

Operaționalizarea comercială a platformei de servicii de autentificare **LegitimId®** www.legitimid.com

Clusterul european inovativ **LegitimId®** anunță lansarea comercială în data de 4 August 2023 a serviciilor puse la dispoziție de platforma de autentificare bazată pe identități digitale **LegitimId®**.

În urma implementării proiectului strategic de cercetare cofinanțat de Uniunea Europeană și Guvernul României care s-a derulat pe parcursul anilor 2020-2023, a fost finalizată platforma tehnică a serviciului **LegitimId®**. Produsele și serviciile de autentificare oferite sunt rezultatul cercetării desfășurate în cadrul proiectului de cercetare strategic cu finanțare europeană **LegitimId®**, realizat de către consorțiul de companii Online Services (leader), Wicom Systems și Next Planet. Cercetarea efectuată s-a concentrat pe o gamă largă de domenii și discipline cuprinzând aspectele legislative privind protecția datelor cu caracter personal, arhitecturile pentru sisteme integrate securizate și reziliente inclusiv cazul situațiilor de dezastru, precum și un important set de tehnologii de ultimă oră printre care enumerăm protocoalele OpenID, tehnologiile criptografice Near Field Communication (NFC), Internet of Things (IoT), Cloud Computing, Deep Mining etc.

Principalele caracteristici ale serviciilor propuse de **LegitimId®**

1. Serviciul **LegitimId®** implementează integral standardul deschis OpenID - scopuri, resurse, profile, revendicări (claims) și roluri, în așa fel încât profilul utilizatorului să fie complet pregătit pentru a satisface cerințele unei multitudini de scenarii de utilizare;
2. Autentificare unică universală (Single Sign On - SSO) bazată pe standardele OpenID Connect și OAuth – ceea ce conferă simultan beneficiarilor productivitate, confort și mai ales siguranță;
3. Autentificare multifactorială, în acord cu cerințele actuale și de perspectivă privind asigurarea unui nivel înalt de încredere;
4. Autorizarea accesului operatorului la date personale sensibile se realizează strict pe baza autentificării, consimțământului și mandatului electronic evaluat în timp real pe baza scopului, rolului și calităților validate pentru momentul accesului aplicând regulamentele GDPR, aspect esențial urmărit în toate etapele proiectului - cercetare, dezvoltare, implementare, testare și exploatarea serviciului **LegitimId®**;
5. Certificarea originii, servicii de combatere a fraudei, imposturii, contrafacerilor;
6. Validarea identității digitale la distanță (videoconferință) devine posibilă prin utilizarea codurilor QR care identifică unic identitățile digitale **LegitimId®**;
7. Opțiunea de autentificare bazată pe utilizarea cardurilor NFC cu procesor criptografic oferă cel mai înalt nivel de încredere, protecție la atacuri de securitate (ex. phishing) dar și autentificare fără parolă, fiind compatibilă cu telefoanele mobile;
8. Utilizatorul își poate configura metoda de autentificare preferată - apel telefonic vocal, SMS, email, autentificator sau transfer optic al autentificării;
9. Utilizarea autentificării pe telefonul mobil pentru exploatarea altor dispozitive sau servicii prin transferul simplificat al identității digitale. Astfel devine posibil ca utilizatorul autentificat pe telefonul mobil să obțină acces rapid la servicii și aplicații Internet aflate pe alt dispozitiv, acces fizic în incinte securizate sau să se autentifice pe stațiile de lucru Windows.
10. Cardurile **LegitimId®** nu afișează și nu stochează date personale. Datele afișate sunt anonime, inutile în cazul pierderii sau furtului. Autorizarea citirii datelor asociate identității digitale **LegitimId®** este acordată numai utilizatorilor autentificați, rezultat al unui proces de validare al multiplilor factori de autentificare;

Produsele care poartă marca înregistrată **LegitimId®** integrează elemente realizate fie pe baza unor brevete proprii fie licențe sau servicii în parteneriat cu companii internaționale.

PRODUSE

Produsele **LegitimId®** sunt componente integrate în sistemul Internet de tip cloud computing care utilizează identitatea digitală **LegitimId®** și protocoale Internet de ultimă generație (OpenID Connect, OAuth) în contextul protecției datelor personale ale utilizatorului, confidențialității și garantând niveluri de asigurare și încredere la cel mai înalt nivel (IAL3, AAL3, FAL3, conform NIST.SP-800-63-3: Digital Identity Guidelines). Asociate cu elementul fizic criptografic NFC - ce nu poate fi copiat sau falsificat - creează premisele pentru utilizare universală în care pe baza autentificării unice (Single Sign ON – SSO) utilizatorul are control asupra utilizării datelor personale și acces rapid autentificat în aplicații web, acces fizic în spații securizate sau pentru operarea stațiilor de lucru. Identitățile digitale **LegitimId®** pot fi utilizate sigur nu numai pentru confirmarea originalității documentelor, obiectelor, operelor de artă etc. respectiv în măsurile de combatere a imposturii, furtului, pierderii și pentru certificarea identității persoanelor de oricare vârstă sau pregătire incluzând persoane cu diferite dizabilități. Identitatea persoanelor, autentificată cu multipli factori pe un dispozitiv mobil poate fi elementul cheie pentru utilizarea altor dispozitive, stații de



