**ROMÂNIA**

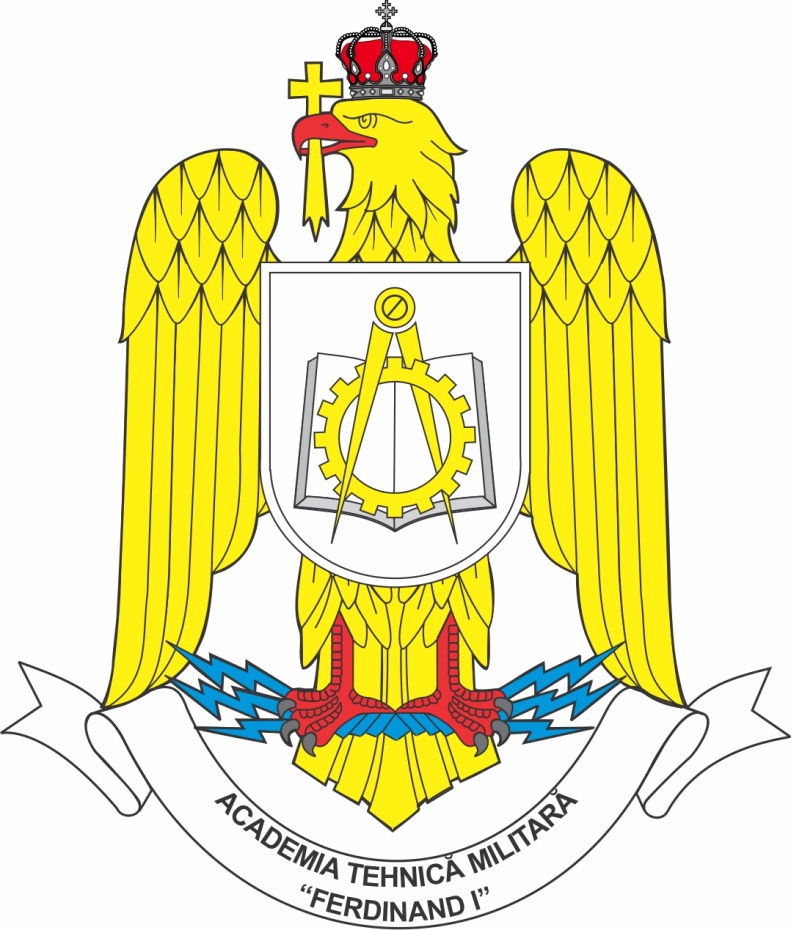
**MINISTERUL APĂRĂRII NAȚIONALE**

**ACADEMIA TEHNICĂ MILITARĂ „FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

***Specializarea: Calculatoare și sisteme informatice pentru apărare***

***și securitate națională***



**Servicii pentru validarea atestărilor electronice de atribute**

Coordonator științific:

**Cpt. Lect. Dr. Ing. Iulian Aciobăniței**

ABSOLVENT:

**Sd. Sg. Maj. Crihană Dragoș-Mihai**

**BUCUREȘTI**

**2025**

# Abstract

In today’s fast-paced digital world, electronic attestations of attributes within digital wallets play a key role in enabling secure and trustworthy digital interactions. This project introduces a mobile application designed to validate electronic attestations stored and presented by digital wallets, in alignment with eIDAS 2 standards for interoperable digital identity services. The system focuses on implementing a robust verification method that ensures the authenticity of attestations while maintaining both security and ease of use for service providers.

The mobile application is designed to validate electronic attestations of attributes according to the eIDAS 2 framework, which provides a legal foundation for secure digital identity services in the European Union. The system supports two complementary methods for verifying the revocation status of credentials: a standardized status list published by the issuer, and a cascade Bloom filter distributed via IPFS. The Bloom filter is encapsulated within a signed JWT, which is stored in IPFS, while its reference (IPFS hash) is published on the blockchain through a smart contract. These mechanisms allow the verifier to accurately determine whether a credential is valid, revoked, or expired, while maintaining high performance and scalability.

The application enables secure and controlled disclosure of personal data, including names, addresses, and birth dates. It generates a QR code containing a presentation request, which can be scanned by the EUDI Wallet to initiate credential sharing. The EUDI Wallet provides users with a simple interface to select and present credentials, while the verifier backend handles validation based on the received data.

