

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din _____
Chișinău

**cu privire la serviciul guvernamental de identificare a persoanei la distanță
(e-KYC)**

În temeiul art.22 lit.c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se aprobă Conceptul serviciului guvernamental de identificare a persoanei la distanță (e-KYC) (se anexează).
2. Se desemnează Instituția publică „Agenția de Guvernare Electronică” în calitate de posesor și deținător al serviciului guvernamental de identificare a persoanei la distanță (e-KYC).
3. Instituția publică „Agenția de Guvernare Electronică”:
 - 1) va asigura implementarea și dezvoltarea continuă a serviciului guvernamental de identificare a persoanei la distanță (e-KYC);
 - 2) va asigura integrarea serviciului guvernamental de identificare a persoanei la distanță (e-KYC) cu serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), în vederea stabilirii identității la distanță a solicitanților de certificare a cheii publice;
 - 3) va asigura furnizarea serviciului guvernamental de identificare a persoanei la distanță (e-KYC) persoanelor juridice de drept public și de drept privat;
 - 4) va aproba condițiile contractuale privind prestarea serviciilor de stabilire a identității persoanei prin intermediul serviciului guvernamental de identificare a persoanei la distanță (e-KYC) și regulile de utilizare aferente;
 - 5) va aproba tarifele pentru:
 - a) furnizarea serviciului guvernamental de identificare a persoanei la distanță (e-KYC) persoanelor juridice de drept public și de drept privat;
 - b) prestarea serviciilor de stabilire a identității persoanelor fizice în vederea obținerii certificatului calificat al cheii publice.
4. Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”:
 - 1) va asigura administrarea tehnică a serviciului guvernamental de identificare a persoanei la distanță (e-KYC);
 - 2) va asigura stabilirea identității solicitanților de certificare a cheii publice prin intermediul serviciului guvernamental de identificare a persoanei la distanță (e-KYC).

5. Entitățile publice implicate în procesul de implementare a serviciului guvernamental de identificare a persoanei la distanță (e-KYC) vor întreprinde acțiunile necesare întru ajustarea cadrului normativ aferent.

Prim-ministru

DORIN RECEAN

Contrasemnează:

**Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării**

Dumitru ALAIBA

**Conceptul
serviciului guvernamental de identificare a persoanei la distanță (e-KYC)**

INTRODUCERE

Transformarea digitală a schimbat dramatic modul în care cetățenii și mediul de afaceri interacționează cu administrația publică și a avut un impact semnificativ asupra serviciilor publice și proceselor administrative. În ultimii ani, progresele în tehnologie digitală au transformat sectorul public, făcându-l mai eficient, transparent și accesibil cetățenilor.

În acest context, Guvernul Republicii Moldova cu sprijinul partenerilor de dezvoltare implementează o serie politici pentru a stimula utilizarea serviciilor electronice, transformarea digitală a sectorului public, digitalizarea economiei Republicii Moldova, dezvoltarea comerțului electronic etc.

Un factor cheie în transformarea digitală este implementarea identității electronice - o componentă esențială a infrastructurii pe care se va construi viitorul sistemelor de e-guvernare și e-servicii private. O identitate electronică cu capacitatea deplină de a face acțiuni obligatorii din punct de vedere legal online - oriunde și oricând - oferă un avantaj imens cetățenilor, companiilor și guvernului deopotrivă.

Ecosistemul e-identității este o parte esențială a strategiei digitale a oricărui guvern către procese digitalizate, sigure, fără hârtie, durabile și cooperarea transfrontalieră sau transorganizațională. Nevoia de identificare și semnătură electronică apare ori de câte ori este nevoie de a lega o decizie sau tranzacție de o anumită persoană sau entitate și de a asigura integritatea datelor.

Evoluția rapidă a tehnologiei a contribuit la apariția unor noi oportunități în domeniul managementului identității digitale, prin crearea condițiilor tehnice de identificare și înregistrare la distanță a solicitanților de identitate electronică. Verificarea identității este procesul prin care un furnizor de servicii colectează și validează informații despre un solicitant și verifică dacă informațiile colectate și validate aparțin efectiv solicitantului. La moment, acest lucru este realizat de către un operator de verificare a identității care este prezent fizic în același loc cu solicitantului, la extragerea informațiilor și verificarea actului de identitate a solicitantului. Însă creșterea pieței digitale a făcut ideea identificării unei persoane de la distanță mai atractivă, deoarece identificarea de la distanță permite clienților aflați la distanță fizică să acceseze astfel servicii. Abilitatea de verificare a identificării de la distanță promovează și crește posibilitatea tranzacțiilor electronice, asigurând în același timp și validitatea identităților partenerilor implicați în tranzacție.