lucru, servicii web sau fizice cum ar fi deschiderea ușii unui laborator. Sistemele Internet care utilizează serviciile **LegitimId®** sunt mai sigure, mai productive, actualizate și mai incluzive din punct de vedere social.

1. Legitimații pentru angajați sau carduri de membru în cadrul organizațiilor;

Legitimațiile (sub forma cardului, brățării, inelelor) sunt purtătoarele unor indicatori digitali, care anonimizează datele purtătorului astfel încât legitimația pierdută este inutilă celui care o găsește. Datele proprietarului nu sunt încorporate în legitimație, sunt stocate numai în bazele de date ale organizației emitente, astfel încât protecția datelor personale este asigurată implicit la cel mai înalt nivel. Legitimația poate fi validată numai prin sisteme conectate Internet (ex. telefon mobil) și numai de către instituții sau persoane autentificate și autorizate. Accesul la date personale sensibile este permis numai pe baza mandatului electronic de acces (utilizatorul se află în exercițiul funcțiunii). Posesorul legitimației, precum și organizația emitentă este informată prin sistemul **LegitimId®** de momentele accesului, calitatea solicitantului etc; identitatea digitală asociată legitimației poate fi utilizată și pentru acces fizic, în sisteme de prezență, autentificare în stațiile de lucru Windows, videoconferințe, accesul securizat și autentificat al aplicațiilor web etc.

2. Abonamente protejate la copiere (ex: abonamente pentru transport integrat);

Aceste produse sunt rezultatul preocupării de a minimiza riscul copierii având ca efect imediat reducerea fraudei și respectiv a pierderilor organizației emitente. Abonamentele nu conțin datele personale ale utilizatorului, acestea fiind înscrise și menținute în bazele de date ale organizației emitente conectate cu serviciul **LegitimId®**. Deoarece cardurile (carton, plastic, metal, brățară etc) implementează tehnologia NFC ele pot fi citite cu telefonul mobil în condițiile de securitate impuse de sistem dar și de echipamente fizice cu care călătorii sunt obișnuiți, respectiv echipamente montate în mijloacele de transport, gări, stații, porți de acces etc. Deoarece sistemul **LegitimId®** menține datele asociate serviciilor exclusiv în serverele cloud computing, utilizatorul nu are nevoie decât de propriul telefon mobil pentru a valida electronic utilizarea serviciilor.

3. Bilete unice, netransferabile, protejate la copiere.

Practic sunt deosebite față de abonamente sau carduri doar prin domeniul de utilizare, plecând de la ideea că sunt emise pentru un singur eveniment (concert, transport, spectacol etc.) dar care poate fi utilizat pentru asigurarea securității evenimentului. De exemplu pentru minimizarea riscului terorist, participarea la eveniment presupune validarea identității. Asocierea biletului cu identitatea participantului este efectuată la momentul emiterii. În acest mod, în momentul accesului la eveniment, identitatea celui care prezintă biletul este verificată cu datele înscrise anterior în sistem. Tehnologiile **LegitimId®** asigură mecanismele de combatere a contrafacerii și a imposturii. Astfel se poate asigura fluidizarea accesului, nivelul de securitate necesar și organizarea corespunzătoare a tratării excepțiilor;

4. Cititoare portabile WiFi pentru validarea în timp real a prezenței fizice a persoanelor.

Cititoarele portabile pot fi utilizate în mediul educațional pentru validarea prezenței la examene, în transportul în comun pentru verificarea abonamentelor, biletelor etc. De exemplu, profesorul poate verifica instantaneu cu datele de secretariat livrate prin sistemul **LegitimId®** dacă studentul este cel care pretinde că este, dacă îndeplinește criteriile academice necesare accesului la examen, dacă are obligațiile achitate la zi etc.;

5. Cititoare fixe pentru carduri/abonamente etc. pentru comanda ușilor, barierelor, zăvoarelor după validarea datelor cardului.

