**ROMÂNIA**

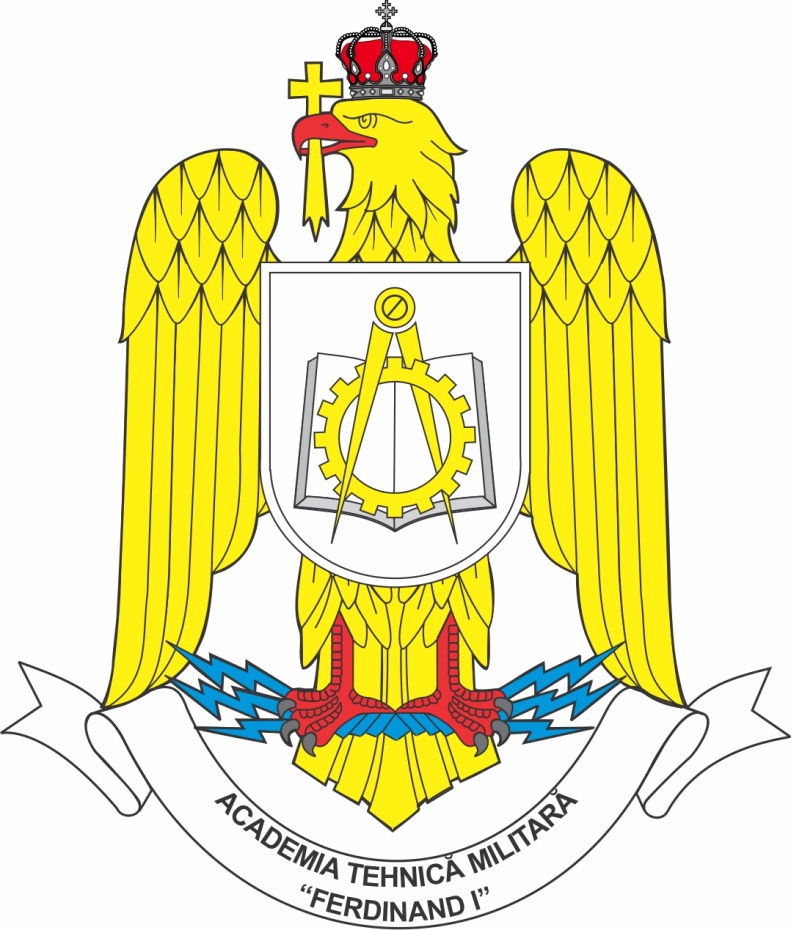
**MINISTERUL APĂRĂRII NAȚIONALE**

**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.

# Atestările electronice

## Introducere

Atestările electronice de atribute (Electronic Attestation of Attributes – EAA) sunt documente digitale care confirmă acuratețea unui anumit atribut, cum ar fi adresa de domiciliu sau o calificare profesională. Spre deosebire de atributul în sine, care este doar un punct de date, EAA-ul are statutul unui document oficial, emis de un furnizor autorizat. Acest lucru garantează autenticitatea informației și oferă atestării aceeași valoare juridică precum un document tipărit. O atestare electronică poate fi adăugată, stocată și prezentată prin intermediul portofelului digital *EUDI Wallet*, oferind un mod standardizat și securizat de a demonstra atributele personale în mediul digital.

Atestările electronice reprezintă un element esențial în infrastructura identității digitale europene propusă de eIDAS 2.0. Ele permit cetățenilor să-și dovedească anumite caracteristici personale precum vârsta, adresa sau statutul profesional într-un mod sigur, verificabil și interoperabil în întreaga Uniune Europeană.

Conform cadrului propus de eIDAS 2.0, există trei tipuri principale de atestări electronice de atribute:

1. **Electronic Attestation of Attributes (EAA) – pentru utilizări de zi cu zi**

Atestările electronice de atribute (EAA) sunt cea mai simplă formă de credențiale digitale prevăzute de eIDAS 2. Ele sunt emise de organizații publice sau private și confirmă informații specifice despre o persoană sau entitate. Fiind folosite în contexte nereglementate, aceste atestări nu trebuie să respecte cerințe legale stricte, precum cele asociate documentelor oficiale.

EAA-urile sunt utile în situații de zi cu zi, unde este necesară o modalitate practică de a demonstra anumite atribute, cum ar fi calitatea de membru, participarea la un eveniment sau statutul de student. De exemplu, pot lua forma unor bilete de acces, carduri de fidelitate, legitimații de angajat sau abonamente la diverse servicii.

Sunt ușor de emis, eficiente din punct de vedere al costurilor și oferă o soluție simplă pentru gestionarea interacțiunilor de zi cu zi între organizații și utilizatori. Cu toate că nu sunt recunoscute în afara mediului în care sunt emise, ele rămân extrem de utile pentru aplicații interne.

1. **Qualified Electronic Attestation of Attributes (QEAA)**

Atestările calificate de atribute (QEAA) sunt credențiale digitale cu un nivel ridicat de încredere, prevăzute de regulamentul eIDAS 2. Acestea sunt emise exclusiv de *Qualified Trust Service Providers* (QTSP) și sunt supuse unor cerințe stricte privind securitatea, auditarea și conformitatea legală

*QEAA*-urile sunt utilizate în contexte reglementate, unde este esențială validarea legală și securizată a informațiilor, cum ar fi serviciile publice, domeniul medical, financiar sau juridic. Pot atesta, de exemplu, o diplomă universitară, o licență profesională sau un certificat de stare civilă.

Aceste atestări au aceeași valoare juridică precum documentele tipărite și sunt protejate prin mecanisme criptografice avansate, precum sigiliile electronice. Datorită standardelor ridicate de încredere, QEAAs sunt acceptate în toate statele membre ale UE, fiind esențiale în schimburile digitale oficiale.

1. **Public Electronic Attestation of Attributes (PuB-EAA)**

Atestările publice de atribute (PuB-EAA) sunt emise în numele instituțiilor publice sau al autorităților oficiale, atunci când datele provin din registre sau baze de date guvernamentale. Acestea au aceeași valoare juridică precum documentele fizice și sunt folosite în special în servicii publice, cum ar fi emiterea certificatelor de naștere sau a permiselor de conducere.

Furnizorii PuB-EAA nu sunt considerați furnizori calificați de servicii de încredere (QTSP), dar trebuie să dețină un certificat calificat emis de un QTSP pentru a putea semna aceste atestări. În acest mod, se asigură că atestările respectă cerințele legale aplicabile documentelor oficiale, în special pentru verificarea unor atribute precum vârsta, adresa, cetățenia sau calificările profesionale.

## Cazuri de utilizare

Atestările electronice de atribute permit cetățenilor să interacționeze în mod securizat, standardizat și eficient cu servicii publice și private. Acestea sunt deja testate în mai multe scenarii concrete, acoperind domenii precum guvernare digitală, sănătate, educație sau transport. Mai jos sunt prezentate principalele categorii de utilizare definite în cadrul proiectului european:

1. **Permis de conducere -** Portofelul digital permite stocarea și prezentarea permisului de conducere în format electronic. Utilizatorul îl poate folosi la controlul în trafic, la închirierea de autovehicule sau în alte situații unde este necesară dovedirea dreptului de a conduce.
2. **Accesarea serviciilor guvernamentale -** Cetățenii pot accesa servicii administrative online, precum actualizarea datelor personale, solicitarea de documente oficiale sau înregistrarea la vot, utilizând atestări verificate din portofelul digital.
3. **Plăți** - Atestările pot fi folosite pentru autorizarea plăților, verificarea identității la tranzacții sensibile sau pentru a demonstra eligibilitatea în cazul reducerilor/subvențiilor. De asemenea, asigură autentificarea în doi pași în sistemele financiare.
4. **Educație** - Instituțiile pot emite diplome, certificate de studii sau atestări privind statutul de student. Acestea pot fi utilizate în procesul de admitere, la angajare sau pentru mobilitate academică în cadrul UE.
5. **Sănătate** - Portofelul digital poate conține prescripții electronice, cardul european de asigurări sociale de sănătate sau alte documente medicale.
6. **Călătorii** - Check-in-ul la aeroport, rezervările de bilete sau identificarea la hotel pot fi efectuate direct din EUDI Wallet, eliminând nevoia de documente tipărite.
7. **Telecomunicații** - Înrolarea într-un serviciu de telefonie mobilă, portarea unui număr sau semnarea unui abonament pot fi realizate exclusiv online.
8. **Semnătură elecronică** - Utilizatorii pot aplica semnături electronice calificate pe documente digitale.
9. **Identități organizaționale** - Angajații pot primi legitimații digitale cu acces securizat în spații fizice sau în sistemele informatice ale instituției.

## Problemele abordărilor PKI clasice

Sistemele clasice de identitate digitală, bazate pe Public Key Infrastructure (PKI) și certificate X.509, au fost esențiale în securizarea comunicațiilor și autentificarea utilizatorilor în ultimele decenii. Ele funcționează prin emiterea de certificate digitale semnate de autorități de certificare, care garantează legătura dintre o cheie publică și identitatea unei entități.

Totuși, odată cu apariția unor nevoi noi, cum ar fi controlul direct al utilizatorului asupra datelor proprii, verificarea selectivă a atributelor, scalabilitate pentru volume mari de utilizatori și eliminarea punctelor unice de încredere, abordările PKI clasice au început să devină insuficiente. Limitările lor nu mai răspund cerințelor moderne privind identitatea digitală descentralizată, interoperabilă și orientată pe confidențialitate, așa cum sunt definite în inițiative precum EUDI Wallet sau standarde precum Verifiable Credentials și SD-JWT.

PKI-ul are mai multe limitări care încep să se vadă tot mai clar atunci când încercăm să îl folosim în scenarii moderne de identitate digitală. Printre cele mai importante probleme se numără:

1. **Single point of failure – centralizare excesivă**

PKI funcționează pe baza încrederii în autorități de certificare (CA), care au rolul de a valida identitatea unei entități și de a semna certificatele digitale. Problema este că întregul sistem depinde de integritatea acestor CA-uri. Dacă una singură este compromisă, atacatorii pot emite certificate aparent valide pentru orice domeniu, ceea ce compromite securitatea comunicațiilor la scară largă. Cazuri precum DigiNotar sau Comodo au arătat exact acest risc: în urma unor atacuri, au fost generate certificate false care au fost apoi folosite în atacuri de tip man-in-the-middle. Astfel de situații arată cât de periculos este să ai un model în care toată încrederea este concentrată într-un singur punct.

1. **Gestionarea complexă a lanțului de încredere**

În PKI, verificarea unui certificat nu înseamnă doar validarea lui individuală, ci presupune parcurgerea unui întreg lanț de încredere. Acest lanț pornește de la certificatul utilizatorului, trece prin una sau mai multe autorități intermediare și ajunge în final la o autoritate root, recunoscută de sistemul de operare sau de browser.

Această structură introduce o complexitate semnificativă. Dacă o verigă din lanț este configurată greșit sau este compromisă, întregul mecanism de încredere poate fi afectat. Un exemplu clar este cazul CNNIC din 2015, când această autoritate root din China a emis un certificat intermediar către un partener numit MCS Holdings. Partenerul a folosit acel certificat într-un proxy HTTPS care permitea interceptarea traficului. Ca urmare, Google și Mozilla au revocat încrederea în CNNIC și au eliminat-o din listele de CA-uri de încredere.

1. **Revocare greoaie și ineficientă**

În PKI, mecanismele clasice de revocare se bazează pe CRL (Certificate Revocation Lists) și OCSP (Online Certificate Status Protocol). CRL-urile sunt liste statice care pot ajunge rapid la dimensiuni mari, ceea ce le face greu de distribuit și ineficiente în sisteme care au nevoie de verificări rapide.

OCSP a fost introdus pentru a rezolva aceste probleme, permițând verificarea în timp real a unui certificat direct de la autoritatea care l-a emis. Totuși, în practică, OCSP vine cu propriile limitări. În primul rând, implică o întârziere vizibilă la stabilirea conexiunii, întrucât browserul trebuie să aștepte răspunsul de la serverul OCSP. În al doilea rând, compromite confidențialitatea: la fiecare verificare, serverul OCSP poate vedea exact ce site accesează utilizatorul, construind astfel un istoric al comportamentului acestuia online.

1. **Criptografie învechită și pregătire slabă pentru viitor**

Una dintre slăbiciunile PKI-ului clasic este faptul că se bazează pe algoritmi criptografici care, în unele cazuri, nu mai sunt considerați siguri. De exemplu, SHA‑1 a fost folosit timp îndelungat pentru semnături digitale, dar în ultimii ani s-a dovedit vulnerabil la coliziuni, adică două fișiere complet diferite pot avea același hash. Acest lucru a fost demonstrat în 2017, când cercetători de la Google și CWI Amsterdam au generat prima coliziune reală de SHA‑11.

