



(12) CERERE DE BREVET DE INVENȚIE

(21) Nr. cerere: a 2021 00078

(22) Data de depozit: 26/02/2021

(41) Data publicării cererii:
29/11/2021 BOPi nr. 11/2021

(71) Solicitant:
• ONLINE SERVICES S.R.L., STR. UNIRII
BL. C1 AP. 29, BUZĂU, BZ, RO

(72) Inventatori:
• LUPU VIOREL, STR. UNIRII, BL. C8, AP. 4,
BUZĂU, BZ, RO

(74) Mandatar:
LAZĂR ELENA CABINET DE
PROPRIETATE INDUSTRIALĂ,
STR. UNIRII CENTRU BL. 16A SC. C ET. 3
AP. 12, BUZĂU

(54) ANSAMBLU CONSTRUCTIV PLATFORMĂ INTERNET
DE CERTIFICARE ȘI VALIDARE A IDENTITĂȚII
UTILIZATORILOR

(57) Rezumat:

Invenția se referă la un ansamblu constructiv de realizare a unei platforme de servicii de certificare și de validare a identității utilizatorilor destinată să asigure niveluri superioare de securitate pentru accesul la aplicații și platforme cum ar fi, de ex., sistemele de videoconferință destinate examenelor. Ansamblul conform invenției cuprinde un terminal (Di), cu acces la Internet, al unui prim utilizator (U1), conectat în sistem de videoconferință cu un alt terminal (Dt) cu acces la Internet, al unui al doilea utilizator (U2), un terminal (M) telefonic inteligent, aparținând primului utilizator (U1), având funcție de scanner și monitor și cuprinzând sisteme pentru citirea automată a cardurilor și pentru recunoașterea imaginii codurilor QR și un alt terminal (T) având funcția de monitor, aparținând celui de-al doilea utilizator (U2), în care cele două terminale (M și T) exploatează serviciile unei platforme (AuthService), fiind conectate și accesibile, atât prin Internet, cât și printr-un sistem telefonic, și un server (Da) de autorizare al platformei care primește cererile de validare a identității și care are acces, printr-o rețea privată, protejată prin servere (F) de securitate ale platformei, la servicii de baze de date și la un dispozitiv (Dc) de comutație, telefonic, conectat la rețeaua privată a platformei și la serviciul telefonic public care are implementate tehnologii de voce și mesaje scrise, prin care platforma (AuthService), ca urmare a unei cereri de validare a identității primite de la terminalul (M)

telefonic, transmite către terminalul (T) al celui de-al doilea utilizator (U2) un mesaj care informează și determină acțiunea celui de-al doilea utilizator (U2) cu platforma astfel încât, prin terminalul (T) telefonic și platforma AuthService, primul utilizator (U1) primește acces la datele personale ale celui de-al doilea utilizator (U2) în baza de date a platformei AuthService, putând decide cu privire la identitatea corespondentului.

Revendicări: 9
Figuri: 11

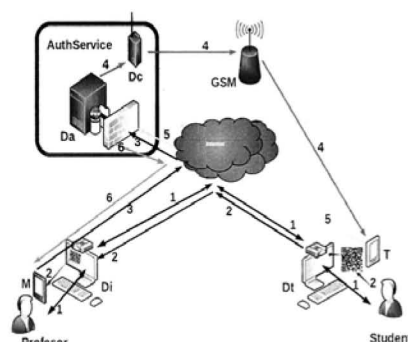
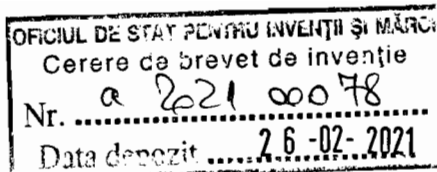


Fig. 1





Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor

Prezenta descriere de invenție se referă la un ansamblu constructiv de realizare a unei platforme de servicii de certificare și de validare a identității utilizatorilor, destinată să asigure nivele superioare de securitate pentru accesul la aplicații și platforme critice cum sunt sistemele de videoconferință destinate examenelor, lucrul la distanță și alte asemenea aplicații.

În stadiu cunoscut al tehnicii au fost identificate câteva soluții apropiate; astfel se cunosc: **Patentul WO2011143729** are ca obiect un sistem antifraudă de protecție împotriva furtului de identitate al utilizatorului în timpul tranzacțiilor pe Internet. Acesta reprezintă o soluție inventivă în care una dintre cerințele fundamentale este posibilitatea combinării cu soluțiile actuale de comerț electronic, sporind securitatea acestora, fără a afecta infrastructura deja existentă și care ia în considerare expunerea excesivă a utilizatorilor pe Internet din cauza rețelelor sociale. În acest scop, sistemul este caracterizat prin aceea că sunt cuprinse procese suplimentare de validare a datelor pentru finalizarea tranzacției, în special validarea dispozitivului de interfață cum este telefonul mobil al utilizatorului; validarea programului de comunicare instalat în dispozitivul de interfață; validarea tranzacției efectuată de către utilizator și validarea tranzacției de către un server de autentificare fără precedent puse în aplicare de către furnizorul de servicii astfel încât serverul de aplicații este conectat printr-o conexiune securizată și printr-un canal de comunicare, în special Internet, la serverul de autentificare, care comunică cu utilizatorul prin intermediul programului de comunicare instalat în dispozitivul de interfață, respectiv telefonul mobil al utilizatorului, pe canalul de comunicare, în special pe Internet.

Sunt identificate următoarele dezavantaje:

- Sistemul este destinat operațiunilor de tip comerț electronic în care este verificată doar identitatea clientului / abonatului;
- Sistemul anti-fraudă nu permite validarea contextuală a utilizatorului prin sisteme de timp real de tip videoconferință

Patentul WO2005083928 care descrie un sistem și o metodă pentru a permite accesul ad-hoc al utilizatorilor în rețelele de comunicații IP fără fir și prin cablu, menținând în același timp și confidențialitatea pentru utilizatori și trasabilitatea accesului pentru furnizorii de servicii. Această metodă cuprinde o interfață de autentificare care permite introducerea elementelor de identificare ale utilizatorului,

precum și o entitate de validare pentru verificarea elementelor de identificare și de autorizarea accesului. Elemente de identificare includ un identificator unic și o parolă creată de sistem. Identificatorul unic este asociat cu o entitate personală a utilizatorului, de exemplu telefonul său mobil. Parola este transmisă utilizatorului prin intermediul unui mesaj de tip SMS pe telefonul său mobil. Sesiunea de Internet a utilizatorului este monitorizată de sistem și toate înregistrările sunt indexate cu numărul telefonului mobil. Acest sistem și metodă permit astfel accesul rapid și trasabil pentru utilizatorii oaspeți în rețelele în care nu sunt deja cunoscuți. Alternativ, utilizatorii nu furnizează identificatorii lor unici, cum ar fi numerele lor de telefon mobil, care sunt deja stocate în sistem. Fiecare utilizator introduce un nume de utilizator și o parolă unică care este creată de sistem și trimisă prin SMS utilizatorului. Acest lucru permite sistemului să valideze identitatea utilizatorului și utilizatorul să valideze identitatea resurselor Internet.

Sunt identificate următoarele dezavantaje:

- Sistemul este destinat accesului trasabil, în calitate de oaspete al rețelilor de comunicații (ex. WiFi) în care este verificată centralizat identitatea clientului / abonatului;
- Sistemul nu este adaptabil pentru a permite validarea contextuală a utilizatorului prin sisteme de timp real de tip videoconferință

Patentul US 6078908: Invenția se referă la o metodă și la un dispozitiv pentru autorizarea în sistemele de transmisie a datelor care utilizează numere de autorizare a tranzacției (TAN) sau o parolă comparabilă. Conform unui prim pas, utilizatorul trimite o identificare calificativă a aparatului de introducere a datelor împreună cu o cerere pentru generarea sau selectarea unui număr de autorizație de tranzacție TAN sau a unei parole comparabile dintr-un fișier de date de la aparatul de introducere a datelor către o autorizație calculator. Într-un al doilea pas, computerul de autorizare generează numărul autorizației de tranzacție TAN sau parola comparabilă sau le selectează pentru a forma un fișier de date. Conform unui al treilea pas, computerul de autorizare trimite numărul autorizației de tranzacție TAN sau parola comparabilă pe o a doua cale de transmisie diferită de prima cale de transmisie către un monitor, de exemplu un pager. Conform unui al patrulea pas, utilizatorul citește acest număr de autorizație de tranzacție TAN sau parola comparabilă de la receptor și introduce numărul de autorizare de tranzacție TAN sau parola comparabilă în aparatul de introducere a datelor. Conform celui de-al cincilea pas, acest număr de autorizare a



tranzacției TAN sau parola comparabilă este transmis către computerul de autorizare. Conform unui al șaselea pas, computerul de autorizare verifică validitatea numărului de autorizare a tranzacției TAN sau a parolei comparabile pentru a stabili sau comuta gratuit, conform unui al șaptelea pas, o conexiune între aparatul de introducere a datelor și unitatea receptor.