Validarea datelor cardului poate fi simplă, respectiv ușa se deschide imediat ce cardul **LegitimId®** este apropiat de cititor, sau validare deosebit de complexă care poate cuprinde următoarele:

- a. Rolul persoanei care deține cardul;
- b. Verificarea momentului (dacă se încadrează în intervalul de timp permis pentru acces). Exemplu: Accesul în laborator pentru persoana X este permis numai de luni până vineri în timpul orelor de program;
- c. Verificarea autorizării pentru accesul în locația solicitată (de exemplu studenții pot intra numai după ce cadrul didactic este prezent și activitatea a fost autorizată de instituție);

Nivelul de securitate privind accesul impune o abordare graduală, de la caz la caz a implementării. Ideea de bază este pe de o parte că sistemul poate fi chiar mai simplu în utilizare decât cel bazat pe accesul cu chei, iar pe de altă parte faptul că poate asigura inclusiv protecția la pierderea cardului sau a furtului etc. Sistemul de acces poate fi implementat astfel încât barierele/ușile să fie acționate prin simpla utilizare a telefonului mobil, sau chiar prin corelare cu sisteme recunoaștere automată video, audio, GPS.

Posesorul cardului confirmă solicitarea accesului prin altă metodă (de exemplu se autentifică utilizând multipli factori de autentificare pe telefonul mobil (smart) personal sau poate răspunde cu Da/Nu la un mesaj SMS trimis de sistemul **LegitimId®**, totul derulându-se în timp real. Complexitatea interacțiunii utilizatorului cu sistemul este reglabilă prin politici impuse de organizație și pot utiliza componente AI pentru detectarea încercărilor de abuz sau fraudă și respectiv impunerea unor politici de acces dinamice în funcție de gradul de încredere calculat dinamic pentru fiecare moment de acces;

6. Cititoare specializate pentru montare în autobuze, vagoane etc.

Acest tip de cititoare au afișaje LCD sunt proiectate și realizate pentru informarea călătorului și validarea costurilor călătoriei. Procesul este coordonat prin conexiunea securizată Internet cu sistemul **LegitimId®**.

7. Info chioșcuri / puncte publice de încărcare credit sau pentru abonamente etc.;

8. Protecția lucrărilor de artă sau a documentelor utilizând chip-uri criptografice încorporate pentru asigurarea imposibilității copierii documentelor dar și certificarea în timp real prin Internet a originalității documentelor

La Expo Dubai 2020 a fost expus prototipul **LegitimId®** privind protecția operelor de artă și a certificatelor de origine;

9. Sisteme logistice. Utilizarea etichetelor NFC înrolate în serviciul **LegitimId®** permite efectuarea inventarierii utilizând telefoane mobile pentru a scana etichetele NFC și pentru completarea automată a listelor de inventariere. Comisia de inventariere are acces instantaneu în momentul scanării etichetelor la datele din baza de date, respectiv la descrierea obiectului, fișa de inventar etc.

10. Sisteme de sigilare unică, cu chip criptografic și detectare automată a violării sigiliului.

Aceste componente, utilizate de exemplu pentru sigilarea ambalajelor, pot fi citite cu telefonul mobil (NFC) în timp real pentru a verifica integritatea sigiliului chiar dacă vizibil nu sunt observate chestiuni deosebite. Ambalajele protejate astfel pot conține mărfuri sau documente cu valoare mare cum sunt documente strict confidențiale, documente unice, care conțin date secrete, obiecte scumpe cum sunt telefoane mobile, bijuterii, piese de schimb originale, etc. Sistemul **LegitimId®** poate informa expeditorul în timp real asupra faptului că sigiliul este citit și starea lui în momentul citirii.

Produsele **LegitimId®** enumerate mai sus nu întocmesc o listă exhaustivă, însă exemplele oferite pot sugera și alt gen de produse sau servicii. Toate produsele enumerate încorporează tehnologii digitale de ultimă generație cum este NFC (Near Field Communication) și Internet of Things (IoT). Tehnologia NFC este omniprezentă în telefoanele mobile smart fiind baza plăților efectuate cu telefonul mobil. NFC permite ca verificarea cardurilor sau a abonamentelor sau biletelor să poată fi efectuată ieftin, public, ocazional doar utilizând telefonul mobil, fără necesitatea de a instala aplicații suplimentare specifice, utilizând doar browser-ul implicit al telefonului mobil.

Alte servicii **LegitimId®**

1. Servicii de integrare a sistemului **LegitimId®** cu sistemele organizației în scopul utilizării accesului securizat, autentificat distribuit și prin protecția datelor personale sensibile (ex: GDPR);
2. Servicii de proiectare, audit tehnic, instruire specializate în domeniul identității digitale;
3. Servicii conexe Clusterului Inovativ European – **LegitimId®**: Evenimente de promovare, acces la documentații, bune practici, specialiști în domeniu etc;
4. Particularizarea produselor fizice: emiteria și particularizarea legitimațiilor, biletelor, abonamentelor, cardurilor etc.;