La fel, cheile RSA mai scurte, cum sunt cele de 1024 de biți, nu mai sunt recomandate pentru uz actual, iar pe termen lung chiar și RSA‑2048 va deveni insuficient. Motivul principal ține de progresul în domeniul calculatoarelor cuantice. Algoritmi precum RSA și ECC sunt vulnerabili la algoritmi cuantici speciali, cum ar fi algoritmul lui Shor, care ar putea sparge aceste metode mult mai rapid decât calculatoarele clasice.

1. **Lipsa controlului utilizatorului**

În PKI, identitatea digitală este emisă și controlată de autorități centralizate. Utilizatorul nu poate decide ce informații sunt incluse într-un certificat și nici cui sau în ce condiții acestea sunt prezentate. Certificatele sunt rigide, iar toate datele conținute devin vizibile în momentul utilizării, indiferent dacă sunt relevante sau nu pentru acel context.

Acest model intră în contradicție cu principiile de *self-sovereign identity* (SSI), care susțin că identitatea digitală ar trebui să aparțină utilizatorului, nu unei entități externe. Într-un sistem SSI, persoana își gestionează propriile credentiale și poate alege ce date să dezvăluie, când și cui. De asemenea, principiul *privacy by design* presupune ca sistemele să fie construite astfel încât să minimizeze colectarea și expunerea de date personale încă din faza de proiectare, lucru pe care PKI-ul clasic nu îl oferă.

## Avantaje ale atestărilor electronice

Utilizarea atestărilor electronice de atribute vine cu o serie de avantaje importante, atât pentru cetățeni, cât și pentru instituții sau companii. Aceste beneficii se datorează în primul rând faptului că vorbim despre documente digitale care pot fi verificate automat, sunt recunoscute la nivel european și sunt integrate într-o infrastructură sigură, cum este cea oferită de EUDI Wallet și de cadrul legal eIDAS.

Câteva dintre avantajele principale oferite de aceste atestări sunt prezentate mai jos:

1. **Creșterea eficienței operaționale**

Prin eliminarea documentelor fizice, a copiilor după acte și a verificărilor manuale, atestările electronice reduc semnificativ timpii de procesare în activități precum verificarea identității pentru acces la servicii, înscrierea la o universitate, autentificarea în platforme educaționale sau validarea statutului de student. Pentru organizații, acest lucru înseamnă automatizare, mai puține erori și economii importante de resurse. Organizațiile pot astfel să economisească timp, să reducă volumul de muncă repetitivă și să minimizeze riscurile de eroare.

1. **Securitate sporită**

Atestările electronice sunt semnate digital de furnizori autorizați sau calificați (QTSP) și pot fi verificate criptografic în timp real. Acest mecanism asigură că informațiile nu au fost modificate și că provin dintr-o sursă de încredere. Astfel, atestările devin rezistente la falsificare și oferă un nivel ridicat de încredere în procesul de validare a identității sau a atributelor unei persoane.

1. **Interoperabilitate la nivel european**

EUDI Wallet este construit pe baza regulamentului eIDAS 2.0, ceea ce asigură recunoașterea și acceptarea atestărilor electronice în toate statele membre. Potrivit Comisiei Europene, această interoperabilitate este esențială pentru ca cetățenii să poată folosi aceleași date de identitate în orice stat membru.

1. **Control deplin asupra datelor**

Atestările electronice sunt păstrate direct în portofelul digital al utilizatorului, nu într-o bază de date centralizată. Acest lucru îi oferă control total asupra modului în care își folosește datele: poate alege ce informații să partajeze, cui le transmite și în ce scop. Modelul respectă principiile *privacy by design* și *self-sovereign identity*, în sensul că utilizatorul nu trebuie să dezvăluie mai mult decât este necesar. Astfel, se evită expunerea inutilă a datelor personale și se menține un control real asupra confidențialității.

1. **Scalabilitate și adaptabilitate tehnologică**

Atestările electronice sunt gândite să se integreze ușor în aplicații digitale actuale, fie că vorbim de platforme publice, fie de soluții din mediul privat. Ele pot susține procese digitale în întregime, de la verificarea identității, până la utilizarea semnăturilor electronice și gestionarea accesului la servicii. Pentru că respectă standarde deschise și sunt compatibile cu diverse sisteme, aceste atestări pot fi adaptate ușor în funcție de nevoile unei organizații sau de schimbările legislative. Această flexibilitate le permite să evolueze odată cu tehnologia și să răspundă cerințelor tot mai diverse ale instituțiilor și utilizatorilor.

## Legislație

eIDAS 2.0 este o actualizare a regulamentului european privind identificarea electronică și serviciile de încredere (eIDAS), adoptat inițial în 2014. Noua versiune, publicată oficial în 2024, adaugă noi funcționalități importante și propune o abordare comună la nivelul Uniunii Europene pentru gestionarea identității digitale. Principalul său obiectiv este să ofere cetățenilor, companiilor și instituțiilor un mod sigur și simplu prin care oamenii își pot dovedi identitatea și folosi datele personale oriunde în UE.

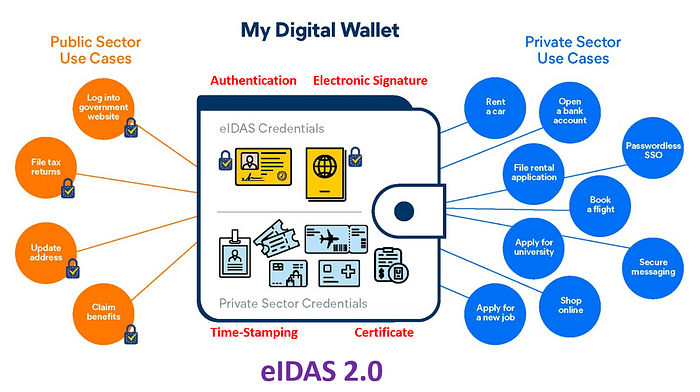
Elementul central introdus de eIDAS 2.0 este European Digital Identity Wallet (EUDI Wallet), un portofel digital standardizat, care va permite cetățenilor UE să stocheze și să utilizeze diverse tipuri de credențiale, cum ar fi datele de identitate (PID), diplome, statut profesional sau alte atestări electronice de atribute. Acest portofel va putea fi folosit atât în relația cu instituțiile publice, cât și cu furnizori de servicii private, fiind recunoscut automat în toate statele membre.

Figura 1 Aplicabilitatea EUDI Wallet în conformitate cu eIDAS 2.0

[[1]](#footnote-1)

Spre deosebire de versiunea inițială a regulamentului, care era orientată în principal pe semnăturile electronice și identificarea online, eIDAS 2.0 vine cu o viziune mult mai largă: construirea unei infrastructuri digitale europene, care să permită utilizatorilor să acceseze servicii din orice stat membru cu aceleași date și nivel de încredere ca în propria țară.

Portofelul digital EUDI va trebui să fie pus la dispoziție gratuit de către fiecare stat membru până cel târziu în 2026. Utilizatorii vor avea control complet asupra datelor lor, putând alege ce informații partajează, cu cine și în ce context. Acest principiu reflectă alinierea eIDAS 2.0 la cerințele GDPR și la conceptele de *privacy by design* și *self-sovereign identity*. Mai exact, datele din portofel nu vor fi partajate automat, ci doar la inițiativa utilizatorului și doar în măsura în care sunt necesare pentru un anumit scop.

Totodată, regulamentul introduce cerințe stricte pentru furnizorii de servicii de încredere (QTSP), care pot emite atestări calificate și pot furniza servicii de semnătură electronică. Aceștia vor trebui să respecte standarde de securitate, interoperabilitate și auditabilitate, pentru a garanta încrederea în ecosistemul european.

eIDAS 2.0 stabilește și recunoașterea juridică automată a documentelor și credentialelor digitale emise într-un stat membru, ceea ce înseamnă că o diplomă digitală eliberată într-o țară UE poate fi folosită direct în altă țară fără traduceri, legalizări sau verificări suplimentare.

Deși inițiativa este primită pozitiv la nivel european, există și opinii critice, mai ales în ceea ce privește riscul de centralizare a datelor și posibilitatea ca portofelul digital să devină un instrument de urmărire sau de colectare excesivă a datelor. Aceste preocupări sunt contrabalansate prin mecanismele de control oferite utilizatorilor și prin obligațiile impuse furnizorilor de identitate și atestări.

eIDAS 2.0 încearcă să facă identitatea digitală mai ușor de folosit, mai sigură și mai clară pentru toată lumea. Cu ajutorul portofelului EUDI, oamenii vor putea să-și dovedească identitatea și alte informații personale într-un mod simplu, fără să piardă controlul asupra datelor lor.

## Standarde

Pentru a asigura interoperabilitate, securitate și transparență în sistemele digitale, implementarea eIDAS 2.0 se sprijină pe o serie de standarde internaționale. Acestea fac posibilă emiterea, stocarea și validarea atestărilor electronice în mod descentralizat, oferind utilizatorilor control real asupra datelor lor.

Unul dintre cele mai importante standarde este *Verifiable Credentials*(VC), dezvoltat de W3C. Acesta definește un format standardizat pentru credențiale digitale, documente care pot conține informații precum identitatea unei persoane, statutul de student, diploma de absolvire sau orice alt atribut verificabil. Credențialele sunt semnate digital de către un emitent și stocate într-un portofel digital, de unde pot fi prezentate unui verificator fără a fi nevoie ca acesta să contacteze emitentul.

Această arhitectură se bazează pe trei roluri esențiale:

* Issuer – entitatea care emite și semnează digital credentialul (ex: o universitate, o instituție guvernamentală)
* Holder – persoana sau organizația care primește și stochează credentialul într-un portofel digital
* Verifier – entitatea care solicită și verifică validitatea credentialului (ex: un angajator, o instituție publică sau o platformă digitală)

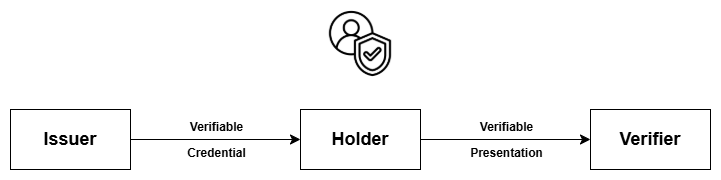
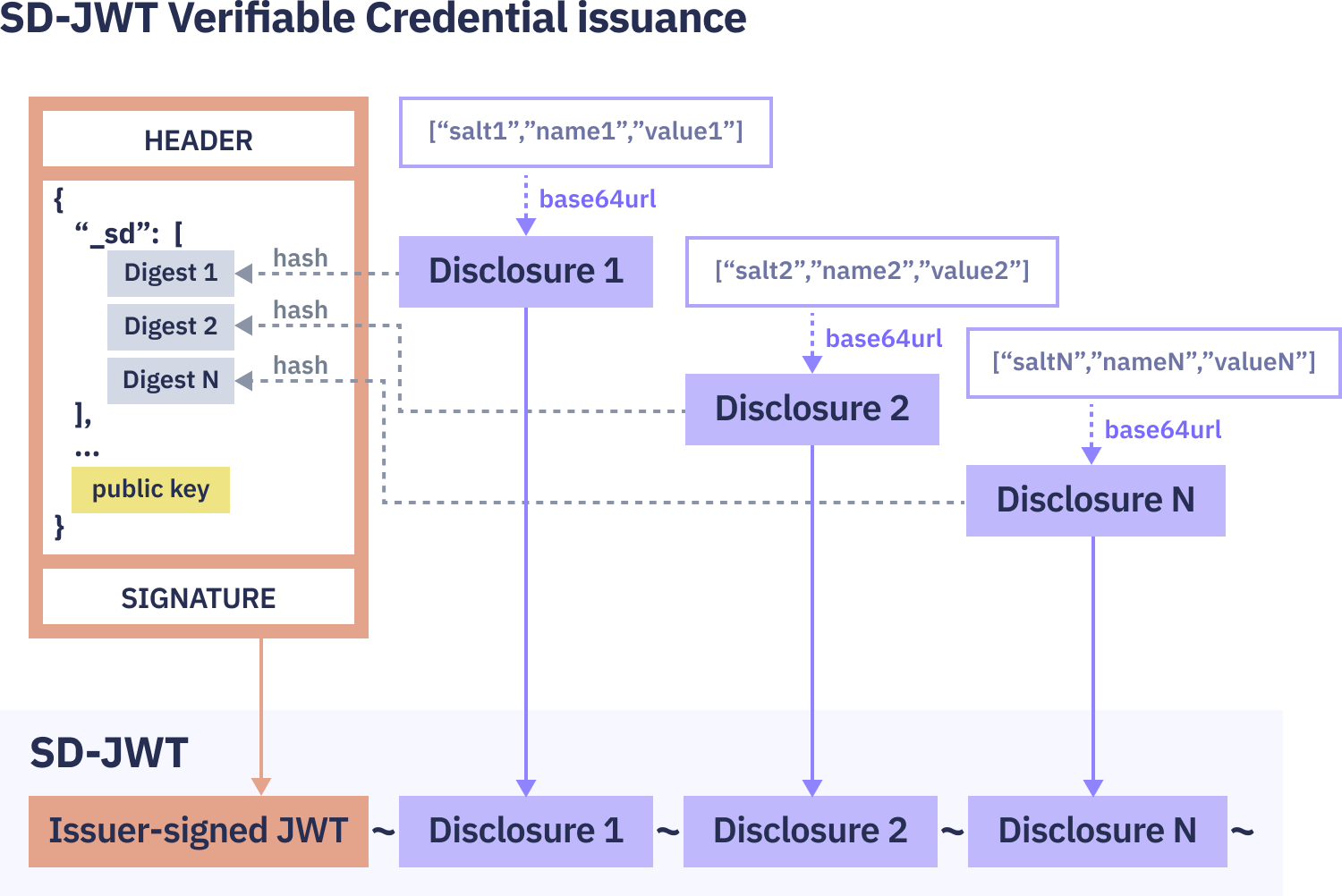