O soluție de identificare electronică la distanță este necesară în multe domenii ale activităților sociale și economice. Necesitatea stringentă la această etapă este de a asigura o soluție calitativă și securizată de identificare la distanță a viitorilor utilizatori a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) și de a furniza o opțiune viabilă pentru prestatorii de servicii financiar-bancare sau notari de a interacționa și identifica clienții la distanță, fără prezența acestora la un ghișeu fizic. Pentru a evita dispersarea investițiilor, implementarea diferitelor standarde și lăsarea în urmă a multor alte sectoare vitale, cum ar fi serviciile publice, educația și asistența medicală, implementarea de către Instituția publică „Agenția de Guvernare Electronică” a unei soluții unificate, multifuncționale și accesibilă publicului este considerată cea mai potrivită soluție pentru mediul de afaceri și cetățeni.

Unul dintre punctele forte cheie ale unei soluții de identificare la distanță reutilizabilă este feedback-ul valoros pe care îl oferă toți subiecții participanți. Atunci când un solicitant face primul contact fizic cu orice jucător din ecosistem, rezultatul - fie el pozitiv sau negativ - poate fi împărțit și utilizat pentru a îmbunătăți și perfecționa în continuare procesul general de identificare la distanță. Această buclă de feedback continuă întărește securitatea și eficacitatea sistemului, oferind beneficii tuturor părților interesate implicate.

În acest sens, proiectul *Republica Moldova: Sprijin acordat Agenției de Guvernare Electronică în dezvoltarea platformei digitale multifuncționale Electronic Know Your Customer (eKYC+)*, inițiat de Instituția publică „Agenția de Guvernare Electronică” împreună cu Consiliul Economic, și susținut financiar de Banca Europeană pentru Reconstrucție și Dezvoltare (BERD), este un răspuns direct la această nevoie tot mai stringentă de instrumente de identificare electronică la distanță a clienților și în Republica Moldova. Proiectul își propune să contribuie la eficientizarea interacțiunii dintre cetățeni și reprezentanții mediului de afaceri cu autoritățile publice, dinamizarea tranzacțiilor electronice, facilitarea dezvoltării serviciilor electronice și creșterea ratei de adopție a identității electronice în rândul populației Republicii Moldova, prin implementarea unui mecanism eficient, fiabil și modern de stabilire la distanță a identității persoanelor.

Capitolul I

DISPOZIȚII GENERALE

1. Serviciul guvernamental de identificare a persoanei la distanță (e-KYC) (în continuare – serviciul e-KYC) este o soluție prin intermediul căreia se realizează acțiunile de identificare și verificare a identității persoanei fizice, în baza actelor de identitate prezentate, a imaginilor capturate și a informațiilor comunicate de persoana fizică sau preluate din surse externe de date, utilizând mijloace digitale.

2. Serviciul e-KYC reprezintă un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, care are drept scop oferirea unui mecanism de identificare a

persoanei la distanță reutilizabil, sigur și ușor de folosit pentru diferite cazuri în care este necesară verificarea identității persoanei la nivelul de asigurare solicitat.

3. În sensul prezentului concept vor fi utilizate următoarele noțiuni de bază:

attribute de identitate - subset al datelor de identificare trimise de serviciul de identificare a persoanei la distanță către serviciul client;

beneficiar al serviciului e-KYC – persoană fizică sau juridică, posesor al unui serviciu client care utilizează serviciul de identificare a persoanei la distanță pentru a identifica persoane fizice în vederea înregistrării a acestora în calitate de clienți sau pentru a le presta servicii;

detectarea biometrică a vitalității feței (Biometric Liveness Detection) - tehnică utilizată pentru a detecta o tentativă de falsificare prin determinarea dacă sursa unei probe biometrice este o ființă umană vie sau o reprezentare falsă. Acest lucru se realizează prin algoritmi care analizează datele colectate de la senzorii biometrici pentru a determina dacă sursa este în direct sau reprodușă;

componenta de securitate – componenta electronică a unui act de identitate electronic, utilizat ca suport de stocare securizat pentru datele de identificare și fotografia deținătorului legitim al actului;

consimțământ - orice indicare liberă, specifică, informată și neechivocă a dorințelor solicitantului prin care acesta, printr-o declarație sau printr-o acțiune afirmativă clară, indică acordul cu privire la prelucrarea datelor cu caracter personal care îl privesc;

date biometrice – date cu caracter personal rezultate în urma prelucrărilor tehnice specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acesteia;