Sunt identificate următoarele dezavantaje:

- Procedura este inițiată de către utilizator prin manevrarea tastaturii terminalului;
- Sistemul nu poate fi exploatat de persoane cu dizabilități fără ajutor uman suplimentar;
- Mesajele pot fi retransmise electronic (automat prin mijlocirea unor programe) într-o fereastră de timp necontrolabilă de către sistem astfel încât face posibilă exploatarea sistemului de către o altă persoană aflată la distanță. Riscul de securitate este redus, dar garanția prezenței utilizatorului în fața terminalului nu poate fi asigurată.
- Sistemul nu este adaptabil pentru a permite validarea contextuală a utilizatorului prin sisteme de timp real de tip videoconferință;

Patentul US 20070107050A1 descrie o procedură simplă realizată prin procesarea de coduri alfanumerice text, coduri pe care utilizatorul le citește de pe ecranul dispozitivul WAP/WML și le introduce în computer utilizând tastatura. Nu sunt referințe despre validitatea în timp a mesajelor. Sunt identificate următoarele dezavantaje:

- Procedura este inițiată de către utilizator prin manevrarea tastaturii terminalului;
- Sistemul nu poate fi exploatat de persoane cu dizabilități fără ajutor uman suplimentar;
- Mesajele pot fi retransmise electronic (automat prin mijlocirea unor programe) într-o fereastră de timp necontrolabilă de către sistem astfel încât face posibilă exploatarea sistemului de către o altă persoană aflată la distanță. Riscul de securitate este mai mic, dar garanția prezenței utilizatorului în fața terminalului nu poate fi asigurată;
- Sistemul nu este adaptabil pentru a permite validarea contextuală a utilizatorului prin sisteme de timp real de tip videoconferință;

Patentul US 8917826B2 descrie un sistem și o metodă pentru eliminarea riscului de securitate "*man in the middle*". Sistemul conform patentului conține un subsistem telefonic vocal interactiv IVR. Utilizatorul inițiază procedura la terminal după care

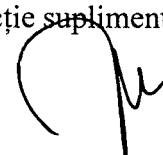


validează codul de acces în interacțiune cu sistemul IVR prin tastele telefonului. Sunt identificate următoarele dezavantaje:

- Procedura este inițiată de către utilizator prin manevrarea tastaturii terminalului și a tastaturii sistemului telefonic;
- Sistemul nu poate fi exploatat de persoane cu dizabilități fără ajutor uman suplimentar;
- Sistemul rezultate este complex utilizând servicii telefonice interactive voce IVR;
- Este posibil cel puțin un scenariu în care utilizatorul care interacționează cu sistemul telefonic nu se află în fața computerului care afișează codul de acces;
- Sistemul nu este adaptabil pentru a permite validarea contextuală a utilizatorului prin sisteme de timp real de tip videoconferință;

Problema tehnică pe care o rezolvă invenția este realizarea constructivă a unei platforme Internet de certificare și validare a identității utilizatorilor printr-un sistem informatic distribuit, tolerant la defecte și cu disponibilitate permanentă, asistat de o structură economică și de servicii care permit dar nu sunt limitative la protecția datelor personale conform cu legislația curentă, profilarea accesului la date de tipul „*need to know basis*” corespunzător caracteristicilor sau profilului entității care le solicită, asigurarea controlului datelor personale de către proprietarul lor, impersonalizarea datelor sensibile, generarea identităților digitale, profilarea identității digitale, asocierea cu identități fizice, asigurarea unor servicii complexe legate în principal de securitatea accesului la date, reducerea riscurilor privind protecția datelor, calitatea serviciilor, consultarea identității de autentificare pentru federalizarea autentificării.

Platforma constructivă este realizată dintr-un terminal Internet al unui utilizator conectat în sistem de videoconferință cu un terminal Internet al unui utilizator pentru desfășurarea sesiunilor de videoconferință și un terminal telefonic inteligent cu funcție de scanner și monitor, care are în configurație subsisteme pentru citirea automată a cardurilor, recunoașterea imaginii codurilor QR afișate prin terminalul Internet, care exploatează autorizat serviciile Internet al unei platforme AuthServices, conectat și accesibil prin sistemul telefonic și Internet, având și funcția de inițiator al cererii de validare al identității, aparținând utilizatorului, pentru care sunt asigurate sisteme de protecție suplimentară și dintr-un terminal telefonic inteligent cu funcția de monitor, conectat și accesibil prin sistemul telefonic și Internet, aparținând utilizatorului, pentru care sunt asigurate sisteme de protecție suplimentară,



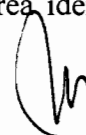
care exploatează serviciile Internet ale platformei AuthServices și dintr-un server autorizare Internet al platformei AuthServices care primește cererile de validare a identității și care are acces prin rețeaua privată protejată prin servere de securitate ale platformei AuthServices la servicii de baze de date și la dispozitivul de comutație telefonic, conectat la rețeaua privată a platformei AuthServices și la serviciul telefonic public ce are implementate tehnologii voce și mesaje scrise SMS fiind realizat și printr-o fermă de servere pentru asigurarea comunicațiilor de mare volum prin care platforma AuthServices urmare a unei cereri de validare a identității primite de la terminalul autorizat, transmite către terminalul utilizatorului un mesaj care informează și determină interacțiunea utilizatorului cu platforma constructiva astfel încât prin terminalul inteligent autorizat și platforma AuthServices primul utilizator primește accesul la datele personale ale utilizatorului din baza de date a platformei AuthServices putând decide în cunoștință de cauză asupra identității corespondentului.

Terminalele telefonice inteligente oferă sisteme de protecție suplimentară cum sunt cele implementate în sistemele Android, Windows, IOS, respectiv autentificare biometrică, cu parolă, cod personal numeric PIN sau gesturi.

Terminalele pentru desfășurarea sesiunilor de videoconferință sunt un computer, o tabletă, un telefon mobil inteligent, un e-reader, care exploatează serviciile Internet ale platformei (AuthServices) și oferă sisteme de protecție cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, PIN sau gesturi.

Serviciul platformei constructive este un serviciu Internet, de tip cloud-computing, software as a service (SAAS) proiectat să respecte legislația privind protecția datelor personale și o serie de restricții ale sistemelor de operare Linux, Android, Apple, Microsoft, și este exploatabil exclusiv în browser, Chrome, Chromium, Edge, Firefox, Samsung, Mi, Opera, Safari și nu utilizează tehnologii precum trackers, localizare, GPS, date biometrice sau tehnologii pentru urmărirea activității utilizatorilor, nu se instalează în sistemul de operare și nu depinde de aplicații care trebuie să fie instalate de către utilizator, browser-ele incluse în telefoanele mobile sau tablete includ implicit posibilitatea scanării codurilor QR.

Primul utilizator prezintă codul QR în fața unei camere de luat vederi a dispozitivului, de pe ecranul telefonului mobil sau de pe o legitimație fizică care are imprimat codul QR, până când acesta este afișat de terminalul în sesiunea video pe ecranul primului utilizator care scanează codul QR de pe ecranul videoconferinței cu ajutorul telefonului mobil inteligent, care deschide automat un browser Internet și care generează o sesiune Internet cu serviciul de autentificare AuthService desemnată în codul QR scanat, prin care solicită automat validarea identității digitale a celui de-al doilea utilizator.



Dacă identitatea utilizatorului doi este cunoscută în baza de date a platformei , atunci sistemul de autentificare pe baza informațiilor din baza de date emite către dispozitivul de comunicație telefonic conectat la rețeaua privată AuthServices un mesaj de avertizare SMS către numărul de telefon al utilizatorului doi, mesajul SMS conține un link unic prin care utilizatorul doi este informat asupra procesului de validare, acționarea link-ului deschide automat o sesiune Internet în browser-ul telefonului mobil prin care este informat de către cine a fost inițiat procesul de validare și cu ce scop și poate opta în cunoștință de cauză asupra opțiunii de a permite accesul la datele sale personale.

Opțiunea utilizatorului doi este colectată în browser-ul telefonului mobil și este transmisă serviciului de autentificare, respectiv utilizatorului unu, informații care permit utilizatorului acestuia să compare și să decidă dacă utilizatorului doi este cel care este posesorul validat al identității digitale prezentate.

Opțiunea utilizatorului doi este colectată în browser-ul telefonului mobil și este transmisă serviciului de autentificare, respectiv utilizatorului unu, informații care permit utilizatorului acestuia să compare și să decidă dacă utilizatorului doi este cel care este posesorul validat al identității digitale prezentate.

Utilizatorul unu se autentifică în prealabil, definește evenimentul în calendarul activităților, scanează codul QR aferent identității digitale a evenimentului după care, ulterior, scanează codurile QR ale utilizatorilor doi participanți la eveniment în timpul acestuia, când sistemul ofera automat datele necesare validării persoanei, astfel încât utilizatorul unu poate analiza și decide în ce măsură persoana prezentată la eveniment este cea înscrisă.