Figura 2 Modelul Issuer–Holder–Verifier în arhitectura Verifiable Credentials

Un alt standard important utilizat în lucrarea de față este SD-JWT (Selective Disclosure JSON Web Token). Acesta extinde formatul clasic JWT și permite ca doar anumite informații să fie partajate dintr-un credențial, păstrând restul datelor confidențiale. De exemplu, un utilizator poate dovedi că are peste 18 ani fără să dezvăluie data completă a nașterii. Tehnic, acest lucru se realizează prin înlocuirea valorilor vizibile cu hash-uri criptografice semnate de emitent, în timp ce valorile reale (numite disclosure-uri) sunt păstrate separat și pot fi prezentate doar la nevoie.

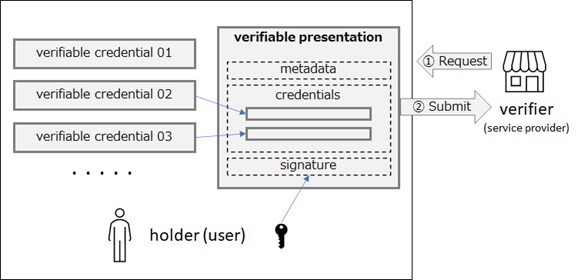
La momentul verificării, portofelul digital trimite prezentarea compusă din JWT-ul semnat și doar disclosure-urile relevante. Verificatorul poate valida integritatea acestora prin recalcularea hash-urilor, fără a avea acces la restul informațiilor din credential. Acest mecanism este compatibil cu infrastructurile existente bazate pe JWT și a fost adoptat în cadrul inițiativelor europene, inclusiv în prototipurile EUDI Wallet. În felul acesta, SD-JWT oferă un control mai bun asupra datelor personale și sprijină aplicarea principiilor din GDPR și eIDAS 2.0 legate de confidențialitate și limitarea informațiilor partajate.

[[2]](#footnote-2)

Figura 3 Structura unui SD-JWT

Pentru prezentarea credențialelor dintr-un portofel digital către un *verifier*, se utilizează protocolul *OpenID for Verifiable Presentations* (OpenID4VP). Acesta extinde standardul *OpenID Connect* și introduce posibilitatea ca o aplicație să trimită o cerere, numită presentation definition, prin care specifică tipul și structura credentialelor dorite. Răspunsul la această cerere constă într-un *Verifiable Presentation* (VP), un document digital semnat care conține unul sau mai multe credențiale și care poate fi validat criptografic de către verificator.

*Verifiable Presentation* este formatul standard prin care un utilizator își poate dovedi atributele digitale într-un mod controlat, selectiv și verificabil. Acest format poate încorpora mecanisme precum SD-JWT VP, care permit dezvăluirea doar a anumitor informații din credentiale, păstrând restul datelor confidențiale. Procesul se desfășoară într-un cadru securizat, în care utilizatorul are control deplin asupra datelor pe care le partajează, iar verificatorul poate valida autenticitatea și integritatea prezentării fără a contacta emitentul.



[[3]](#footnote-3)

Figura 4 Fluxul standard de utilizare a unui Verifiable Presentation

## Studiu comparativ privind cele mai populare platforme disponibile

Atunci când analizăm platformele disponibile pentru gestionarea atestărilor electronice, este important să ținem cont de diferențele semnificative dintre ele în modul în care pot fi utilizate și implementate, funcționalitățile suportate și gradul de conformitate cu standardele europene, precum eIDAS 2.0. Fiecare platformă este dezvoltată pentru un anumit tip de utilizare, de la aplicații de tip portofel digital pentru utilizatori finali, până la soluții complete pentru emiterea și verificarea credentialelor digitale.

De asemenea, unele platforme pun accentul pe simplitate și integrare rapidă, în timp ce altele oferă capabilități extinse și flexibilitate tehnică, fiind dedicate echipelor de dezvoltare sau infrastructurilor publice. Aceste diferențe sunt sintetizate în tabelul următor, care oferă o privire de ansamblu asupra celor mai reprezentative soluții disponibile în prezent:

|  |  |  |  |
| --- | --- | --- | --- |
| **Platformă** | **Tip acces** | **Avantaje** | **Dezavantaje** |
| **EUDI Wallet** | Demo public / gratuit | * Suportă Verifiable Presentations conform specificațiilor eIDAS 2.0 * Asigură interoperabilitate perfectă între statele membre UE și protejează datele utilizatorilor * Ideal ca portofel digital pentru cetățeni, oferind funcționalitate de stocare și prezentare simplă | * Nu permite emiterea sau verificarea credențialelor, doar stocare și prezentare * Funcționalitatea este limitată în versiunea demo * Nu oferă API sau SDK pentru integrare programatică, rol strict de wallet pentru utilizator |
| **walt.id** | Open-source / Enterprise | * Suport complet pentru emiterea și verificarea VC-urilor în formate W3C, SD-JWT și mDoc * Suportă OID4VCI, OID4VP, key-binding, revocare și QR/URL * Administrează chei DID și X.509 prin SDK-uri puternice | * Interfața principală e realizată prin SDK/API, necesită timp și resurse pentru implementare * Complexitatea tehnică ridicată poate reprezenta o provocare pentru echipe mici sau proiecte POC |
| **Talao Wallet** | Open-source | * Emite și verifică Verifiable Credentials, inclusiv formate SD-JWT, prin OID4VCI * Open-source, compatibil EBSI/EUDI, cu încorporare a mecanismelor de disclosure selectiv * Permite integrare rapidă în fluxuri cross-device, QR & URL, plus demo-uri publice pentru utilizatori | * Lipsesc componente grafice și interfețe pentru utilizator final, majoritatea fluxurilor sunt prin CLI/API * Necesită cunoștințe tehnice pentru integrare și scalare |
| **Dock Wallet** | Open-source / comercial | * Permite emiterea și verificarea completă a VC printr-un API și portal no‑code accesibil dezvoltatorilor și organizațiilor * Suport integrat pentru biometrie și backup în cloud * Este compatibil cu ecosisteme EBSI/EUDI și standardul OpenID4VP | * Documentația este uneori incompletă și poate necesita clarificări tehnice suplimentare pentru configurări complexe * Platforma se bazează pe blockchain-ul proprietar Dock |
| **Trinsic** | Comercial (SaaS) | * Oferă un portal no-code * Suportă emitere și verificare de VC cu OpenID4VP și posibilitatea de integrare prin API/SDK * Beneficiază de securitate enterprise | * Model comercial (SaaS) cu costuri lunare, fără opțiune open-source * Nu include mecanisme de selective disclosure (SD-JWT) ieftin și nativ |
| **ZealiD Wallet** | Comercial | * Oferă semnături electronice calificate, conform eIDAS, compatibile cu platforme precum Adobe * Permite stocarea și prezentarea de VC | * Nu oferă emitere directă de credențiale digitale standard prin API * Nu are suport pentru SD‑JWT sau OpenID4VP * Model comercial cu abonament |

Tabelul 1 Analiză comparativă a platformelor utilizate pentru prezentarea, emiterea și verificarea atestărilor electronice

Prin urmare, alegerea unei platforme pentru atestări electronice ține de scopul aplicației, complexitatea integrării și compatibilitatea cu standardele relevante.

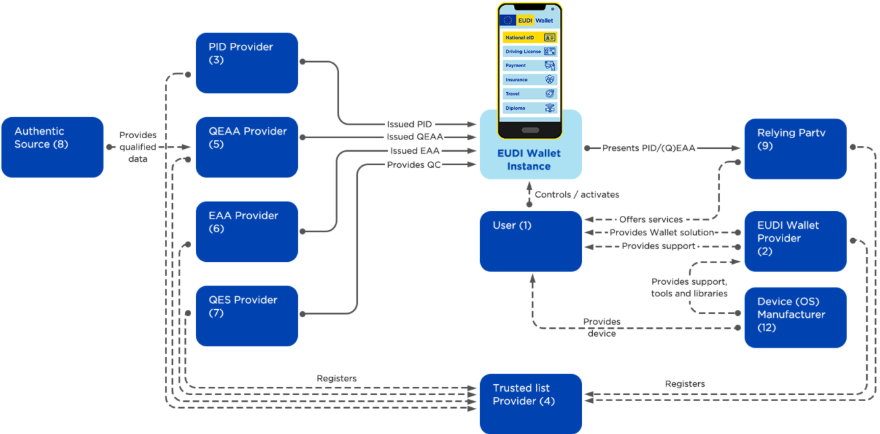
# Arhitectura serviciilor pentru atestări electronice

## Principalele componente

Pentru ca un sistem de atestări electronice să fie funcțional și de încredere, este necesară existența unui set de componente care colaborează într-un mod bine structurat. Fiecare dintre aceste elemente are un rol bine definit în procesul de emitere, stocare, prezentare și validare a credentialelor. Împreună, ele formează o arhitectură construită pe fundamente de securitate, protecția datelor și compatibilitate între sisteme, în conformitate cu cerințele cadrului legal eIDAS 2.0 și cu standardele tehnice internaționale.

În această secțiune sunt prezentate, pe scurt, componentele principale care stau la baza unui astfel de sistem.

1. **Autoritatea emitentă -** entitatea responsabilă cu generarea și semnarea digitală a credentialelor. Aceasta validează datele inițiale despre utilizator și le încorporează într-o structură standardizată, semnată criptografic, care poate fi verificată ulterior de alte părți
2. **Furnizorul de servicii -** entitatea care solicită prezentarea unui credential și realizează verificările necesare privind autenticitatea, integritatea și validitatea acestuia. În funcție de rezultat, stabilește acordarea accesului la un serviciu sau resursă
3. **Portofelul digital –** aplicația prin care utilizatorul își gestionează credentialele.
4. **Deținătorul credențialelor -** utilizatorul final care primește credentialele de la emitent și le prezintă către diferiți verificatori
5. **Trust Framework -** ansamblul de reguli, politici și cerințe tehnice care stabilesc condițiile de funcționare ale ecosistemului
6. **Registrul de încredere -** listă oficială care conține informații despre emitenții, verificatorii și autoritățile recunoscute din sistem
7. **Mecanismele de status –** soluții care permit verificatorilor să determine dacă un credential este încă valabil
8. **Stratul de interoperabilitate -** componenta care cuprinde protocoalele și formatele standardizate ce asigură compatibilitatea între platforme



[[4]](#footnote-4)

Figura 5 Arhitectura serviciilor pentru atestări electronice

## Autoritatea de emitere a atestărilor electronice

Autoritatea de emitere, denumită și „issuer”, este entitatea care se ocupă cu generarea și semnarea digitală a credentialelor electronice. Aceasta are responsabilitatea de a verifica datele despre utilizator și de a construi pe baza acestora un credential digital, semnat criptografic. Semnătura oferă garanția că informațiile sunt autentice și pot fi ulterior verificate de alte entități din sistem. Emitentul poate fi o instituție publică, cum ar fi un furnizor de identitate sau o universitate, sau o organizație privată, dacă este autorizată conform legislației, prin regulamentul eIDAS 2.0.

