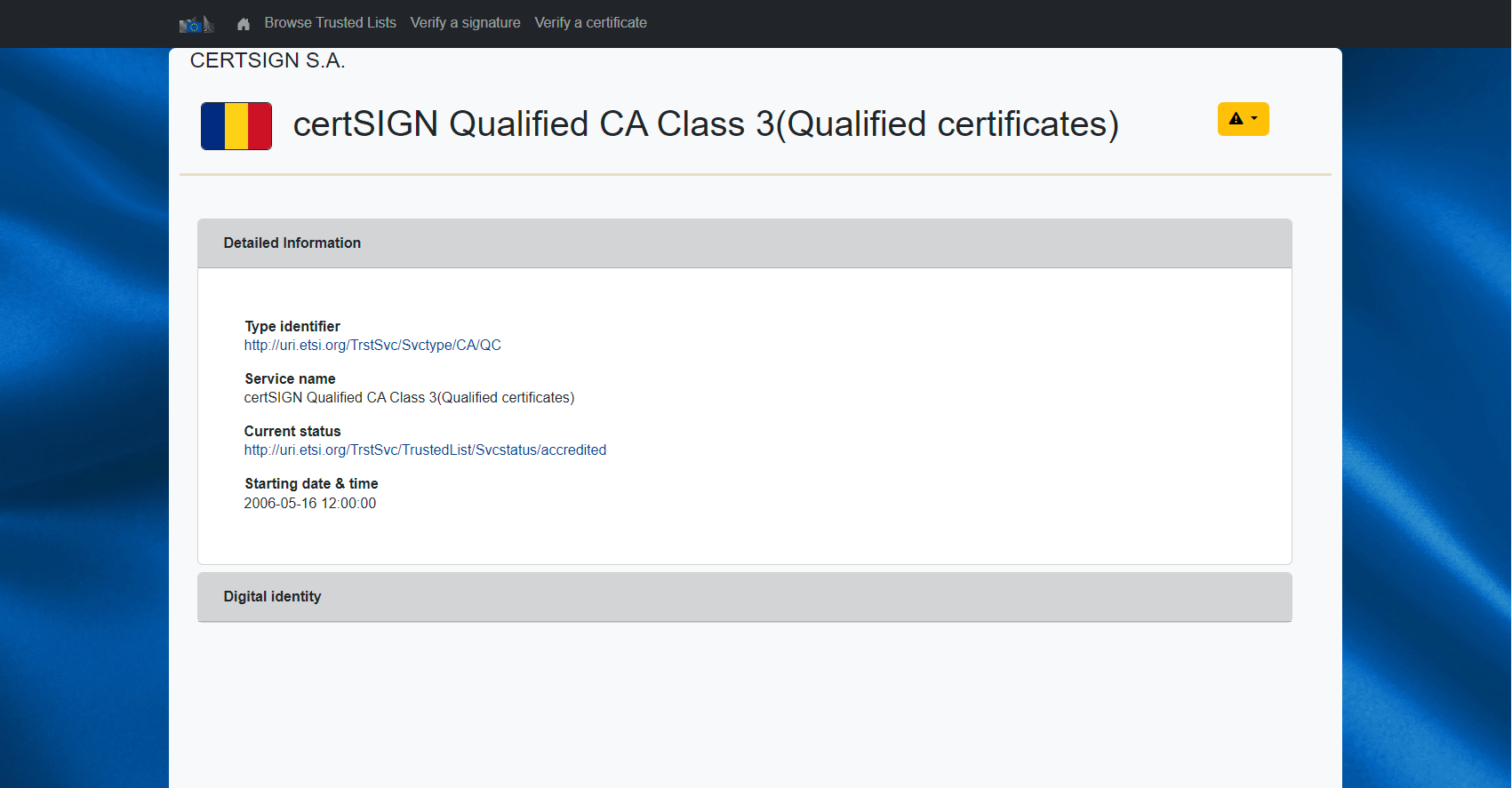
Istoricul serviciului poate fi accesat din tab-ul *„History”*, unde sunt prezentate toate statusurile deținute de serviciul respectiv, împreună cu dățile de început ale acestora.

### Afișarea informațiilor despre o stare istorică a unui serviciu criptografic

La fel ca la punctul 3.4.3, componenta UI primește de la serviciul REST lista de încredere asociată statului membru în care furnizorul își execută activitatea, de unde extrage informația serviciului criptografic dorit.

Comunicația între serverul web și serviciul REST este identică cu cea din Figura 8, cu excepția faptului că diferă cererea utilizatorului către componenta UI, iar răspunsul returnat de UI către utilizator conține doar informațiile instanței istorice a serviciului criptografic cerut.

Informațiile despre statutul istoric al serviciului sunt prezentate utilizatorului conform imaginii de mai jos:



Prezentarea statutului istoric al unui serviciu se aseamănă destul de mult cu prezentarea informațiilor aferente serviciului, întrucât structura definită în standardul ETSI TS 119 612 este asemănătoare.

În pagină ne sunt prezentate, la fel ca și la starea actuală a serviciului, tipul serviciului, statusul acestuia, numele, și data de început a stării istorice. De asemenea, putem accesa informații extrase din certificatele digitale ale serviciului accesând tab-ul *„Digital identity”*, cu mențiunea că, conform standardului, formele întregi, codificate PEM, ale certificatelor asociate serviciului criptografic sunt omise.

# 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.
8. European Commission, *„Digital Signature Service”*, Accesibil: <https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html>, Accesat la 03.01.2023 10:00.
9. Wikipedia, *„Network Socket”*, Accesibil: <https://en.wikipedia.org/wiki/Network_socket>, Accesat la 04.01.2023 10:00.
10. Spring, *„Spring Boot Reference Documentation”*, Accesibil: <https://docs.spring.io/spring-boot/docs/current/reference/htmlsingle/>, Accesat la 04.11.2022 11:00.
11. Wikipedia, „Model-view-controller”, Accesibil: <https://en.wikipedia.org/wiki/Model-view-controller>, Accesat la 06.02.2023 15:00.