Invenția prezintă următoarele **avantaje** :

- se pot aplica în sistemul de legitimare și certificare al identității la distanță, în timp real:
 - studenților și cadrelor didactice
 - pacienților și medicilor angajați în sistemul de telemedicină;
 - medicilor din centrele de transplant autorizate în relație cu autoritățile competente;
 - medicilor care sunt implicați în sistemul medical pentru donare și transplant;
 - avocaților, procurorilor și judecătorilor în procesul sesiunilor în sistem la distanță;



- membrilor diferitelor organizații distribuite teritorial în zone geografice mari sau greu accesibile, pentru certificarea calității de membru și a drepturilor de participare la evenimente etc.;
- verificarea calității în barouri de avocați, instituții de învățământ, alte domenii;
- certificarea în timp real a mărcilor, producătorilor, documentelor etc.
- pentru lupta împotriva falsului, imposturii, fraudei;

Se dă în continuare un exemplu de realizare al invenției în legătură cu **figurile 1 si 2**, care reprezintă:

- fig. 1 – ansamblu constructiv – platforma;
- fig. 2 – diagrama de funcționare;
- fig. 3-11 – afisaj ecran etape de verificare, verificare si validare utilizator.

Sistemele de videoconferință au devenit un mijloc de desfășurare a examenelor orale și al altor activități ce presupun munca de la distanță, aceste noi modalități de desfășurare a activităților implică și multe probleme tehnice și de securitate, în special lipsa mijloacelor pentru verificarea identității participanților la întâlnirile video prin Internet.

Într-un exemplu de realizare al invenției, *Ansamblu constructiv – platformă Internet de verificare și validare a identității utilizatorilor* cuprinde:

- Sistem hardware, software și de comunicații structurat în două sau mai multe noduri active, care asigură disponibilitatea serviciilor în caz de dezastru. Cele două noduri active completează infrastructura existentă, care dispune de o serie de echipamente instalate în nodul central de comunicații;
- Departament de cercetare industrială prin care produsele de identitate digitală și serviciile sunt definite și realizate;
- Departament pentru generarea identităților digitale, înrolarea lor în sistemul informatic;
- Departament pentru realizarea token-urilor (carduri, inele etc.);
- Departament pentru relația cu clienții;
- Departament de instruire;
- Departament tehnic, de întreținere, testare etc.;
- Departament pentru dezvoltare software, inclusiv integrarea serviciilor în cadrul infrastructurilor de securitate existente la clienți;

Sistemul informatic este realizat cu ajutorul tehnologiilor de tip cloud-computing, având la bază comunicații Internet de bandă largă. Disponibilitatea permanentă a serviciilor



va fi asigurată prin utilizarea echipamentelor și tehnologiilor avansate adecvate, respectiv prin distribuirea puterii de calcul în timp real în noduri de comunicații distribuite geografic, canale de comunicații redundante (fibră optică, radio, telefonie și date mobile), servere tolerante la defecte utilizând tehnologii (RAID, ECC etc.) și servicii de detecție automată și corecție automată a erorilor (date, comunicații, procesare, stocare, baze de date).

În prezent sunt pe piața servicii care răspund parțial la aceeași nevoie ce urmează a fi adresată și de *Ansamblu constructiv – platformă Internet de certificare și validare a identității utilizatorilor*, printre aceste cele mai populare sunt:

- Autentificare pe bază de nume și parolă (tip cont predefinit);
- Autentificare - Platforma pe bază de token / cryptocard și PIN;
- Autentificare în doi pași (tip 2fa): user/pass și token / SMS;

Însă nici una dintre acestea nu realizează un grad de securizare atât de înalt ca în cazul soluției propuse deoarece:

- Platformele de videoconferință sunt în general deschise și permissive astfel încât obiectivul autentificării este readucerea nivelului de utilizare neautorizată a serviciului, limitându-se în cazul platformelor de videoconferință cu plată doar la validarea contului celui care inițiază sesiunea.
- Sistemele actuale de autentificare sunt proiectate pentru autentificarea utilizatorilor pentru exploatarea serviciilor;

Dezavantajele enumerate mai sus sunt demontate deoarece:

- Noua platformă constructivă, conform invenției, utilizează două medii de comunicații complet distincte în procesul de autentificare;
- Utilizatorul personalizează anumite elemente din procesul de autentificare pentru a crește nivelul de securitate adăugând elemente de securitate cunoscute doar de el;
- Furnizează unui ecosistem multi-layer de autentificare pentru fiecare utilizator;
- Noua platformă constructivă, conform invenției, completează sistemele de videoconferință, fiind independentă de acestea. Autentificarea utilizatorilor invitați la videoconferință este solicitată de utilizatorul care invită, numai după ce acesta este autentificat în platforma constructivă, conform invenției;
- Noua platformă constructivă, conform invenției, protejează datele personale ale utilizatorilor eliberând aceste date numai după ce utilizatorul solicită identitatea este autentificat și motivul (mandatul) pentru care solicită datele este validat. În



aceste condiții utilizatorul este informat în timp real despre solicitarea eliberării datelor personale din sistem către inițiator, situație în care utilizatorul poate opta să acorde accesul la date sau nu în timp real, respectiv în timpul sesiunii de videoconferință.

Platforma constructivă respectă normele pentru autentificare sigură și este compatibilă FIDO Alliance.

Descrierea **figurii 1** – ansamblu constructiv și a **figurii 2** – diagrama metodei.

Utilizatorii : „U1”- Profesor – „U2” - Student, conform cu exemplul de realizare a invenției, sunt doi dintre posibili utilizatori ai platformei de certificare și validare a identității.

M – Terminal telefonic vocal cu funcția de monitor, aparținând utilizatorului „U1”- „Profesor”. Terminalul telefonic „M” este conectat și accesibil prin sistemul telefonic (telefonie fixă sau mobilă GSM sau alte sisteme de telefonie, de exemplu Internet). Terminalul telefonic (M) oferă sisteme de protecție suplimentară cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, cod personal numeric PIN sau gesturi.

T – Terminal telefonic vocal cu funcția de monitor, aparținând utilizatorului „U2” - „Student”. Terminalul telefonic „T” este conectat și accesibil prin sistemul telefonic (telefonie fixă sau mobilă GSM sau alte sisteme de telefonie, de exemplu Internet). Terminalul telefonic „T” aparținând utilizatorului „U2” - „Student” oferă sisteme de protecție suplimentară cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, cod personal numeric PIN sau gesturi.

Di – Terminal Internet pentru desfășurarea sesiunilor de videoconferință al utilizatorului care organizează videoconferința (cadrul didactic, profesor). Terminalul Di poate fi computer, tabletă, telefon mobil inteligent, e-reader etc. care exploatează serviciile Internet ale platformei „AuthServices”. Terminalul Internet Di are și funcția de inițiator al cererii de autorizare acces. Terminalul internet (Di) oferă sisteme de protecție suplimentare pentru accesul utilizatorului „U1” - „Profesor” cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, PIN sau gesturi. Terminalul internet (Di) are în configurație subsisteme pentru citirea automată a cardurilor, recunoașterea imaginii codurilor QR, recunoaștere vocală, etc.



Dt – Terminal Internet pentru desfășurarea sesiunilor de videoconferință al utilizatorului invitat (studentului). Terminalul Dt poate fi computer, tabletă, telefon mobil inteligent, e-reader etc.) care exploatează serviciile Internet ale platformei „AuthServices”. Terminalul Internet (Dt) oferă sisteme de protecție suplimentare pentru accesul utilizatorului „U2” - „Student” cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, PIN sau gesturi. Terminalul internet (Dt) are în configurație subsisteme pentru citirea automată a cardurilor, recunoașterea imaginii codurilor QR, recunoaștere vocală, etc.

Da - Server autorizare Internet al platformei constructive „A” de servicii electronice Service căruia îi sunt transmise cererile de autorizare acces. Serverul de autorizare are acces prin rețeaua protejată privată „AuthServices” a platformei la servicii de baze de date, dispozitive de comunicație etc. Rețeaua privată a platformei constructive „A” este protejată prin servere de securitate numite în literatura de specialitate și zid de protecție sau firewall „F”;

Dc – Dispozitiv de comunicație telefonic conectat la rețeaua privată „AuthServices” a platformei constructive „A” și la serviciul telefonic public (GSM mobil sau rețeaua de telefonie fixă). Dispozitivului de comunicație Dc implementează tehnologii voce și mesaje scrise SMS. Dispozitivul de comunicații D poate fi realizat și printr-o fermă de servere pentru asigurarea comunicațiilor de mare volum.