Procesul de emitere respectă standarde tehnice precum *OpenID4VCI* și *SD-JWT*. După validarea informațiilor, credentialul este semnat digital și transmis portofelului digital al utilizatorului, printr-un flux securizat și bine definit. Acest schimb are loc prin API-uri standardizate, care asigură interoperabilitatea între diferitele componente ale sistemului.

Un aspect important este faptul că emitentul nu are vizibilitate asupra utilizării ulterioare a credentialului. Acest principiu, numit *unlinkability*, este esențial pentru respectarea vieții private, fiind aliniat atât la cerințele eIDAS, cât și la cele prevăzute de GDPR.

Pe lângă emiterea propriu-zisă, autoritatea de emitere are și rolul de a furniza informații privind starea credentialelor. Acestea pot fi puse la dispoziție prin liste de status sau prin mecanisme optimizate, cum ar fi filtrele Bloom, care permit verificarea eficientă a validității unui credential.

## Furnizorii de servicii

Furnizorii de servicii, denumiți adesea *verifiers*, reprezintă entitățile care solicită utilizatorilor să prezinte unul sau mai multe credentiale electronice, în scopul validării anumitor informații. Aceste entități pot fi organizații publice sau private care oferă acces la un serviciu sau resursă condiționat de furnizarea unei dovezi, cum ar fi identitatea unei persoane, vârsta, statutul educațional sau calitatea de membru al unei instituții.

În arhitectura sistemelor bazate pe *verifiable credentials*, rolul verificatorului este de a defini ce informații dorește să obțină, de a primi prezentarea din partea portofelului utilizatorului și de a valida conținutul acesteia. Validarea presupune mai multe etape:

* verificarea semnăturii digitale
* verificarea structurii și formatului datelor
* consultarea *status list-urilor*
* conslutarea listelor de încredere
* analiza informațiilor primite pentru a verifica dacă acestea corespund cerințelor impuse

Pentru a iniția o prezentare, furnizorul de servicii definește o *presentation definition*, un set de reguli tehnice care descriu tipul de credentiale acceptate și atributele care trebuie prezentate. Această definiție este apoi pusă la dispoziția portofelului utilizatorului printr-un cod QR sau un link, de obicei în contextul unui protocol standardizat precum OpenID4VP.

Furnizorul nu are acces la mai multe date decât cele solicitate explicit, ceea ce face ca acest model să respecte principiile de minimizare a datelor și de confidențialitate. Prezentările sunt deseori generate prin mecanisme care permit dezvăluirea selectivă a informațiilor, cum este cazul formatului SD-JWT, oferind utilizatorului control asupra a ceea ce partajează.

Pentru a valida semnătura unui credential, furnizorul se bazează pe informațiile disponibile în registrul de încredere, care conține date despre emitenți recunoscuți și cheile publice asociate acestora. De asemenea, poate interoga un registru de stare, furnizat de emitent, pentru a verifica dacă credentialul a fost revocat.

În funcție de contextul de utilizare, furnizorul de servicii poate fi integrat într-o aplicație mobile, un portal web sau un sistem automatizat. Indiferent de implementare, acesta trebuie să respecte regulile definite de trust framework-ul ecosistemului din care face parte, pentru a asigura interoperabilitatea și încrederea în întregul proces.

## Registrul pentru starea atestărilor electronice

Registrul pentru starea atestărilor electronice este componenta care permite verificatorilor să determine dacă un credential este încă valabil sau dacă a fost revocat sau expirat. Această verificare este esențială pentru menținerea încrederii în sistem și pentru prevenirea utilizării unor credentiale care nu mai sunt de actualitate sau au fost compromise.

Responsabilitatea pentru publicarea și menținerea unui astfel de registru revine emitentului. În funcție de implementare, acest registru poate lua mai multe forme. Una dintre cele mai răspândite este *status list-ul*, un mecanism standardizat care folosește o structură de tip listă de biți (bitstring), unde fiecare poziție corespunde unui credential emis, iar valoarea indică starea acestuia. Această abordare este eficientă din punct de vedere al spațiului și poate fi publicată ca un document static, accesibil oricărui verificator.

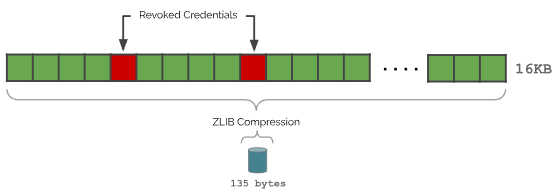
 [[5]](#footnote-5)

Figura 6 Exemplu de listă de revocare în format bitstring

O altă soluție este utilizarea filtrelor Bloom în cascadă, o extensie a filtrelor Bloom clasice, care permite reprezentarea compactă a unui set de credentiale revocate, păstrând în același timp un control precis asupra ratelor de eroare. Acest mecanism presupune o structură pe niveluri, în care fiecare filtru este folosit pentru a corecta eventualele rezultate fals pozitive generate de nivelul anterior. În acest fel, verificarea stării unui credential devine rapidă, eficientă și ușor de scalat, fără a compromite precizia. Mai mult decât atât, această abordare permite protejarea confidențialității, prin adăugarea de elemente fictive care maschează informații sensibile, precum numărul de credentiale emise sau revocate. Filtrele Bloom în cascadă sunt deosebit de utile în sisteme care gestionează volume mari de credentiale, unde este esențial să se obțină un echilibru între performanță, economie de spațiu și protejarea metadatelor.

În proiectarea acestor registre, este important să fie luat în considerare și aspectul legat de confidențialitate, în special proprietatea numită *unlinkability*. Acest principiu presupune că prezentarea unui credential nu ar trebui să poată fi corelată cu o altă prezentare a aceluiași utilizator. În anumite cazuri, modul în care este construit registrul (de exemplu, dacă pozițiile dintr-o status list sunt fixe și identificabile) poate duce la riscul de corelare între sesiuni diferite. De aceea, implementările moderne caută soluții care să reducă această expunere, astfel încât verificarea stării unui credential să nu compromită anonimitatea sau controlul utilizatorului asupra propriei identități.

Indiferent de forma tehnică adoptată, registrul de stare trebuie să fie accesibil public, actualizat periodic și semnat digital, pentru a garanta integritatea informației. Verificatorul consultă acest registru în momentul validării unei prezentări, pentru a se asigura că credentialul prezentat este încă acceptat de emitent.

Gestionarea corectă a stării credentialelor este o cerință fundamentală pentru orice sistem de încredere. Indiferent de soluția aleasă, ceea ce contează este ca verificarea stării unui credential să se integreze firesc în procesul de validare, fără să introducă întârzieri sau riscuri suplimentare legate de securitate sau confidențialitate.

## Listele de încredere

Listele de încredere (Trust Lists) sunt componente esențiale în arhitectura ecosistemului EUDI, deoarece permit stabilirea și menținerea unui cadru de încredere între entitățile participante: emitenți, verificatori, furnizori de portofel, autorități de certificare și alți actori relevanți. Aceste liste oferă un mecanism standardizat prin care se comunică, în mod transparent și verificabil, care entități sunt recunoscute oficial și în ce condiții.

În cadrul EUDI Wallet Architecture & Reference Framework (ARF), listele de încredere sunt structurate și menținute la nivel național de către autoritățile competente, care sunt responsabile pentru înscrierea entităților relevante. Mai apoi, aceste liste pot fi notificate Comisiei Europene pentru recunoaștere între statele membre. Fiecare listă este semnată digital și accesibilă public, pentru a putea fi interogată automat de portofele și verificatori.

Fiecare înregistrare dintr-o listă de încredere conține, în general, informații despre identitatea entității, cheile publice asociate, tipul de servicii oferite, date despre înregistrare și validitate, precum și *endpoint-urile* pentru serviciile suportate. În plus, există și un câmp status, care indică starea actuală a entității în cadrul listei. Valori precum *granted*, *suspended* sau *revoked* permit portofelului sau verificatorului să stabilească dacă o entitate este autorizată să emită sau să verifice credentiale.

Ecosistemul EUDI include mai multe tipuri de liste distincte, fiecare având un scop bine definit: lista pentru furnizorii de portofel, pentru *PID Providers*, pentru autoritățile de emitere a atributelor calificate, pentru entitățile publice eligibile â sau pentru *Relying Parties* care solicită credentiale.

În prezent, conform documentației EUDI, înregistrările din listele de încredere nu sunt publicate într-un format unificat accesibil direct, dar arhitectura specifică modul în care aceste liste trebuie construite pentru a putea fi verificate automat. Fiecare entitate trebuie să fie descrisă într-un format *machine-readable*, precum JSON sau XML, iar lista trebuie semnată digital și să conțină metadate precum versiune, dată de emitere și entitate emitentă.

Un exemplu simplificat de structură pentru un PID Provider poate fi următoarea:

{

"id": "did:example:pid",

"type": "pid\_provider",

"status": "granted",

"name": "Registrul Național de Identitate",

"country": "RO",

"registered\_at": "2025-04-01T00:00:00Z",

"valid\_until": "2026-04-01T00:00:00Z",

"public\_keys": ["https://example.ro/keys/jwks.json"],

"service\_endpoints": {

"openid4vci": "https://example.ro/oid4vci",

"status": "https://example.ro/statuslist.json"

},

"policy\_uri": "https://example.ro/pid-policy"

}

Figura 7 Exemplu de înregistrare JSON pentru un PID Provider

Prin integrarea acestor liste în fluxurile de validare, portofelele și verificatorii pot determina automat dacă o semnătură digitală aparține unei entități autorizate. Astfel, listele de încredere contribuie direct la securitatea și interoperabilitatea întregului sistem, fără a adăuga complexitate pentru utilizatorul final.

## EUDI Wallet

EUDI Wallet este aplicația digitală propusă la nivelul Uniunii Europene pentru a permite cetățenilor să își gestioneze și utilizeze identitatea electronică într-un mod standardizat, sigur și interoperabil. Conform cerințelor regulamentului eIDAS 2.0, portofelul este dezvoltat pentru a funcționa ca un instrument de încredere, prin care utilizatorii pot stoca, accesa și prezenta în mod controlat credentiale digitale emise de entități autorizate.

Aplicația este concepută cu o structură modulară, care combină o interfață ușor de utilizat cu o arhitectură bine structurată. În ecranul principal, utilizatorul are acces rapid la funcțiile principale oferite de portofel: autentificare, partajarea documentelor și semnătura electronică. Interfața este gândită astfel încât funcțiile esențiale să fie ușor de înțeles și folosit, fără să ceară cunoștințe tehnice din partea utilizatorului.

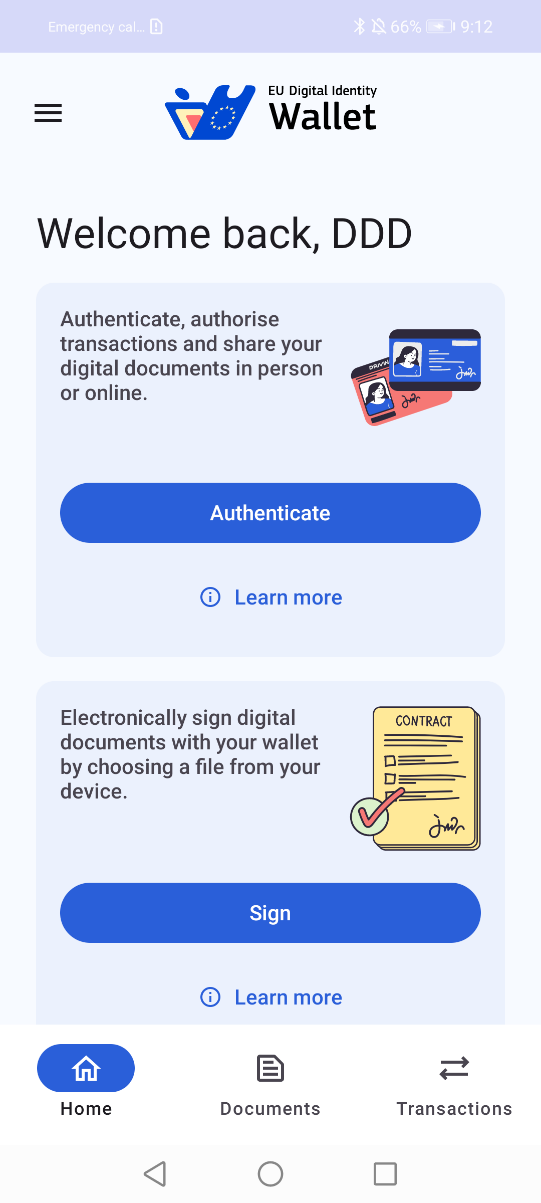


Figura 8 Ecranul principal al aplicației EUDI Wallet

Portofelul permite stocarea de credențiale în formate conforme cu standardele tehnice adoptate la nivel european. Unul dintre cele mai importante este SD-JWT, care oferă mecanisme avansate pentru dezvăluirea selectivă a informațiilor. Astfel, în loc ca un utilizator să prezinte întregul set de date dintr-un document, poate alege să partajeze doar informația necesară în context, cum ar fi faptul că este major, fără a furniza data completă a nașterii.