Credential validation includes checks for digital signature authenticity, expiration date, and selective disclosure integrity, particularly through sd\_hash consistency verification. The system is fully compatible with the SD-JWT format, enabling efficient and standards-compliant processing of credential data. For securing access to the backend, user authentication and authorization are managed through Keycloak, which provides robust and flexible access control layer. Additionally, all communications between system components are secured using HTTPS, with Cloudflare acting as a reverse proxy and TLS termination layer to ensure encrypted and authenticated traffic across the network.

In conclusion, the solution represents a comprehensive tool for enabling secure and efficient validation of electronic attestations. It also offers developers a straightforward integration path, supporting the growth and scalability of digital identity ecosystems.

# Rezumat

În contextul dinamic al lumii digitale de astăzi, atestările electronice ale atributelor stocate in portofele digitale joacă un rol esențial în facilitarea unor interacțiuni sigure și de încredere. Acest proiect propune o aplicație *mobile* destinată validării atestărilor electronice stocate și prezentate prin intermediul portofelelor digitale, în conformitate cu standardele eIDAS 2 pentru furnizarea interoperabilă a servciilor de identitate digitală. Sistemul are în vedere implementarea unei metode robuste de verificare, care să asigure autenticitatea atestărilor, menținând totodată securitatea și ușurința în utilizare pentru furnizorii de servicii.

Aplicația *mobile* este concepută pentru a valida atestările electronice ale atributelor în conformitate cu cadrul eIDAS 2, care oferă o bază legală pentru furnizarea sigură a serviciilor de identitate digitală în Uniunea Europeană. Sistemul suportă două metode complementare de verificare a stării de revocare a credențialelor: un *status list* standardizat, publicat de emitent, și un filtru Bloom în cascadă, distribuit prin IPFS. Acest filtru este încorporat într-un JWT semnat, care este stocat în IPFS, iar referința sa (*hash*-ul IPFS) este publicată pe blockchain prin intermediul unui *smart contract*. Aceste mecanisme permit verificatorului să determine cu acuratețe dacă un credențial este valid, revocat sau expirat, menținând totodată o performanță ridicată și scalabilitate.

Aplicația permite o dezvăluire sigură și care respectă confidențialitatea datelor personale, inclusiv nume, adrese și date de naștere. Ea generează un cod QR care conține o cerere de prezentare, ce poate fi scanat prin intermediul *EUDI Wallet* pentru a iniția transmiterea credențialelor. *EUDI Wallet* oferă utilizatorilor o interfață simplă pentru selectarea și prezentarea atestărilor, în timp ce componenta backend a verificatorului gestionează procesul de validare pe baza datelor primite.

Validarea credențialelor include verificarea autenticității semnăturii digitale, a datei de expirare și a integrității dezvăluirii selective, în special prin compararea consistenței sd\_hash. Sistemul este pe deplin compatibil cu formatul SD-JWT, permițând procesarea eficientă și conformă cu standardele actuale a datelor din credențiale. Pentru securizarea accesului la backend, autentificarea și autorizarea utilizatorilor sunt gestionate prin Keycloak, care oferă un mecanism robust și flexibil de control al accesului. În plus, toate comunicațiile dintre componentele sistemului sunt securizate prin HTTPS, utilizând Cloudflare ca *reverse proxy* și punct de terminare TLS, pentru a asigura criptarea și autentificarea traficului în rețea.

În concluzie, soluția propusă reprezintă un instrument complet pentru validarea sigură și eficientă a atestărilor electronice. De asemenea, aceasta oferă dezvoltatorilor o cale clară și ușor de integrat, sprijinind dezvoltarea și scalabilitatea ecosistemelor de identitate digitală.

# Listă de abrevieri

* eIDAS *Electronic Identification, Authentication and Trust Services*
* IPFS *Interplanetary File System*
* QR *Quick Response*
* SD-JWT *Selective Disclosure JSON Web Token*
* TLS *Transport Layer Security*
* HTTPS *Hypertext Transfer Protocol Secure*
* EUDI *European Digital Identity*

# Introducere

## Importanța temei

Pe măsură ce tot mai multe activități se desfășoară în mediul digital, devine esențial ca utilizatorii să își poată dovedi identitatea într-un mod sigur, rapid și verificabil. Fie că este vorba despre accesarea unor servicii publice, înscrierea într-o instituție educațională sau încheierea unui contract electronic, este nevoie de un mecanism standardizat prin care identitatea și anumite atribute personale să poată fi prezentate în mod controlat, fără riscul de falsificare sau abuz.