Săgețile numerotate reprezintă interacțiunile dintre componentele sistemului în ordinea apariției evenimentelor astfel:

Etapa 1

Cei doi utilizatorii: “U1” = Profesor și “U2” = Student, stabilesc contactul audio-video printr-un sistem de videoconferință și utilizatorul “U1” - Profesorul solicită amprenta QR a identității digitale a utilizatorului “U2” - Studentului;

Etapa 2

Utilizatorul “U2” - Studentul prezintă amprenta (codul) QR în fața camerei de luat vederi “Cv” a dispozitivului Dt. Codul QR poate fi prezentat prin afișarea lui pe ecranul telefonului mobil “T” și apropierea ecranului telefonului mobil “T” de camera de luat vederi “Cv”, sau prin prezentarea unei legitimații fizice “Lg” care are imprimat codul QR etc. Codul QR al identității digitale a utilizatorului “U2”- student va fi afișat de terminalul “Di” în sesiunea video pe ecranul utilizatorului “U1” profesor. Utilizatorul “U1” - Profesor scanează codul QR afișat de “Di” pe ecranul videoconferinței cu ajutorul telefonului lui mobil “M”;

Etapa 3

Telefonul mobil "M" al utilizatorului "U1" - profesor va deschide automat un browser Internet care va genera o sesiune Internet cu serviciul de autentificare (AuthService) desemnat în codul QR, prin care va solicita automat validarea identității digitale a utilizatorului "U2" - student.

Etapa 4

Serviciul Internet de Autentificare va utiliza serviciile interne (Servere, baze de date, servicii etc.) pentru validarea identității utilizatorului "U2" - student. Dacă solicitarea provine de la un terminal cunoscut sistemului, și dacă identitatea utilizatorului "U2" - student este cunoscută, atunci sistemul de autentificare pe baza informațiilor din baza de date va emite către Dispozitivul de comunicație telefonic Dc conectat la rețeaua privată „ AuthServices” un mesaj de avertizare (SMS) către numărul de telefon "T" al utilizatorului "U2" - student. Mesajul SMS va conține un link unic prin care utilizatorul "U2" - student poate continua (sau nu) procesul de validare;

Etapa 5

Dacă utilizatorul "U2" - student, posesor al identității solicitate, recunoaște procesul, atunci va acționa prin a atinge link-ul cuprins în mesajul SMS primit conform etapelor anterioare. Acționarea link-ului va deschide automat o sesiune Internet în browser-ul telefonului mobil (T) prin care este informat de către cine a fost inițiat procesul și cu ce scop. Astfel utilizatorul "U2" - student poate opta în cunoștință de cauză asupra opțiunii de a permite sau nu accesul la datele sale personale. Opțiunea utilizatorului "U2" - student este colectată în browser-ul telefonului mobil (T) și este transmisă serviciului de autentificare.

Etapa 6

Serviciului de autentificare, pe baza opțiunii utilizatorului "U2" – student (etapa 5), va transmite utilizatorului "U1" - profesor în timp real datele personale ale utilizatorului "U2" - student, date care cuprind fotografia la înscriere a utilizatorului "U2" - student și alte date care permit utilizatorului "U1" - profesor să compare și să decidă dacă utilizatorului "U2" - student aflat în videoconferință este cel care este posesorul validat al identității digitale prezentate.

Exemplu de implementare

Posibilitatea cunoașterii nemijlocite între cadrele didactice și studenți (în special a celor din primul an de studii) este un efect major al crizei sanitare și al condițiilor restrictive de lucru. Examinarea orală limitează posibilitatea instituției de a asigura un



cadru legal privitor la autenticitatea participării la examene. Cadrul didactic are instrumente limitate în mediul Internet privind verificarea identității, iar fără constrângeri, studenții pot relativ ușor să imagineze scheme frauduloase pentru trecerea examenelor. Impostura și fraudă trebuie descurajate permanent și ele au consecințe grave atât asupra mediului educațional în general cât și asupra prestigiului instituțiilor implicate.

Identificarea, legitimarea persoanei trebuie efectuată în cadrul unui mandat legal. De exemplu ofițerii care în sarcinile de serviciu au atribuții de legitimare a cetățenilor, atunci când sunt aflați în timpul liber, în afara orelor de serviciu, nu pot îndeplini aceste atribuții. Prin analogie, un cadru didactic chiar dacă este obligat și îndreptățit să legitimeze studenții participanți la examen, va efectua aceste verificări doar în contextul examenelor anunțate de către instituție. Presupunând că studentul și cadrul didactic nu se cunosc nemijlocit, sistemul trebuie să dea certitudinea identității atât studentului cât și cadrului didactic, asigurând respectarea legii.

Serviciul se bazează pe transmisiuni de date în timp real, securizate, integrând tehnologiile de baze de date cu sistemele de telecomunicații telefonice (Voce, SMS, GSM) pentru a permite managementul identităților digitale ale participanților la examen prin gesturi simple cum este scanarea codurilor optice QR.

În viziunea sistemului, cadrul didactic se autentifică în prealabil, definește examenul în calendarul activităților, scanează codul QR aferent identității digitale a examenului după care, ulterior, poate scana codurile QR ale studenților participanți în videoconferință. Scanând codurile QR ale studenților în timpul examenului, sistemul va oferi automat datele necesare validării persoanei (fotografia, datele despre actele legale de identitate etc.) astfel încât cadrul didactic poate analiza și decide în ce măsură persoana prezentată la examen este cea înscrisă de secretariat. Sistemul implementează două moduri de interacțiune cu datele personale ale studenților.

- **Acord prezumat.** Oferă un mod de lucru simplificat, productiv, în care studentul a dat acordul la înscrierea în cadrul facultății astfel ca datele personale să fie prelucrate în timpul examenelor de către cadrele didactice;
- **Acord explicit.** Acordul studentului este obținut în timpul procedurii de validare a identității în timpul examenului;

Serviciul platformei este un serviciu Internet, de tip *cloud-computing*, *software as a service* (SAAS) proiectat să respecte legislația privind protecția datelor personale, și



o serie de restricții cum sunt compatibilitățile cu sistemele de operare Linux, Android, Apple, Microsoft. Astfel sistemul a fost testat pe computere actualizate la versiunile curente ale sistemelor de operare Linux (Ubuntu, Debian, Raspian), Microsoft Windows 10, Android 5-11, Apple IOS.

Serviciul este exploatabil exclusiv în browser. (Chrome, Chromium, Edge, Firefox, Samsung, Mi, Opera, Safari). Serviciul nu utilizează tehnologii precum trackers, localisation, GPS, date biometrice sau tehnologii pentru urmărirea activității utilizatorilor. Serviciul nu se instalează și nu depinde de aplicații care trebuie să fie instalate de către utilizator. Browser-ele testate pe telefoanele mobile / tablete includ implicit posibilitatea scanării codurilor QR.

Sistemul de verificare nu depinde de un anumit serviciu de videoconferință. El a fost testat cu Google Meet, Microsoft Skype, WhereBy, Zoom etc.

Serviciul se bazează pe pagini web care conțin componente conforme standardului ECMA script / Java script. Java script este activat implicit în browser și nu presupune acțiunea explicită a utilizatorului. În cazul în care utilizatorul a dezactivat Java script, atunci serviciul nu poate fi utilizat, afișând un mesaj concludent în acest sens. Utilizatorul are opțiunea de a activa Java script și de a reveni.

Funcționare

Identității digitale îi corespunde o înregistrare fizică în registrul matricol al instituției și respectiv o persoană care are calitatea de student sau cadru didactic. Înregistrările din registrul matricol sunt verificate de către secretariatul instituției care au atributele legale în acest scop, și sunt realizate în baza unui depozit legal de documente fizice. Serviciul conform invenției, emite pentru fiecare persoană cel puțin o identitate digitală materializată într-o structură de date care poate fi reprezentată electronic printr-un hyperlink (adresă Internet) sau echivalentul optic în cod optic rapid (QR) sau câmp radio de proximitate (NFC) sau alte tehnologii care permit transferul acestor structuri (Bluetooth, Wifi, IoT...).

Identitatea digitală, respectiv Hyperlink-ul echivalent anonimizează datele personale aferente identității digitale, conform cu recomandările GDPR fiind de forma:

<https://www.legitimid.com/ase/?ix=AQAAAPt+965hR9OxUavEZHQhHrxWD7z3FWx0Hg==>

Prefixul https inclus în hyperlink, se referă la utilizarea explicită a protocolul Internet securizat bazat pe utilizarea certificatelor digitale. Astfel, datele transmise între dispozitivul utilizatorului și serviciul platformei sunt criptate automat de către browser atât la citire cât și la scriere, utilizând cheia publică a platformei de servicii. Sufixul



particular *AQAAAPt+965hR9OxUavEZHQhHrxWD7z3FWx0Hg==* este o structură de date criptată prin care la recepție, serviciul verifică validitatea, integritatea și extrage referința din baza de date a identității digitale utilizate.

În funcție de context, identitatea digitală poate desemna date personale, evenimente, documente etc.. Prin design, serviciul platformei maschează toate identitățile digitale în același format, astfel încât utilizatorii nu pot prezice nici contextul și nici tipul identităților digitale, astfel încât sunt reduse șansele unor posibile scurgeri necontrolate de date (hacking).

Modul de lucru în timpul examenului oral

Datele personale au un nivel de protecție suplimentar și sunt accesate numai cu acordul explicit persoanei. Pentru a derula procedura de acces a datelor personale sensibile, cadrul didactic trebuie să fi înregistrat deja în sistem evenimentul (examenul) pentru a obține o identitate digitală echivalentă mandatului care asigură garanția interogării legale a identităților. Înregistrarea examenului este efectuată după autentificarea cadrului didactic și marcarea în calendar a examenelor.