Credentialele sunt afișate într-o secțiune dedicată a aplicației. În captura următoare se observă două astfel de credentiale: unul pentru identificarea personală (PID), iar celălalt privind absolvirea unei instituții de învățământ.

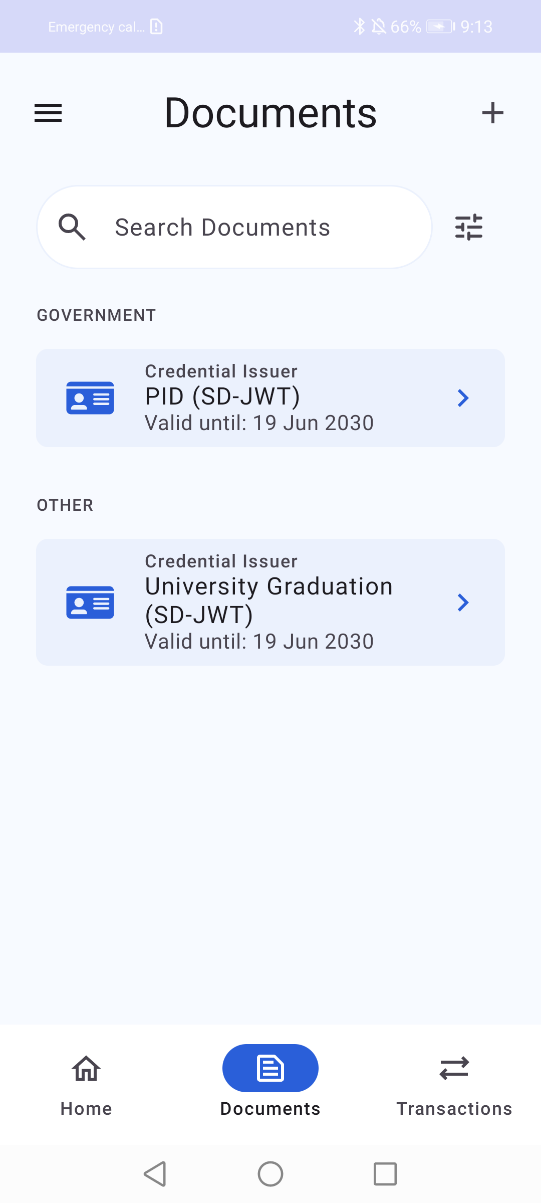


Figura 9 Lista de credențiale electronice stocate în portofel

Fiecare credential poate fi explorat în detaliu, iar aplicația permite consultarea tuturor atributelor incluse în document. În figura următoare este afișat conținutul unui credential PID, cu informații precum vârsta, data nașterii, numele și țara emitentă. Formatul este structurat și lizibil, pentru ca utilizatorul să înțeleagă exact ce informații deține și va partaja:

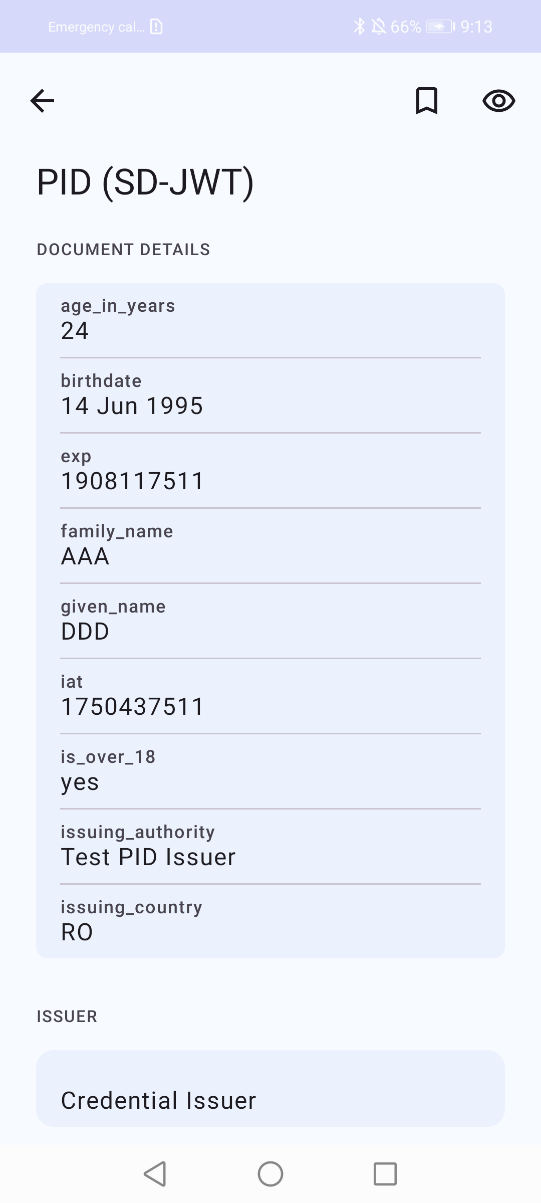


Figura 10 Vizualizarea detaliată a unui credential PID (SD-JWT)

Dincolo de vizualizare și prezentare, portofelul integrează și funcționalități avansate precum generarea de semnături electronice calificate. Acestea sunt conforme cu cerințele eIDAS și pot fi utilizate pentru semnarea de documente digitale într-un mod recunoscut legal. Semnătura este produsă prin utilizarea unei chei private protejate în interiorul unui element de securitatepăstrând cheia strict în interiorul dispozitivului. Acest mecanism asigură atât conformitatea cu legislația europeană, cât și o protecție sporită împotriva abuzurilor.

Aplicația funcționează pe baza unor protocoale standardizate, printre care se numără OpenID4VCI pentru obținerea credentialelor, OpenID4VP pentru prezentarea acestora și ISO/IEC 18013-5 pentru scenarii de utilizare în proximitate fizică. Aceste protocoale permit interoperabilitatea portofelului între toate sistemele conforme din Uniune, indiferent de statul în care este utilizat.

Pe tot parcursul funcționării sale, aplicația respectă principiile de confidențialitate și securitate prin design. Prezentările sunt construite astfel încât să fie imposibil de corelat între ele *unlinkability*, iar portofelul nu înregistrează centralizat istoricul utilizatorului. Toate aceste măsuri contribuie la păstrarea anonimității și la susținerea unui model sigur și transparent de identitate digitală europeană.

## Implementări existente

În ceea ce privește implementările existente, în prezent se remarcă mai multe soluții care oferă funcționalități de tip portofel digital, emitere și verificare a atestărilor electronice.

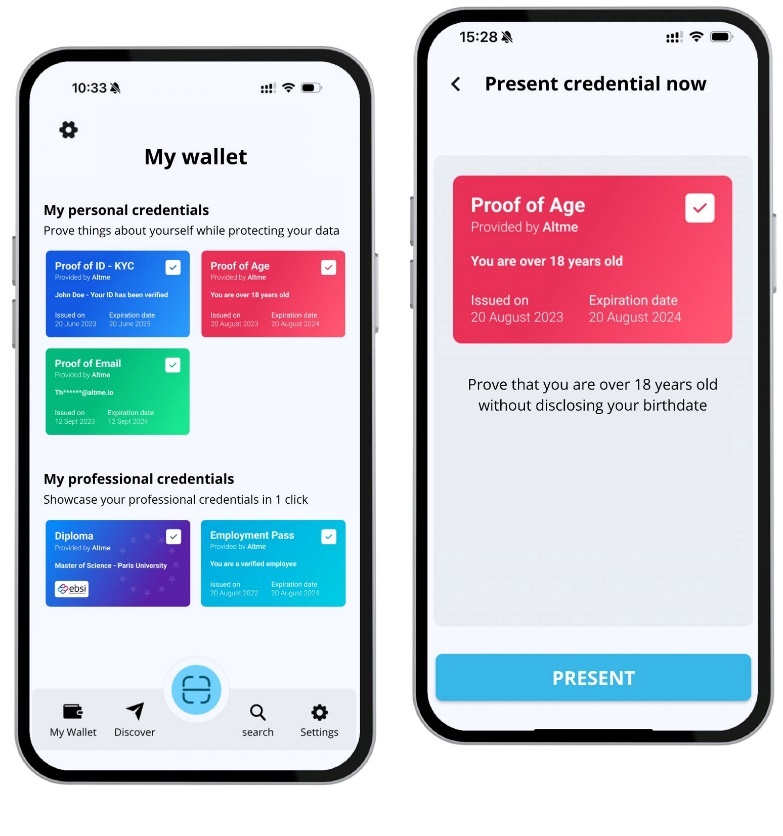
### Talao

Talao este o soluție open-source completă axată pe identitate digitală descentralizată (SSI), care oferă portofel, emitere și verificare într-o singură suită interoperabilă. Apărută inițial în spațiul blockchain, Talao a evoluat către o platformă compatibilă EUDI, conformă cu cerințele eIDAS 2.0, ARF și EBSI‑V3.

În privința componentelor, Talao are un portofel mobile disponibil pentru Android și iOS, programat în Dart (Flutter), cu suport pentru stocare de VC și prezentare selectivă de date. Emiterea este realizată printr-un server *issuer*, capabil să genereze credentiale PID, de vârstă sau alte atribute, cu notificări către portofel utilizând OpenID4VCI. Verificarea se face printr-un serviciu verifier, care gestionează cereri OpenID4VP și validează prezentările primite .

Din punct de vedere tehnic, sistemul implementează protocoalele standard: OpenID for Verifiable Credential Issuance, OpenID for Verifiable Presentations și suport SD‑JWT, oferind și compatibilitate cu profile EBSI și DIIP. Componenta de status folosește *status list* (bitstring) pentru gestionarea revocărilor.

Avantajul distinct este flexibilitatea arhitecturală: componentele sunt separate și independențe, dar pot fi folosite în combinație sau integrat într-un ecosistem mai larg. De exemplu, poți folosi doar *talao-issuer* și integra alt *wallet* propriu, sau doar componenta *verifier*.



[[6]](#footnote-6)

Figura 11 Interfața portofelului Talao

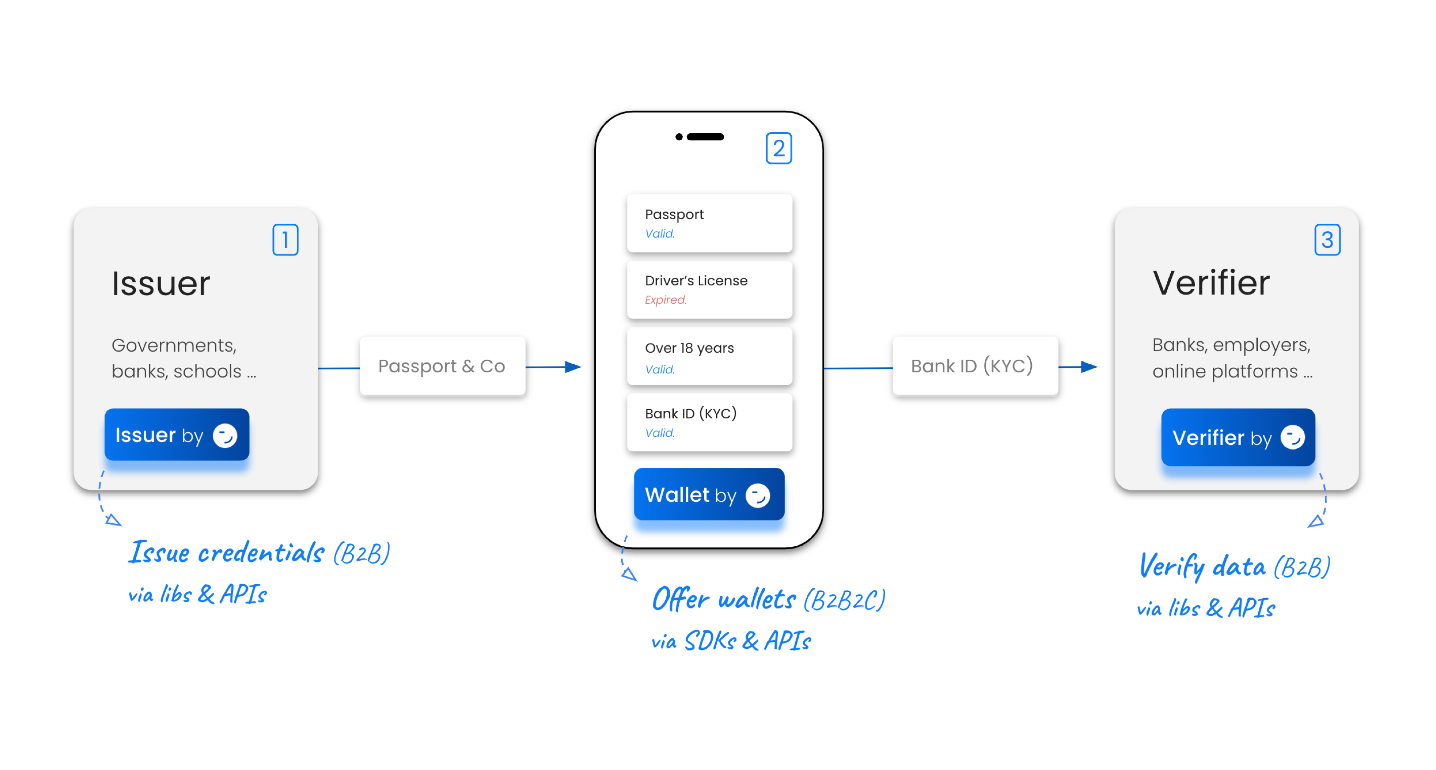
### Walt.id

Walt.id este o platformă open-source de infrastructură pentru identitate digitală și portofel. Scopul său este de a oferi un set complet de instrumente care simplifică adoptarea arhitecturii de tip issuer‑holder‑verifier, respectând standarde cheie precum W3C Verifiable Credentials, OpenID4VCI, OpenID4VP, SD‑JWT și regulamente precum eIDAS 2 și GDPR.