Tranziția de la documentele fizice către cele digitale a adus numeroase beneficii, precum automatizarea proceselor, creșterea eficienței și o accesibilitate mai ridicată a serviciilor. Totuși, această schimbare a generat și provocări importante legate de încredere, securitate și interoperabilitatea dintre platforme. În acest context, Uniunea Europeană, prin inițiativa European Digital Identity (EUDI) și noul regulament eIDAS 2.0, propune un cadru unificat pentru identitatea digitală. Acest cadru permite fiecărui cetățean să dețină și să prezinte atestări electronice, cum ar fi numele, vârsta, cetățenia sau statutul educațional, folosind un portofel digital securizat, recunoscut la nivel european.

Pentru ca acest ecosistem să funcționeze corect, este esențială existența unor mecanisme de verificare automatizată și de încredere, prin care entitățile care solicită aceste atestări să poată valida autenticitatea, integritatea și starea lor (valid/revocat/expirat). Aici intervine importanța lucrării de față, care propune dezvoltarea unui serviciu de validare a atestărilor electronice în conformitate cu aceste standarde. Soluția urmărește să fie sigură, scalabilă și ușor de integrat în infrastructuri existente, fără a compromite experiența utilizatorului sau cerințele de securitate.

Pe măsură ce serviciile digitale devin tot mai prezente în viața de zi cu zi, nevoia de a verifica rapid și corect atestările electronice este tot mai evidentă. Lucrarea de față vine în întâmpinarea acestei nevoi, oferind o soluție practică pentru validarea acestor atestări într-un mod sigur, automatizat și adaptat cerințelor actuale de interoperabilitate și protecție a datelor.

## Obiectivele lucrării

Fiind în contextul dezvoltării unei soluții pentru verificarea atestărilor electronice, lucrarea de față își propune realizarea unui sistem care poate valida în mod automat credențiale digitale prezentate de utilizatori prin intermediul unui portofel digital. Scopul principal este acela de a oferi o metodă sigură, rapidă și conformă cu cerințele actuale de identitate digitală.

Aplicația urmărește să faciliteze procesul de validare a unor atribute personale precum numele, vârsta sau statutul educațional, fără a compromite confidențialitatea datelor. Un alt obiectiv este integrarea acestui proces într-un scenariu practic, care poate fi extins și adaptat în contexte reale, atât în sectorul public, cât și în cel privat.

Totodată, lucrarea își propune explorarea unor metode eficiente de verificare a autenticității și valabilității atestărilor, luând în considerare și nevoia de interoperabilitate în cadrul unei identități digitale europene.

## Metodologia de cercetare

Metodologia de cercetare a avut la bază o etapă de documentare extinsă asupra conceptelor cheie din domeniul identității digitale. Au fost studiate elemente precum regulamentul eIDAS 2.0, structura Verifiable Credentials, formatul SD-JWT și specificațiile asociate fluxurilor OpenID for Verifiable Presentations (OpenID4VP), toate analizate în contextul inițiativei European Digital Identity (EUDI).

În paralel cu documentarea teoretică, a fost investigat comportamentul portofelului digital EUDI Wallet, prin sesiuni de testare și debugging. Pentru a înțelege fluxul de prezentare al unui credential și cerințele asociate unui verifier, s-au analizat în detaliu cererile și răspunsurile generate de aplicație. Această etapă a ajutat la înțelegerea modului în care trebuie construite și conectate componentele pentru ca sistemul să funcționeze corect.

Pe baza acestor observații, a urmat etapa de definire a arhitecturii aplicației, stabilind rolul fiecărei componente în cadrul fluxului de validare. Implementarea a fost abordată treptat, începând cu funcționalitățile de bază și continuând cu integrarea componentelor necesare pentru verificarea credențialelor, generarea codurilor QR și comunicarea cu portofelul.