Autentificarea profesorului pentru înregistrarea evenimentului (examenului)

Procesul autentificării inițiatorului videoconferinței (cadrul didactic, profesorul), care înregistrează evenimentul (examenul) pentru a obține o identitate digitală care validează posibilitatea interogării celorlalte identități ale participanților (studenți), este un proces de autentificare multi-factorial al unui abonat la un serviciu web. În procesul descris, autentificarea se bazează pe utilizarea identității digitale a profesorului înregistrată în sistem, prezentată în forma unui identificator transferabil dar (lista nu este limitată) de tip QR, NFC, Internet hyperlink etc., primește parola printr-un apel telefonic și o formează prin acționarea (atingerea) ecranului terminalului Internet.

Utilizatorul declanșează procesul autentificării prin utilizarea identității digitale. De exemplu acționează prin scanarea codului QR sau asupra hyperlink-ului echivalent. Browser-ul va deschide o sesiune criptată cu serviciul Internet de autentificare, conform invenției, și va afișa implicit o imagine sugestivă, respectiv (Fig. 3): Accesul la datele personale este refuzat. Acest mesaj rezultă din simplul fapt că interogarea identității digitale în mediu public în context necunoscut nu este permisă (de lege).

Recomandările normelor privind protecția datelor personale impun ca asocierea publică între numele complet al persoanei și contextul utilizării numelui să nu poată fi efectuată fără consimțământul explicit al persoanei. De aceea numele este afișat



trunchiat (Fig. 3, 4), astfel încât să nu fie explicit dar să rezulte faptul că sistemul este operațional.

Utilizatorul va tasta codul PIN pentru a declanșa un apel telefonic de verificare în care va este comunicată parola generată aleator și de unică întrebuintare. Pentru ca tastele să fie corect interpretate, tastatura trebuie să fie asociată cu conținutul browser-ului. Un click în zona albă din interiorul chenarului asigură acest fapt. Codul PIN este format (implicit) din ultimele 3 cifre ale numărului de telefon mobil înregistrat la înrolare (sau oricare altă regulă), urmat de (tasta) <Enter>. Codul PIN poate fi schimbat oricând de utilizator după autentificare.

Apelul pentru comunicarea parolei de unică utilizare este astfel inițiat. Preluarea apelului telefonic (răspunsul abonatului) va determina în timp real schimbarea paginii web care va afișa o altă imagine din care utilizatorul înțelege faptul că este în timpul unui apel telefonic de verificare sincronizat cu aplicația web. Răspunsul persoanei apelate determină schimbarea paginii web în timp real (Fig. 4). În toate celelalte situații, în care legătura telefonică nu poate fi efectuată (linie telefonică ocupată, rețea telefonică congestionată, abonat în afara ariei de acoperire, apel respins – rejectat, serviciu telefonic deranjat sau PIN incorect), este afișată pagina web cu mesajul *Apelul telefonic pentru comunicarea parolei nu poate fi efectuat*.

În timpul apelului telefonic sunt dictate imaginile care formează parola. Utilizatorul va selecta (click, atinge) imaginile indicate în cel mai scurt timp (Fig. 4). Compunerea parolei trebuie să fie finalizată înainte de închiderea automată a apelului telefonic. Dacă parola este incorect formată sau depășește timpul apelului telefonic atunci pagina web se schimbă pentru a anunța eșecul. Utilizatorul poate relua procesul autentificării de câteva ori. În cazul în care sunt cumulate trei încercări de autentificare nereușite, atunci sistemul va bloca autentificarea pentru următoarele 10 minute (exemplu).

Finalizarea cu succes a procesului de autentificare pe dispozitivul pe care a fost inițiată autentificarea va salva automat codul PIN, astfel încât procedurile ulterioare sunt simplificate, astfel nu mai este necesar codul PIN. (Dacă codul PIN este schimbat pe alt dispozitiv, atunci este necesară inițializarea memoriei locale prin acționarea tastei sau click pe sigla CSIE. Pagina web va conține mesajul: *Sunteți autentificat pentru confirmarea autentificării*. (Pagina este afișată timp de două secunde).

Imediat după confirmarea autentificării, sistemul va afișa calendarul evenimentelor poziționat în ziua calendaristică curentă (Fig. 5). Sistemul permite înregistrarea unui



singur eveniment în fiecare zi (exemplu). Nu sunt încă impuse reguli privind ora la care începe evenimentul (examenul) dar limita maximă de timp a unui eveniment este de 20 ore. Gestiunea evenimentelor este efectuată în pagina web.

Evenimentele sunt salvate în baza de date a platformei de servicii prin acționarea butonului verde. Identitatea digitală a evenimentului și codul QR asociat (Fig. 5) sunt generate automat cu salvarea evenimentului.

Prin scanarea codului QR cu telefonul mobil, este asigurat transferul identității digitale a evenimentului în telefon și salvarea ei în memoria criptată a browser-ului telefonului. Identitatea digitală a evenimentului, astfel salvată în browser asigură contextul necesar accesului la datele personale ale studenților prin scanarea identităților lor digitale în intervalul de timp definit de eveniment.

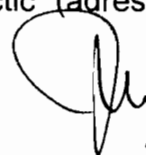
Dacă evenimentul este în curs de desfășurare sau s-a desfășurat în trecut, sistemul va utiliza o gamă de culori adecvate și va afișa explicit starea evenimentului. Evenimentele programate în viitor pot fi corectate de către utilizatorul care a efectuat înregistrarea lor. Sistemul nu permite editarea evenimentelor din trecut.

Accesul la datele personale protejate (Informarea și solicitarea acordului studentului)
Modul de lucru în timpul examenului oral, se bazează pe ideea informării studentului asupra contextului în care este solicitat acordul pentru acces la datele personale. Acordul implicit deși oferă productivitate maximă, nu oferă controlul persoanei asupra datelor personale, așa cum sunt recomandările privind protecția acestor date. Prin urmare, este posibil ca fiecare acces la datele personale să solicite acordul explicit, contextual al persoanei. În continuare, sunt prezentate modurile de lucru pentru accesul la datele personale cu solicitarea contextuală a acordului.

Acord implicit pentru acordarea accesului la date

Procedura de verificare interumană, la distanță, a identităților între cadrul didactic și student(ți) se bazează pe schimbul identităților digitale prin sistemul de videoconferință. Cadrul didactic inițiază procedura, în calitate de organizator al examenului, fiind îndreptățit legal să verifice identitatea fiecărui student. Telefonul mobil al cadrului didactic trebuie să fie conectat Internet (Wifi sau prin date mobile GSM) și să utilizeze un browser care permite scanarea codurilor QR. Astfel sunt urmate secvențial următoarele etape:

- Profesorul și studentul / studenții, stabilesc contactul audio-video printr-un sistem de videoconferință. La cererea cadrului didactic (adresată vocal),



studentul va prezenta în fața camerei video codul QR aferent identității sale digitale;

- Cadrul didactic scanează (cu telefonul mobil) codul QR prezentat de student. Platforma (AuthServices) este accesată pe baza hyperlink-ului scanat. Sunt efectuate prin software în cadrul serviciului verificările necesare asupra contextului scanării, respectiv dacă profesorul efectuează scanarea în cadrul unui eveniment autorizat de instituție etc. Dacă rezultatul este pozitiv, atunci procesul poate continua.
- Serviciul Internet al platformei, conform invenției, a efectuat verificările necesare și sunt îndeplinite condițiile necesare. Pe terminalul cadrului didactic vor fi afișate în timp real fotografia și numele integral al studentului citite din baza de date a instituției (Fig. 6). În majoritatea cazurilor, probabil profesorul poate certifica identitatea studentului în această stare și nu sunt necesare investigații suplimentare.
- În anumite situații, cadrul didactic trebuie să vizualizeze mai multe date pentru a stabili identitatea studentului. În acest scop poate utiliza un buton al interfeței web (verde în Fig.6) pentru a accesa date personale aflate sub protecție suplimentară și pentru care studentul a consimțit (anterior examenului) să fie utilizate. Dacă sunt accesate datele personale, atunci sistemul va informa studentul despre contextul în care au fost solicitate datele prin transmiterea unui mesaj SMS informativ, care conține un hyperlink către o pagină web securizată cu detalii (Fig. 8). Simultan cu informațiile trimise către student, cadrul didactic va afișa datele solicitate (Fig. 9).

Acord explicit pentru acordarea accesului la date

Accesul la datele personale în acest mode de lucru impune ca scanarea identității digitale a studentului să fie sub mandatul unui eveniment deja înregistrat și în curs de desfășurare.

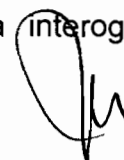
- Profesorul și studentul / studenții, stabilesc contactul audio-video printr-un sistem de videoconferință. La cererea cadrului didactic (adresată vocal), studentul va prezenta în fața camerei video codul QR aferent identității sale digitale;
- Cadrul didactic scanează (cu telefonul mobil) codul QR prezentat de student. Platforma (AuthServices) este accesată pe baza hyperlink-ului scanat. Sunt efectuate prin software în cadrul serviciului verificările necesare asupra



contextului scanării, respectiv dacă profesorul efectuează scanarea în cadrul unui eveniment autorizat de instituție etc. Dacă rezultatul este pozitiv, atunci procesul poate continua.