Platforma include un SSI‑Kit, o suită de biblioteci și API‑uri care permit generarea de chei și DIDs, emiterea și verificarea credentialelor, și gestionarea portofelului de identitate. Acest kit este acum integrat în *Walt.id identity stack*, o soluție ce oferă interfețe REST, CLI și aplicații web pentru fiecare rol: *issuer*, *verifier* și *wallet*. Interfața *web‑wallet* permite stocarea, vizualizarea și prezentarea credentialelor, iar aplicațiile issuer și verifier facilitează emiterea prin OIDC4VCI și verificarea prin OIDC4VP/SIOPv2.

Fluxul începe cu generarea DID‑urilor prin API‑uri sau CLI, urmată de emiterea credentialelor în formate JSON‑LD sau JWT/SD‑JWT, stocarea acestora în portofel și prezentarea selectivă către verificatori. Totul este susținut de un sistem de gestionare a revocării prin token status list.

Un avantaj major al Walt.id este că oferă o documentație clară și bine structurată, ceea ce ajută la procesul de integrare și dezvoltare pentru echipele tehnice. Echipa oferă suport comunitar și commercial și consultanță pentru entități guvernamentale și enterprise .

Totuși, utilizarea Walt.id implică operarea și mentenanța infrastructurii backend, ceea ce poate necesita resurse DevOps și atenție la securitate. În funcție de nevoi, pot fi utilizate doar anumite componente ale platformei, fără a fi necesară integrarea întregului sistem.

[[7]](#footnote-7)

Figura 12 Diagrama fluxului Walt.id

### Dock Wallet

Dock este o platformă de identitate descentralizată care oferă infrastructură completă pentru emiterea, stocarea și verificarea credențialelor digitale. Soluția include o rețea blockchain proprie (Dock Chain), dar și un portofel digital disponibil pentru Android și iOS, denumit Dock Wallet.

Dock Wallet este conceput să funcționeze atât pentru persoane fizice, cât și pentru organizații. Utilizatorul poate primi credențiale de la entități acreditate, le poate vizualiza în aplicație și le poate transmite ulterior către verificatori prin fluxuri de prezentare. Aplicația folosește formate de tip JWT și JSON-LD pentru credențiale, iar verificările se bazează pe semnăturile asociate și, acolo unde este necesar, pe statusul publicat de emitenți.

Pe lângă aplicația mobile, Dock pune la dispoziție și un SDK pentru emiterea și verificarea credențialelor, precum și o consolă web destinată organizațiilor care doresc să devină furnizori de atestări electronice.

Un avantaj al Dock este integrarea cu propria rețea blockchain, care permite înregistrarea metadatelor referitoare la credențiale și ancore criptografice pentru verificare. Această abordare oferă un strat suplimentar de încredere și integritate, fără a compromite confidențialitatea datelor utilizatorului. Portofelul nu stochează datele pe blockchain, ci doar semnături și identificatori anonimi, menținând astfel principiul de minimizare a datelor.

Platforma Dock este disponibilă atât sub formă open-source, cât și ca serviciu comercial. Soluția este în continuă dezvoltare, iar compatibilitatea cu standardele europene este în curs de consolidare.

Totuși, Dock nu este încă integrat oficial într-un cadru reglementat precum cel al portofelului european, dar oferă o bază solidă pentru proiecte care vizează adoptarea standardelor deschise și construirea unor sisteme de identitate descentralizată.

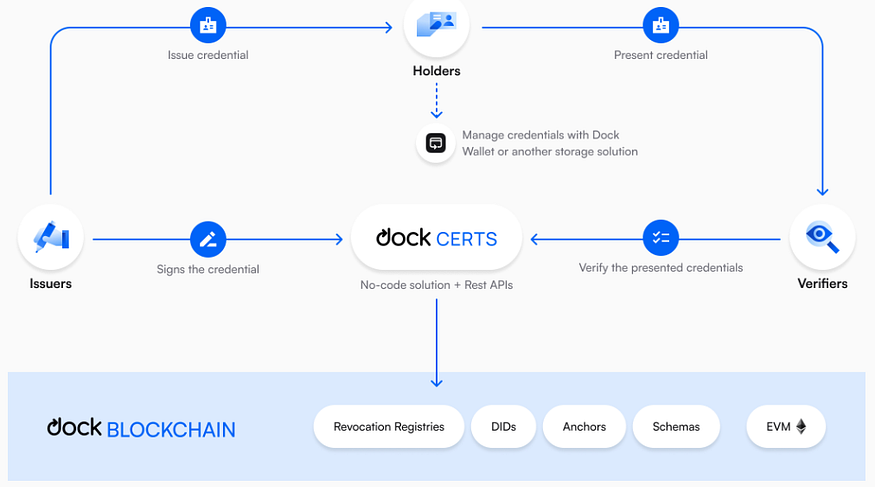
 [[8]](#footnote-8)

Figura 13 Arhitectura Dock Wallet

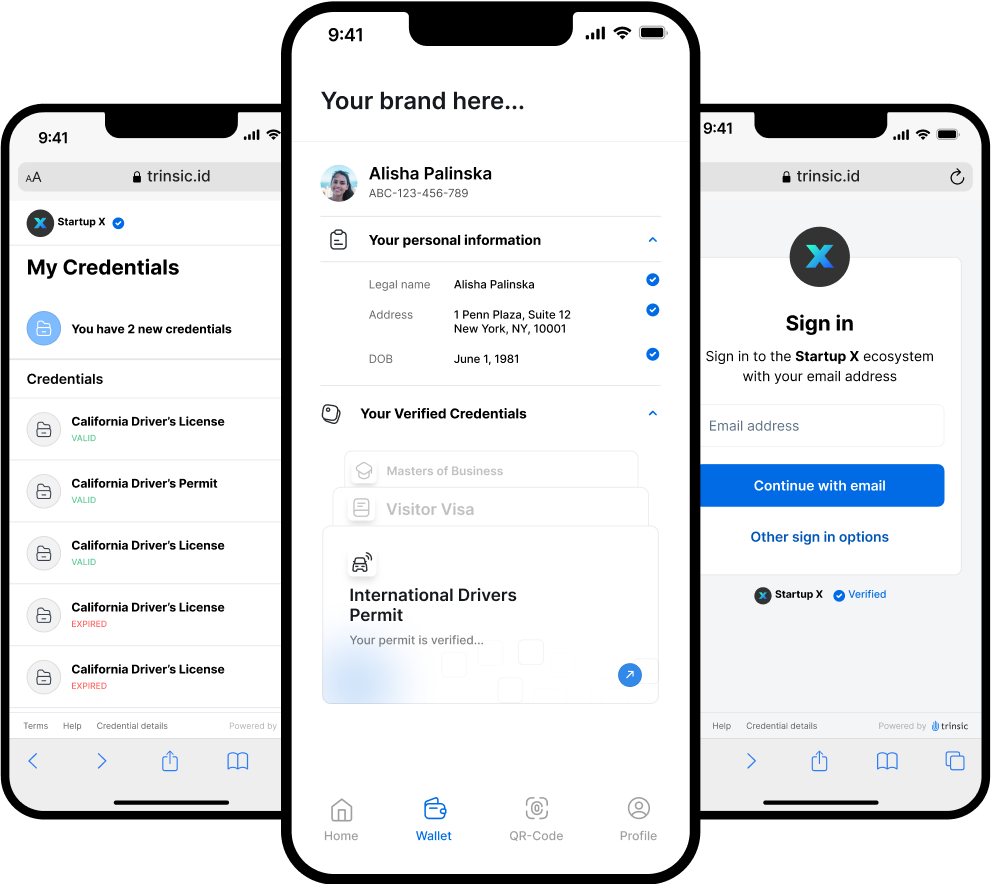
### Trinsic

Trinsic este o platformă comercială dedicată construirii de aplicații și servicii bazate pe identitate digitală descentralizată, punând la dispoziția dezvoltatorilor o infrastructură completă pentru emiterea, stocarea și verificarea credentialelor. Soluția este oferită ca serviciu și include un SDK, API-uri REST și o aplicație portofel care poate fi personalizată sau integrată în aplicații existente.

Platforma este compatibilă cu standardele W3C pentru Verifiable Credentials și utilizează formate de tip JSON-LD. Trinsic sprijină fluxuri de prezentare care respectă principiile dezvăluirii selective. Aplicația este construită astfel încât utilizatorul să păstreze controlul complet asupra propriilor date, fără ca acestea să fie accesibile platformei.

Un element central al ecosistemului Trinsic este Trinsic Studio, o interfață web intuitivă prin care organizațiile pot crea, emite și gestiona credentiale digitale. Prin intermediul acestei console, se pot defini scheme de credentiale, se pot trimite invitații către utilizatori și se pot urmări răspunsurile la cererile de prezentare. Studio-ul este gândit pentru a reduce barierele tehnice și a permite adoptarea rapidă a identității descentralizate chiar și de către organizații fără expertiză tehnică avansată.

Pe partea de integrare, Trinsic oferă SDK-uri pentru mai multe limbaje, precum și API-uri standardizate care permit crearea rapidă de fluxuri de autentificare, onboarding sau verificare. Portofelul furnizat de Trinsic poate fi utilizat ca aplicație de sine stătătoare sau poate fi încorporat în alte aplicații mobile prin SDK.

Limitarea principală a Trinsic este caracterul său comercial, deși oferă o versiune gratuită pentru testare, funcționalitățile avansate și scalarea sistemului necesită un plan plătit. De asemenea, pentru proiecte care urmăresc conformitate strictă cu standardele europene, este necesară o evaluare atentă a compatibilității și eventual integrarea unor componente externe.

[[9]](#footnote-9)

Figura 14 Interfața soluției Trinsic

### ZealiD Wallet

ZealiD este o soluție de identitate digitală certificată la nivel european, care oferă un portofel mobil cu funcționalitate extinsă, inclusiv semnături electronice calificate și gestionarea unui certificat calificat eIDAS.

Portofelul este disponibil pentru Android și iOS, iar funcția centrală o constituie identificarea la distanță a utilizatorului și emiterea unui certificat digital calificat direct în aplicație. Procesul de înregistrare implică verificarea actului de identitate, selfie video cu detectare facială, verificarea numărului de telefon și a unui cont bancar asociat.

Soluția este concepută pentru a funcționa ca portofel de identitate digitală, oferind interacțiune cu servicii externe prin autentificare și semnătură, cu scopul de a înlocui identificarea clasică cu username și parolă în scenarii cu valoare legală ridicată.

Spre deosebire de alte portofele din zona *verifiable credentials*, ZealiD nu este orientată în primul rând către modelul *issuer–holder–verifier* din ecosistemul EUDI/SSI, ci mai degrabă către un model tradițional PKI,dar centrat pe utilizator. Totuși, poziția sa ca QTSP și integrarea cu sisteme de semnătură electronică o fac extrem de relevantă pentru viitoarele cerințe de identitate digitală în Europa, inclusiv în contextul eIDAS 2.0 și al viitorului EUDI Wallet oficial.