Procesul de cercetare a fost influențat și de stadiul incipient al unor standarde, cum este cazul status list-ului, integrat în lucrare chiar dacă a fost adoptat oficial destul de târziu. În plus, majoritatea implementărilor existente au fost dezvoltate în limbajul Kotlin, necunoscut inițial, ceea ce a făcut adaptarea mai dificilă, având în vedere că soluția propusă a fost construită în Java.

Întregul proces de dezvoltare a fost abordat pas cu pas, prin testare continuă și ajustări bazate pe comportamentul observat în fiecare etapă de integrare. Soluția finală s-a conturat prin combinarea aspectelor teoretice studiate cu observațiile practice obținute în timpul implementării.

## Rezultatele obținute

Rezultatul obținut în urma procesului de cercetare, documentare și dezvoltare este un sistem funcțional de validare a atestărilor electronice, conceput să fie compatibil cu standardele promovate prin eIDAS 2.0 și inițiativa European Digital Identity. Soluția permite inițierea fluxului de prezentare a credențialelor printr-o aplicație mobile și validarea automată printr-un serviciu backend dedicat.

Aplicația este construită să funcționeze cu formatul SD-JWT și suportă verificarea stării credențialelor prin două mecanisme complementare: status list și filtrul Bloom în cascadă, a cărui referință este publicată pe blockchain. Sistemul asigură integrarea cu portofelul EUDI Wallet, facilitând interacțiunea dintre utilizator și serviciul de verificare. Printre funcționalitățile realizate se numără:

* Generarea unui QR code pentru inițierea prezentării (OpenID4VP)
* Arhitectură adaptabilă la evoluția specificațiilor EUDI și eIDAS 2.0
* Suport pentru validarea mai multor tipuri de atestări electronice
* Validarea credențialelor SD-JWT, inclusiv semnătură, sd\_hash și expirare
* Verificarea stării prin status list și filtru Bloom stocat în IPFS
* Integrare cu EUDI Wallet pentru partajarea credențialelor
* Selectarea atributelor care vor fi prezentate în procesul de validare
* Configurarea comportamentului aplicației prin sistem de feature flags
* Gestionarea autentificării și autorizării utilizatorilor prin Keycloak
* Expunerea serviciului prin HTTPS, cu protecție oferită de Cloudflare.

## Rezumatul lucrării pe capitole

Capitolele lucrării surprind parcursul complet al dezvoltării unei soluții pentru validarea atestărilor electronice, de la justificarea alegerii temei și prezentarea cadrului teoretic, până la detalierea implementării și interpretarea rezultatelor obținute. Structura este concepută astfel încât să reflecte atât componentele tehnice implicate, cât și contextul legislativ și standardele de interoperabilitate care fundamentează soluția propusă.

Primul capitol oferă contextul general al temei, evidențiind importanța validării atestărilor electronice în actualul ecosistem digital. Sunt prezentate obiectivele urmărite, metodologia aplicată în dezvoltarea soluției și rezultatele obținute în urma procesului de cercetare.

În al doilea capitol sunt abordate noțiunile fundamentale privind atestările electronice. Se discută atât avantajele și provocările acestor mecanisme în raport cu soluțiile clasice PKI, cât și aspectele legislative și standardele relevante. Este inclus și un studiu comparativ între platformele existente.

Al treilea capitol este dedicat descrierii arhitecturii serviciilor implicate în procesul de emitere, gestionare și verificare a atestărilor electronice. Sunt analizate componentele principale, cum ar fi autoritățile emitente, furnizorii de servicii, registrele de stare și portofelul digital EUDI Wallet, alături de exemple de implementări existente.

În cel de-al patrulea capitol este detaliată soluția implementată. Sunt definite cerințele funcționale, este prezentată arhitectura generală și sunt descrise modulele componente. Tot aici sunt evidențiate tehnologiile utilizate și sunt interpretate rezultatele testelor efectuate.

Capitolul al cincilea sintetizează concluziile desprinse din elaborarea lucrării și propune direcții de dezvoltare ulterioară care pot consolida sau extinde funcționalitatea soluției propuse.

Ultimul capitol conține bibliografia utilizată în procesul de documentare, reunind surse teoretice, materiale tehnice și resurse oficiale relevante pentru tematica abordată.