- Serviciul Internet al platformei, conform invenției, a efectuat verificările necesare și sunt îndeplinite condițiile necesare. Pe terminalul cadrului didactic vor fi afișate în timp real fotografia și numele integral al studentului citite din baza de date a instituției (Fig. 6). În majoritatea cazurilor, probabil profesorul poate certifica identitatea studentului în această stare în modul de lucru actual considerăm că sunt necesare investigații suplimentare.
- Cadrul didactic acționează (click, atinge) butonul verde din pagină pentru a solicita accesul la datele personale protejate. Pentru a fi în conformitate cu recomandările privind protecția datelor personale, în mod normal, cadrul didactic se va asigura de faptul că ecranul care afișează aceste pagini web nu este urmărit de alte persoane, de camere de supraveghere, nu este înregistrat sau nu se află în moduri de transmitere la distanță etc. Pagina web afișată este ilustrată în figura 7.
- Cererea de acces este înregistrată în și este emisă automat o identitate digitală specifică și o semnătură temporală asociată acestei cereri. Urmare a înregistrării cererii, sistemul transmite în timp real un hyperlink conținut într-un mesaj text (GSM / SMS) către numărul de telefon înregistrat în prealabil în baza de date a sistemului, persoanei a cărei identitate digitală este interogată. Imediat ecranul terminalului profesorului va fi actualizat pentru a-l informa de faptul că cererea de acces a fost transmisă (SMS) (sau nu). Telefonul mobil al studentului va recepționa în timp real mesajul text SMS care conține hyperlink-ul specific. Sistemul de operare al telefonului va face posibil ca prin atingerea conținutului mesajului SMS (hyperlink-ului) să fie implicat și automat instanțiată o sesiune web securizată (cu AuthService) în browser. (Datele mobile sau conexiunea WiFi trebuie să fie activă pe telefon).

Pe ecranul telefonului mobil al studentului va fi afișat (Fig. 8) un mesaj de tipul *Accesul la datele dumneavoastră personale este solicitat de către <prof. Nume Prenume> pentru participarea la: examenul <NumeExamen>. Observații <Observații>. Acordați accesul acționând butonul Da, refuzați accesul acționând butonul Nu.* Studentul este astfel informat asupra scopului (examenul), asupra persoanei care are mandatul de a interoga datele



personale (cadrul didactic) etc.. Informarea studentului este un drept și o recomandare a normelor legale privind protecția datelor personale (GDPR). Studentul poate opta să accepte accesul, să respingă accesul sau să nu acționeze. Dacă acționează, atunci ecranul telefonului afișează confirmarea înregistrării în baza de date.

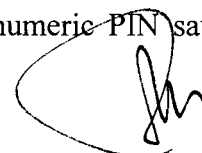
Înregistrarea opțiunii studentului asupra cererii de acces în baza de date a serviciului AuthService determină informarea în timp real a profesorului asupra stării cererii de acces la datele personale. Astfel simultan cu procesul desfășurat pe telefonul mobil al studentului, pe telefonul mobil al cadrului didactic sunt afișate în timp real stările prin care trece cererea de acces (Fig. 7, 8). În momentul în care studentul deschide mesajul SMS, pe ecranul cadrului didactic pagina web va afișa un mesaj de tipul *Cererea este deschisă, probabil pentru a fi citită. Așteptăm răspunsul persoanei.*

- În etapa următoare, cadrul didactic – profesorul este informat în timp real asupra stării cererii de acces:
 - în situația în care studentul a acceptat accesul la datele personale, acestea sunt afișate în timp real pe ecranul cadrului didactic. (Fig. 9);
 - în situația în care studentul nu acceptă accesul la datelor personale, atunci ecranul cadrului didactic va afișa un mesaj similar cu *Persoana a refuzat accesul.* Respingerea cererii de acces poate avea și semnificația faptului că persoana vizată nu este cea care se prezintă la examen, etc. (Fig. 10);
 - Cererea de acces la datele personale nu primește răspuns în timp util. Situația în care cererea de acces la datele personale nu primește răspuns în timp util poate avea mai multe cauze cum sunt: sistem de comunicații GSM deranjat, telefonul studentului nu este în aria de acoperire, studentul ignoră mesajul SMS etc. În toate aceste situații, prin lipsa obținerii acceptului explicit, accesul la datele personale nu este acordat. (Fig. 11);



REVENDICĂRI:

1. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, caracterizat prin aceea că o platformă constructivă (A) este realizată dintr-un terminal Internet (Di) al unui utilizator (U1) conectat în sistem de videoconferință cu un terminal Internet (Dt) al unui utilizator (U2) pentru desfășurarea sesiunilor de videoconferință și un terminal telefonic inteligent (M) cu funcție de scanner și monitor, care are în configurație subsisteme pentru citirea automată a cardurilor, recunoașterea imaginii codurilor QR afișate prin terminalul Internet (Di), care exploatează autorizat serviciile Internet al unei platforme (AuthServices), conectat și accesibil prin sistemul telefonic și Internet, având și funcția de inițiator al cererii de validare al identității, aparținând utilizatorului (U1), pentru care sunt asigurate sisteme de protecție suplimentară și dintr-un terminal telefonic inteligent (T) cu funcția de monitor, conectat și accesibil prin sistemul telefonic și Internet, aparținând utilizatorului (U2), pentru care sunt asigurate sisteme de protecție suplimentară, care exploatează serviciile Internet ale platformei (AuthServices) și dintr-un server autorizare Internet (Da) al platformei (AuthServices) care primește cererile de validare a identității și care are acces prin rețeaua privată protejată prin servere de securitate (F) ale platformei (AuthServices) la servicii de baze de date și la dispozitivul de comutație telefonic (Dc), conectat la rețeaua privată a platformei (AuthServices) și la serviciul telefonic public ce are implementate tehnologii voce și mesaje scrise SMS fiind realizat și printr-o fermă de servere pentru asigurarea comunicațiilor de mare volum prin care platforma (AuthServices) urmare a unei cereri de validare a identității primite de la terminalul autorizat (M), transmite către terminalul (T) al utilizatorului (U2) un mesaj care informează și determină interacțiunea utilizatorului (U2) cu platforma constructivă (A) astfel încât prin terminalul inteligent autorizat (T) și platforma (AuthServices) utilizatorul (U1) primește accesul la datele personale ale utilizatorului (U2) în baza de date a platformei (AuthServices) putând decide în cunoștință de cauză asupra identității corespondentului.
2. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicarea 1, caracterizat prin aceea că terminalele telefonice inteligente (M) și (T) oferă sisteme de protecție suplimentară cum sunt cele implementate în sistemele Android, Windows, IOS, respectiv autentificare biometrică, cu parolă, cod personal numeric PIN sau gesturi.



3. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicarea 1 și 2, caracterizat prin aceea că, terminalul (Di) și (Dt) sunt un computer, o tabletă, un telefon mobil inteligent, un e-reader, care exploatează serviciile Internet ale platformei (AuthServices) și oferă sisteme de protecție cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, PIN sau gesturi.
4. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicarea 1-3, caracterizat prin aceea că, serviciul platformei constructive (A) este un serviciu Internet, de tip cloud-computing, software as a service (SAAS) proiectat să respecte legislația privind protecția datelor personale și o serie de restricții ale sistemelor de operare Linux, Android, Apple, Microsoft, și este exploatabil exclusiv în browser, Chrome, Chromium, Edge, Firefox, Samsung, Mi, Opera, Safari și nu utilizează tehnologii precum trackers, localizare, GPS, date biometrice sau tehnologii pentru urmărirea activității utilizatorilor, nu se instalează în sistemul de operare și nu depinde de aplicații care trebuie să fie instalate de către utilizator, browser-ele incluse în telefoanele mobile sau tablete includ implicit posibilitatea scanării codurilor QR.
5. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicările 1-4, caracterizat prin aceea că utilizatorul (U2) prezintă codul QR în fața unei camere de luat vederi (Cv) a dispozitivului (Dt), de pe ecranul telefonului mobil (T) sau de pe o legitimație fizică (Lg) care are imprimat codul QR, până când acesta este afișat de terminalul (Di) în sesiunea video pe ecranul utilizatorului (U1) care scanează codul QR de pe ecranul videoconferinței cu ajutorul telefonului mobil inteligent (M), care deschide automat un browser Internet și care generează o sesiune Internet cu serviciul de autentificare (AuthService) desemnată în codul QR scanat, prin care solicită automat validarea identității digitale a utilizatorului (U2).
6. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicările 1-5, caracterizat prin aceea că dacă identitatea utilizatorului (U2) este cunoscută în baza de date a platformei (A), atunci sistemul de autentificare pe baza informațiilor din baza de date emite către dispozitivul de comunicație telefonic (Dc) conectat la rețeaua privată (AuthServices) un mesaj de avertizare SMS către numărul de telefon (T) al utilizatorului (U2), mesajul SMS conține un link unic prin care utilizatorul (U2) este informat asupra procesului de validare, acționarea link-ului deschide automat o sesiune Internet în browser-ul telefonului mobil (T) prin care este informat de către cine a fost inițiat procesul de



validare și cu ce scop și poate opta în cunoștință de cauză asupra opțiunii de a permite accesul la datele sale personale.

7. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicările 1-6 , caracterizat prin aceea că, opțiunea utilizatorului (U2) este colectată în browser-ul telefonului mobil (T) și este transmisă serviciului de autentificare, respectiv utilizatorului (U1), informații care permit utilizatorului acestuia (U1) să compare și să decidă dacă utilizatorului (U2) este cel care este posesorul validat al identității digitale prezentate.
8. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicările 1-7, caracterizat prin aceea că, opțiunea utilizatorului (U2) este colectată în browser-ul telefonului mobil (T) și este transmisă serviciului de autentificare, respectiv utilizatorului (U1), informații care permit utilizatorului acestuia (U1) să compare și să decidă dacă utilizatorului (U2) este cel care este posesorul validat al identității digitale prezentate.
9. Ansamblu constructiv platformă Internet de certificare și validare a identității utilizatorilor, conform cu revendicările 1-8 , caracterizat prin aceea că, utilizatorul (U1) se autentifică în prealabil, definește evenimentul în calendarul activităților, scanează codul QR aferent identității digitale a evenimentului după care, ulterior, scanează codurile QR ale utilizatorilor (U2) participanți la eveniment în timpul acestuia, când sistemul oferă automat datele necesare validării persoanei, astfel încât utilizatorul (U1) poate analiza și decide în ce măsură persoana prezentată la eveniment este cea înscrisă.