Un avantaj major al ZealiD este faptul că soluția este deja în producție, este recunoscută legal și funcționează în regim live pentru semnături calificate, fără intervenția fizică a operatorului uman în procesul de identificare. Limitarea, în schimb, este că ZealiD funcționează mai degrabă ca o aplicație verticală, cu o serie funcționalități fixe, și nu oferă aceeași flexibilitate pentru dezvoltatori precum platforme precum Walt.id sau Trinsic. De asemenea, nu există o infrastructură deschisă pentru *issuer/verifier*, ci mai degrabă o platformă închisă, certificată și gestionată integral de furnizor.



[[10]](#footnote-10)

Figura 15 Interfața portofelului ZealiD

# Descrierea implementării

## Definirea cerințelor

Implementarea acestui proiect are ca scop dezvoltarea unei soluții care să faciliteze validarea atestărilor electronice, în conformitate cu cerințele cadrului european eIDAS 2.0 și ale ecosistemului EUDI. Aplicația oferă suport pentru verificarea semnăturilor și stării credentialelor, precum și integrarea cu portofele digitale.

Scopul general este de a oferi un sistem sigur, scalabil și interoperabil, care să permită instituțiilor sau actorilor privați să verifice în mod automat, rapid și standardizat autenticitatea și validitatea unui credential digital prezentat de un utilizator. Aplicația oferă o interfață intuitivă, un API accesibil și suport pentru standardele și formatele actuale de credentiale electronice, fiind adaptabilă pentru contexte diverse, precum educație, administrație publică sau domeniul juridic.

Punctele forte ale implementării sunt evidențiate prin satisfacerea unor cerințe esențiale, precum:

**Verificarea stării unei atestări electronice**

Una dintre funcționalitățile esențiale ale aplicației este posibilitatea de a verifica dacă o atestare electronică prezentată de un utilizator a fost revocată sau este încă activă. Pentru aceasta, sistemul consultă un registru de stare asociat cu emitentul credentialului. În cadrul implementării, această verificare se realizează prin două mecanisme complementare: un *status list* de tip *bitstring* (conform specificațiilor VC Status List) și o structură avansată de filtre Bloom organizate în cascadă, stocată sub formă de blob stocat în blockchain. Aplicația extrage din credential informația necesară pentru a determina poziția corespunzătoare și evaluează starea acestuia în mod automat, fără intervenția utilizatorului.

**Verificarea veridicității unei atestări electronice prin intermediul listelor de încredere**

Pe lângă starea credentialului, sistemul trebuie să asigure și validitateasemnăturii sale și a emitentului. În acest sens, aplicația consultă o listă de încredere, ce conține entitățile autorizate să emită anumite tipuri de credentiale. Lista include, de regulă, metadate precum chei publice, adrese URL, tipuri de credentiale suportate și nivelul de certificare al fiecărei entități. Verificarea presupune extragerea identității emitentului din credential, compararea acesteia cu informațiile din listă și validarea semnăturii folosind cheia publică corespunzătoare. Doar credentialele emise de entități recunoscute vor fi acceptate de aplicație.

**Verificarea criptografică a atestărilor electronice**

O componentă fundamentală a validării este verificarea criptografică a credentialelor primite din partea portofelului. După ce utilizatorul trimite credentialul, aplicația execută mai mulți pași de validare internă. Sistemul verifică semnătura digitală aplicată de emitent, apoi compară informațiile dezvăluite cu hash-urile stocate în structura credentialului (SD Hashes). Această verificare asigură că datele prezentate nu au fost modificate și că provin din credentialul original semnat. Procesul este automat, iar eventualele erori sunt raportate direct furnizorului de servicii.

**Interfață (API) ușor de utilizat furnizorilor de servicii**

Pentru ca aplicația să poată fi utilizată în contexte reale, de către furnizori de servicii care nu dispun neapărat de infrastructură tehnică proprie, este esențială existența unei interfețe API simplu de integrat. Aceasta oferă funcții precum trimiterea unei cereri de verificare, primirea unei prezentări, rularea validărilor interne și obținerea unui rezultat clar. API-ul este documentat, oferă răspunsuri structurate și este gândit astfel încât să poată fi integrat rapid în aplicații web sau mobile existente.

**Integrare cu EUDI Wallet**

Validarea atestărilor presupune existența unui portofel digital prin care utilizatorul poate transmite credentialele sale. Aplicația este compatibilă cu EUDI Wallet și folosește protocolul OpenID4VP pentru a iniția un proces de prezentare. La nivel practic, acest lucru presupune generarea unui cod QR care conține o cerere de prezentare, iar wallet-ul utilizatorului răspunde la această cerere, trimițând credentialul într-un format standardizat. Acest flux este gândit pentru a funcționa fără intervenții complicate din partea utilizatorului.

**Aplicație mobile pentru verificator**

Pentru a sprijini utilizarea practică a platformei, a fost dezvoltată o aplicație mobile destinată entităților care doresc să verifice atestări electronice. Aplicația joacă rolul unui verificator și poate fi utilizată, spre exemplu, de instituții sau operatori privați care trebuie să confirme anumite informații despre o persoană, cum ar fi vârsta minimă sau statutul de student.

Aplicația generează un cod QR corespunzător unei cereri de prezentare, interacționează cu EUDI Wallet pentru a primi credentialul și comunică ulterior cu backend-ul pentru efectuarea tuturor verificărilor necesare. În urma procesării, aplicația afișează rezultatul validării într-un format clar și ușor de înțeles, simulând experiența reală a unui verificator.

Aplicația este gândită să poată fi distribuită către terți, iar entitățile care doresc să o folosească vor primi un cont dedicat, configurat în funcție de context de propriul context.

**Configurabilitate prin feature flags**

Aplicația mobile include un sistem de *feature flags* care permite adaptarea comportamentului în funcție de nevoile verificatorului, fără a modifica aplicația sau a relansa codul. Prin aceste mecanisme, se poate controla dinamic ce tipuri de informații sunt solicitate dintr-un credential electronic.

Acest sistem oferă flexibilitate ridicată și permite personalizarea cerințelor de validare pentru diferite scenarii. Activarea sau dezactivarea anumitor funcționalități se face din configurare, iar modificările au efect imediat, fără întreruperi în utilizare.

**Instalare și rulare în containere Docker**

Platforma este concepută astfel încât toate componentele sale să poată fi instalate și rulate în containere Docker. Această abordare simplifică procesul de instalare, oferă un mediu izolat pentru fiecare serviciu și permite reproducerea facilă a mediului de execuție, indiferent de sistemul pe care este implementată aplicația.

Folosirea containerizării asigură o gestionare mai ușoară a dependențelor și permite dezvoltatorilor sau operatorilor tehnici să pornească rapid întregul sistem printr-un set minim de comenzi, fără configurări complexe suplimentare.

**Conformitate cu standardele privind atributele electronice**

Credentialele procesate de aplicație conțin atribute electronice conforme cu formatele agreate de comunitatea internațională (W3C Verifiable Credentials) și cele aflate în curs de standardizare în cadrul ecosistemului EUDI. Aplicația este capabilă să interpreteze corect aceste atribute și să aplice reguli de validare asupra lor, de exemplu, verificarea vârstei, a calității de student sau a unei anumite identități juridice.

**Interfață grafică intuitivă**

Aplicația este însoțită de o interfață grafică concepută să fie clară și ușor de utilizat, indiferent de nivelul tehnic al utilizatorului. Navigarea prin aplicație este logică, iar acțiunile principale sunt accesibile în mod direct, fără a necesita cunoștințe avansate.

Elementele vizuale și mesajele afișate în timpul procesului de verificare au fost gândite pentru a oferi o experiență coerentă și prietenoasă, reducând la minimum pașii necesari pentru finalizarea unei validări.

**Respectarea bunelor practici de securitate**

Aplicația este construită respectând bunele practici din domeniul securității software, atât la nivel de comunicare, cât și la nivel de acces și control al datelor. Toate schimburile de informații se realizează exclusiv prin conexiuni criptate, folosind protocolul HTTPS, pentru a preveni interceptarea sau modificarea datelor în tranzit.

Pentru autentificare și autorizare, sistemul integrează Keycloak, o soluție open-source robustă, care permite gestionarea conturilor, a rolurilor și a permisiunilor într-un mod centralizat și sigur.

În cazul aplicației mobile, este implementată și autentificarea biometrică, care asigură protecția accesului la datele locale și la funcțiile critice ale aplicației, fără a compromite experiența utilizatorului.

## Arhitectura soluției

Figura 16 Diagrama de arhitectură a sistemului

Aplicația a fost construită pe o arhitectură bine gândită, care combină mai multe tehnologii moderne pentru a oferi o soluție sigură și ușor de folosit. Fiecare componentă joacă un rol important, iar împreună asigură funcționarea corectă a sistemului, astfel încât utilizatorii să poată valida atestări electronice într-un mod rapid și de încredere. Arhitectura soluției se bazează pe două mari elemente:

* Frontend (interfața grafică, aplicația mobile prin care utilizatorul interacționează cu sistemul)
* Backend (sistemul care gestionează logica aplicației și procesarea datelor)
* Infrastructură și comunicație (componentele care susțin securitatea și distribuția serviciilor)

Fiecare dintre cele trei componente principale ale aplicației este alcătuită din unul sau mai multe module, care colaborează pentru a permite funcționarea corectă a întregului sistem. Aceste module sunt:

* Frontend:
* Aplicația mobile CredCheck, dezvoltată în Android Studio cu Java
* Backend:
* Serviciul principal este dezvoltat cu Spring Boot (Java) și expune o serie de endpoint-uri REST prin care gestionează procesul de validare al credentialelor
* Integrarea cu portofelul digital se face conform specificațiilor OpenID4VP și SD-JWT
* Baza de date PostgreSQL este utilizată pentru logarea evenimentelor
* Registrul de stare este implementat în două forme:
* Status List bitstring, publicabil ca document static
* Filtre Bloom în cascadă, serializate într-un blob și distribuite printr-un nod blockchain
* Keycloak folosit pentru gestionarea autentificării și autorizării serviciilor și a aplicației mobile, pe baza protocolului OAuth2
* Unleash, folosit pentru configurarea dinamică a regulilor de validare, prin intermediul unui sistem de feature flags
* Infrastructură și comunicație:
* Docker folosit pentru containerizarea serviciilor backend, oferind instalare rapidă, izolare și portabilitate între medii
* Cloudflare Tunnel folosit pentru securizarea comunicațiilor externe prin HTTPS și expunerea controlată a serviciilor către utilizatori sau aplicații terțe
* Fiecare serviciu este disponibil printr-un subdomeniu dedicat:
* **auth.credcheck.site** pentru Keycloak
* **flags.credcheck.site** pentru Unleash
* **backend.credcheck.site** pentru serviciul de validare

## Descrierea modulelor componente

### Frontend

Aplicația mobile CredCheck este componenta prin care furnizorii de servicii pot verifica rapid atestările electronice prezentate de utilizatori. Dezvoltată în Java pentru platforma Android, CredCheck oferă o interfață simplă și intuitivă, astfel încât oricine o utilizează să poată efectua verificările fără a avea nevoie de cunoștințe tehnice avansate.

Unul dintre principalele roluri ale aplicației este generarea unui cod QR, care conține cererea de prezentare formulată conform standardului OpenID4VP. Codul este scanat de către portofelul digital al utilizatorului, care trimite direct credentialul semnat către backend-ul platformei. Ulterior, aplicația interoghează backend-ul pentru a obține starea tranzacției.

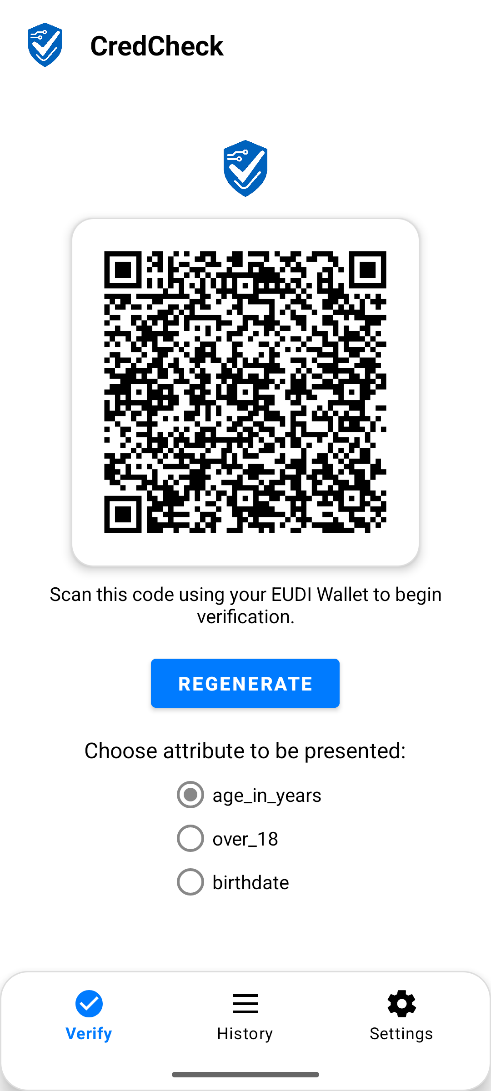


Figura 17 Pagina principală „Verify” a aplicației CredCheck

După generarea și trimiterea credentialului, aplicația afișează rezultatul verificării într-un mod ușor de înțeles, folosind iconuri vizibile și mesaje clare, astfel încât utilizatorul să poată interpreta imediat răspunsul primit. Sunt afișate atât mesajele de acceptare, cât și cele de respingere a credentialelor verificate.