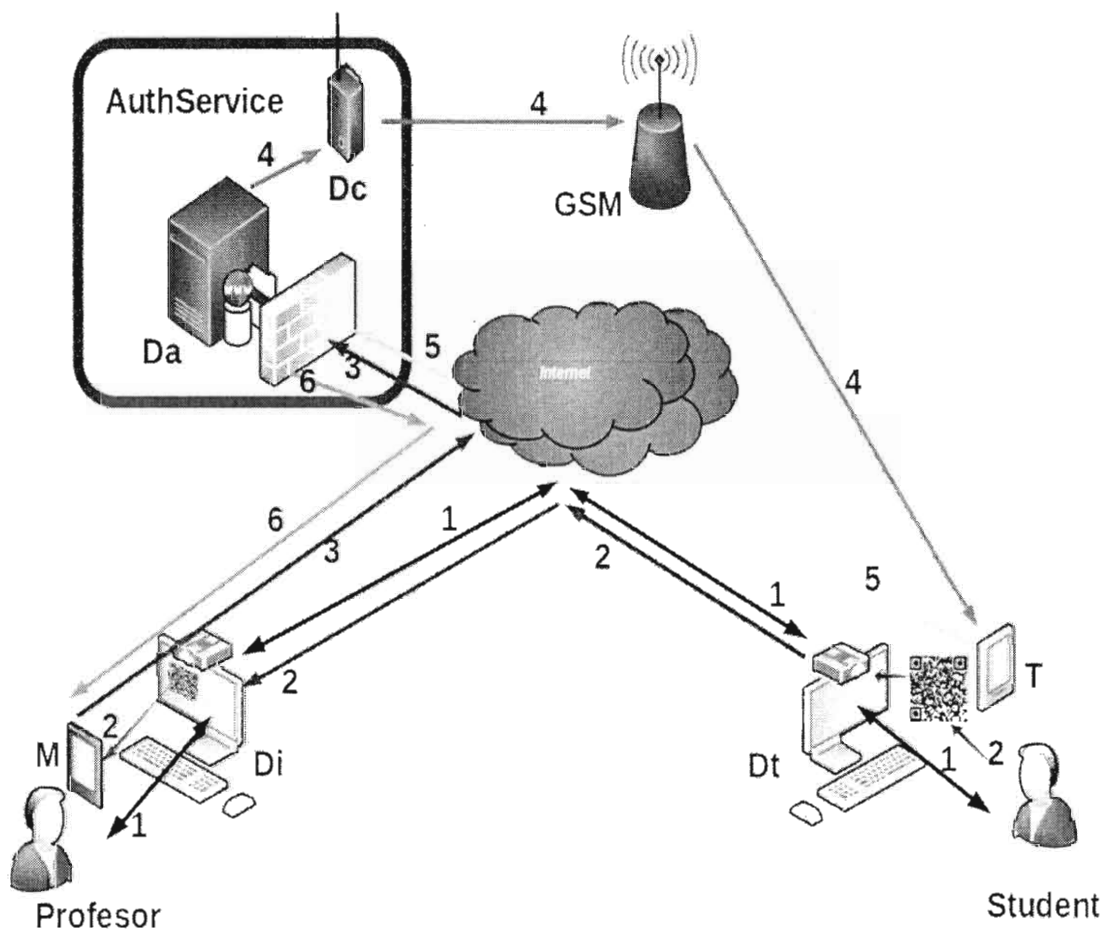


Fig. 1

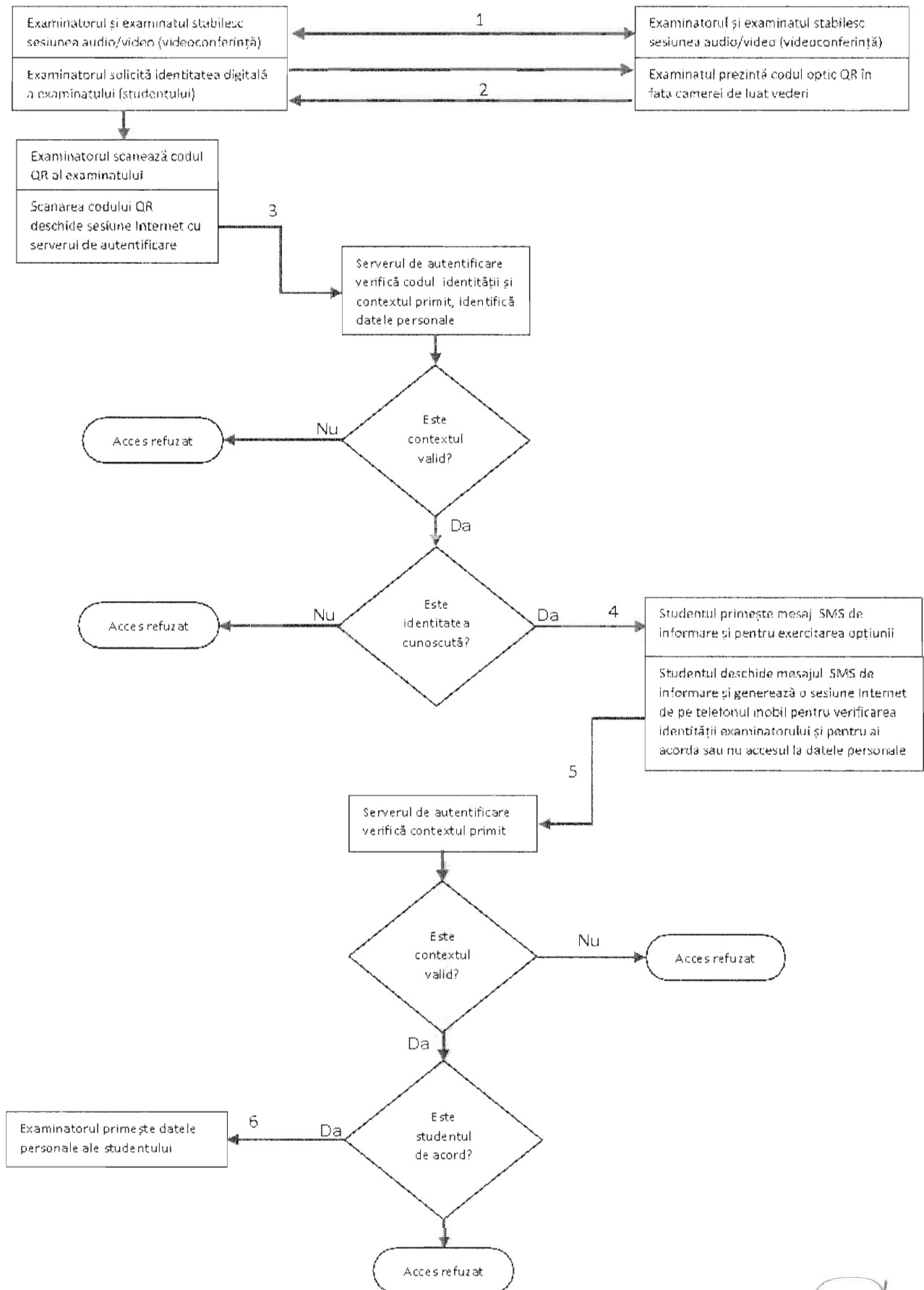


Fig. 2

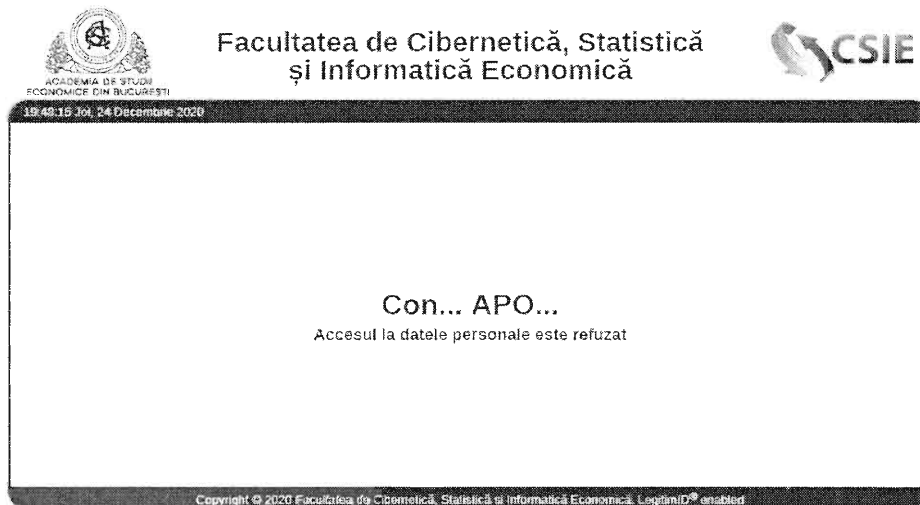


Fig.3



Fig.4

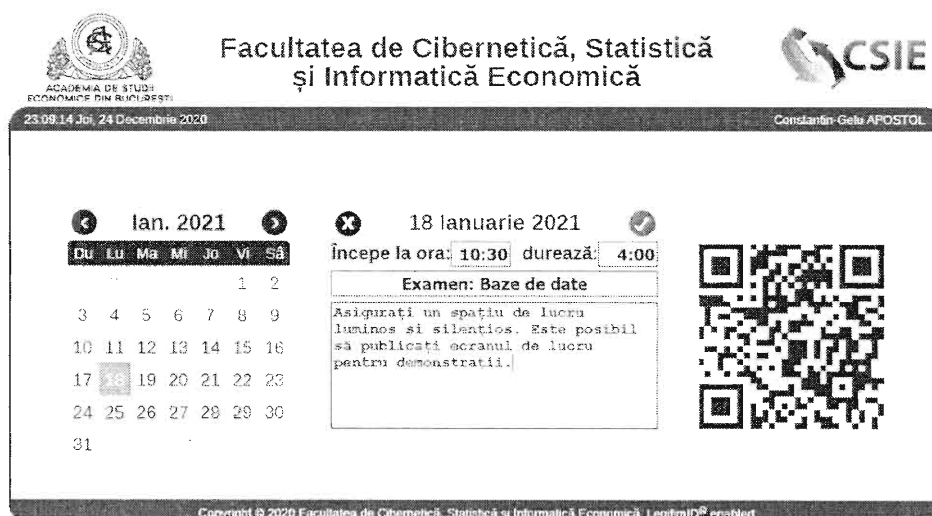


Fig. 5

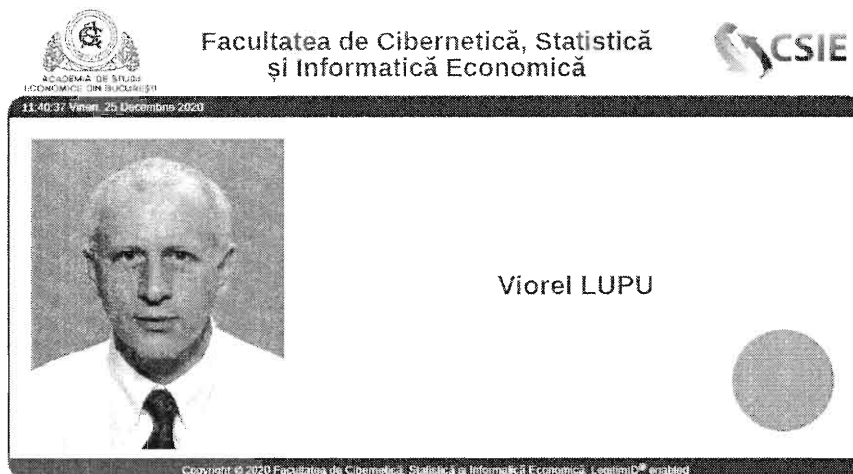


Fig. 6

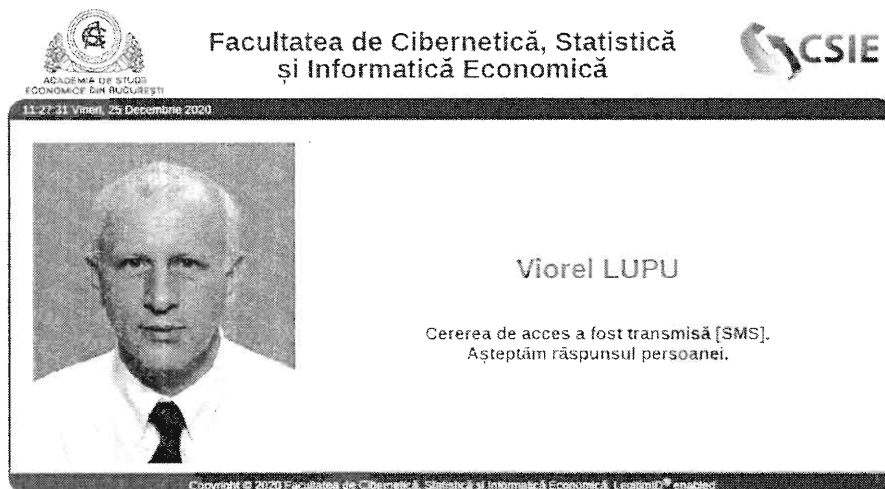


Fig. 7

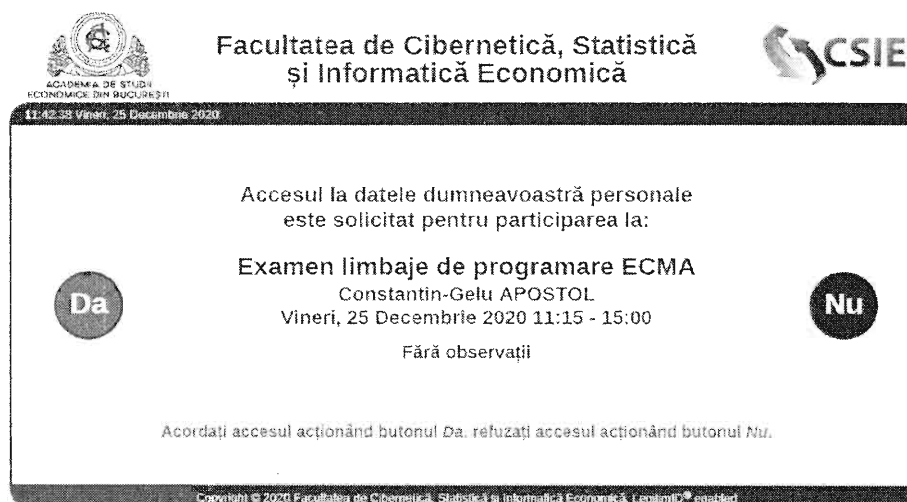


Fig. 8


**Facultatea de Cibernetică, Statistică
și Informatică Economică**


11:43:34 Vineri, 25 Decembrie 2020



Viorel LUPU

Matricol: AXXA7652736b, 12/09/2016
 CNP: Român, 1200902101021
 Născut în: Gălbinași, 27/03/2020
 Înregistrat: Carte de identitate, BBXA654564321, 03/04/2020
 Studii: An I, Grupa A, 12/09/2016
 Comunic: 642068057, viorel.lupu@onlineservices.ro

Copyright © 2020 Facultatea de Cibernetică, Statistică și Informatică Economică. LegitimID® enabled

Fig. 9


**Facultatea de Cibernetică, Statistică
și Informatică Economică**


11:46:56 Vineri, 25 Decembrie 2020



Viorel LUPU

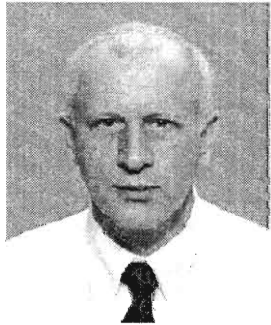
Accesul la datele personale nu este acceptat.
 Persoana a refuzat accesul.

Copyright © 2020 Facultatea de Cibernetică, Statistică și Informatică Economică. LegitimID® enabled

Fig. 10


**Facultatea de Cibernetică, Statistică
și Informatică Economică**


11:48:14 Vineri, 25 Decembrie 2020



Viorel LUPU

Accesul la datele personale nu este acceptat.
 Timpul de așteptare a expirat.

Copyright © 2020 Facultatea de Cibernetică, Statistică și Informatică Economică. LegitimID® enabled

Fig. 11