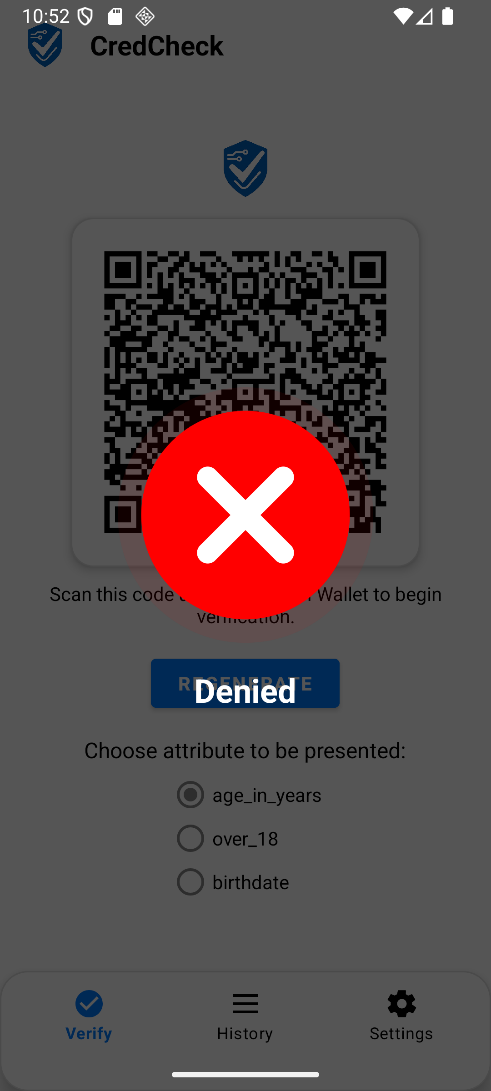
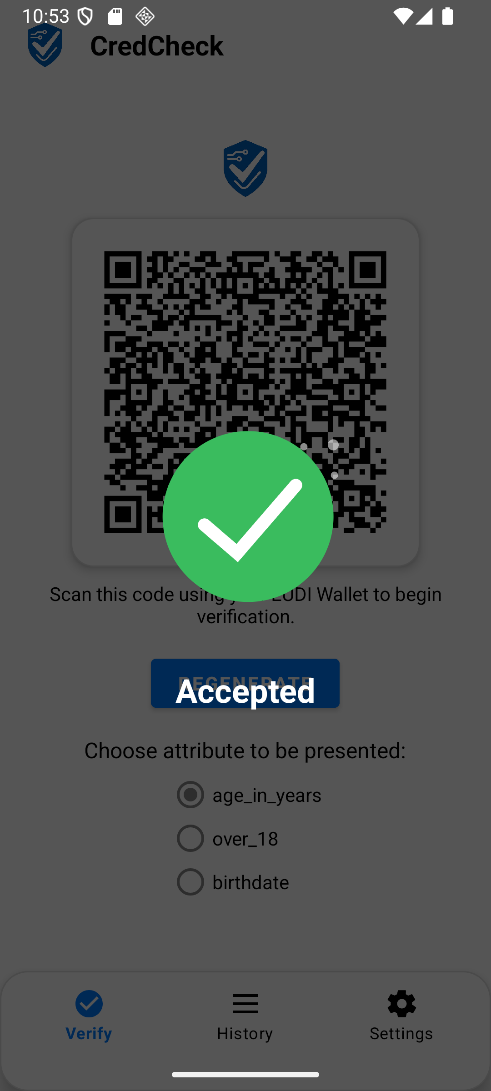


Figura 18 Feedback vizual pentru un credential validat cu succes

Figura 19 Feedback vizual pentru un credential invalid sau respins

Aplicația permite configurarea atributele ce urmează a fi solicitate din credential, prin intermediul unui radio button gestionat dinamic prin feature flags. Astfel, în funcție de scenariul de utilizare, se pot solicita doar anumite date, precum vârsta, confirmarea că utilizatorul este major sau data completă a nașterii.

De asemenea, CredCheck include o secțiune dedicată istoricului tranzacțiilor efectuate, unde utilizatorul poate consulta lista tuturor verificărilor anterioare. Pentru o vizualizare rapidă a statisticilor, aplicația afișează și un grafic de tip pie chart, care evidențiază proporția credentialelor validate cu succes față de cele respinse.

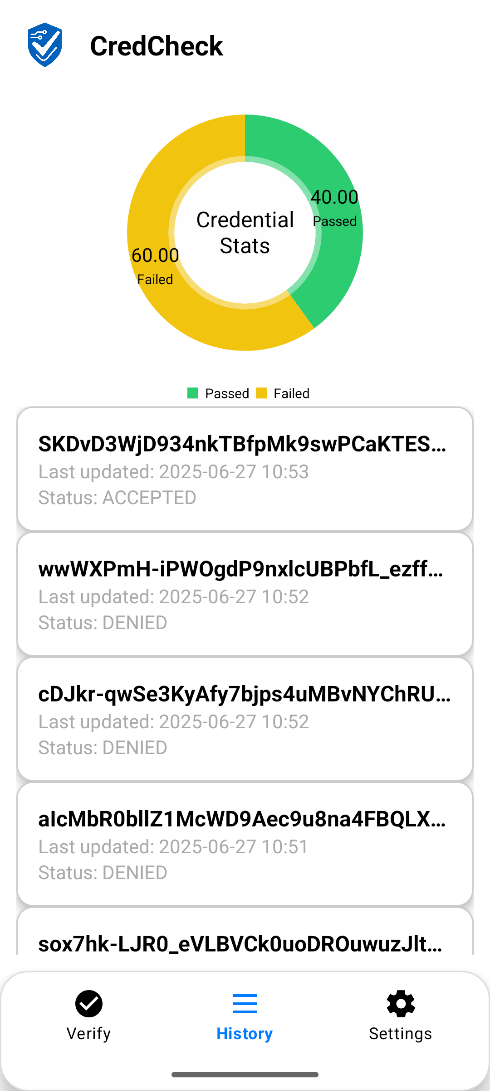


Figura 20 Pagina „History” a aplicației CredCheck

Nu în ultimul rând, aplicația oferă o pagină de setări, unde utilizatorul poate vizualiza informații despre aplicație, cum ar fi versiunea curentă și datele de contact pentru suport. Tot aici există opțiunea de a modifica tema aplicației, alegând între modurile disponibile, precum și posibilitatea de a activa sau dezactiva autentificarea biometrică, pentru un plus de securitate și acces rapid.

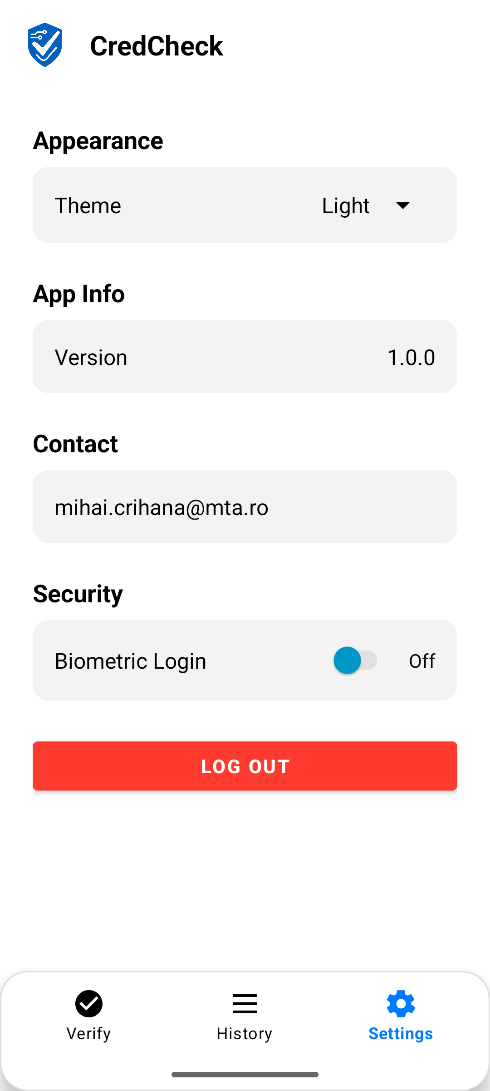


Figura 21 Pagina „Settings” a aplicației CredCheck

Prin integrarea tuturor acestor funcționalități într-o singură aplicație, CredCheck reușește să facă din validarea atestărilor electronice un proces accesibil și rapid, astfel încât utilizatorii să poată folosi această soluție fără dificultăți, indiferent de contextul în care au nevoie de ea.

Fluxul complet al interacțiunilor dintre aplicația mobilă CredCheck, portofelul digital al utilizatorului, serviciul de autentificare Keycloak și backend-ul platformei este ilustrat în *Figura 22*, evidențiind fiecare pas important din procesul de autentificare, generare a cererii de prezentare și validare a credentialelor, pentru o mai bună înțelegere a modului în care aceste componente colaborează în arhitectura sistemului.

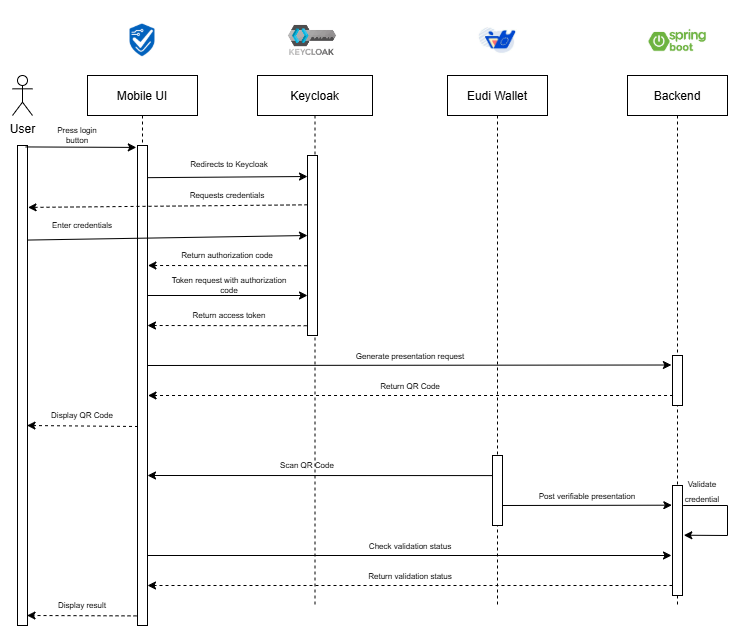


Figura 22 Diagrama de secvență a interacțiunii dintre CredCheck, Keycloak, EUDI Wallet și backend

1. https://medium.com/datafrens-sg/unerstanding-the-eidas-2-0-and-its-implication-for-individuals-privacy-and-data-protection-rights-df0ae62eaafa [↑](#footnote-ref-1)
2. https://www.criipto.com/blog/sd-jwt-based-verifiable-credentials [↑](#footnote-ref-2)
3. https://tsmatz.wordpress.com/2020/06/25/what-is-verifiable-credentials/ [↑](#footnote-ref-3)
4. https://www.intesigroup.com/en/news/eudi-arf/ [↑](#footnote-ref-4)
5. https://www.w3.org/TR/vc-bitstring-status-list/ [↑](#footnote-ref-5)
6. https://www.talao.io/talao-wallet/ [↑](#footnote-ref-6)
7. https://walt.id/white-paper/decentralized-identity-playbook [↑](#footnote-ref-7)
8. https://medium.com/beyond-the-crypto-horizon/time-to-research-dock-aa94158d2bd2 [↑](#footnote-ref-8)
9. https://trinsic.id/platform/ [↑](#footnote-ref-9)
10. https://www.zealid.com/en/identity-wallet [↑](#footnote-ref-10)