date de identificare – set de date cu caracter personal, inclusiv date biometrice, colectate și verificate de către serviciul de identificare a persoanei la distanță în vederea verificării identității unei persoane fizice;

dispozitivul solicitantului – orice dispozitiv inteligent (telefon sau tabletă) aflat în posesia solicitantului, care este compatibil cu sistemul informatic pentru identificarea persoanei la distanță;

dosar electronic de evidență – element reținut de serviciul e-KYC care colectează datele relevante ce urmează să fie păstrate pentru soluționarea litigiilor sau în cazul unei investigații și în special în vederea furnizării de probe în instanță;

identitate electronică – datele de identificare a persoanelor în format electronic reprezentând în mod unic o persoană fizică;

identificarea persoanei la distanță prin mijloace digitale - procesul de identificare și verificare a identității persoanei fizice, în baza actelor de identitate prezentate, măsurătorilor semnalmentelor biometrice faciale, comparării de imagini și a informațiilor comunicate de persoana fizică și/sau preluate din surse de date externe, utilizând mijloace digitale;

mijloace digitale - mijloace care utilizează tehnologii digitale inovatoare care folosesc, printre altele, mijloace video, inteligența artificială și/sau procese de învățare automată (machine learning), cum ar fi aplicațiile care realizează identificarea unei persoane și/sau verificări ale actelor de identitate (prin capturi de

imagini digitale, măsurători ale semnalmentelor biometrice faciale, comparare de imagini), tehnologia de comunicare în câmp apropiat (Near Field Communication) încorporată în actele de identitate electronice;

mijloace video - mijloace de identificare la distanță ce utilizează tehnologii care presupun fie transmiterea audiovideo de succesiuni de imagini în mișcare, în timp real, în cadrul unei videoconferințe cu prezența unui operator uman, fie transmiterea de succesiuni de imagini în mișcare reprezentând capturi video cu persoana fizică, fără prezența unui operator uman, cu verificarea acestora cu sau fără implicarea unui operator uman;

Zona de citire automată (Machine Readable Zone MRZ) - zonă a unui act de identitate, care conține informații personale ale titularului și este concepută pentru a fi citită automat de către dispozitivele sau sistemele de recunoaștere optică a caracterelor (OCR), denumit în continuare - MRZ;

Comunicare în câmp apropiat (Near Field Communication) - tehnologie de comunicare wireless pe distanțe scurte, care permite schimbul de date între dispozitive compatibile, aflate la o distanță până la câțiva centimetri, denumit în continuare - NFC;

prestator de servicii de încredere calificat – astfel cum este definit conform prevederilor Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere;

rezultatul verificării identității de la distanță – toate informațiile trimise de serviciul de identificare a persoanei la distanță către serviciul client, inclusiv verdictul (reușit sau nereușit) al verificării identității la distanță, motivul eșecului, dacă există, atributele de identitate legate de solicitant cerute de serviciul client și verificate de către furnizorul de servicii de identificare și orice date suplimentare solicitate de serviciul client;

surse externe de date – sisteme informaționale și registre de stat sau private.

4. Obiective de bază specifice stabilite pentru serviciul e-KYC:

- 1) automatizarea procesului de identificare a persoanei la distanță;
- 2) implementarea unor mijloacele digitale reutilizabile de identificare a persoanei la distanță;
- 3) utilizarea tehnologiilor emergente, cum ar fi inteligența artificială, pentru a spori securitatea și eficacitatea procesului de identificare a persoanei la distanță;
- 4) reutilizarea serviciilor guvernamentale de platformă și a sistemelor informaționale de stat pentru eficientizarea procesului de identificare a persoanei la distanță;
- 5) creșterea adopției identității electronice în rândul populației Republicii Moldova, prin facilitarea obținerii acesteia la distanță;
- 6) reducerea costurilor operaționale de identificare a persoanei la distanță;
- 7) celeritatea procesului de identificare a persoanei la distanță;
- 8) eliminarea cererilor pe suport de hârtie din procesul de identificare a persoanei la distanță.

5. Principiile de bază ale serviciului e-KYC sunt:

- 1) principiul legalității, care presupune crearea și exploatarea serviciului e-KYC în conformitate cu legislația națională;

2) principiul conformității prelucrării datelor cu caracter personal, prin care se înțelege prelucrarea datelor cu caracter personal ale beneficiarilor serviciului e-KYC în conformitate cu prevederile art. 4 din Legea nr. 133/2011 privind protecția datelor cu caracter personal;

3) principiul neexcesivității și pertinentei prelucrării datelor cu caracter personal, care relevă necesitatea limitării volumului datelor cu caracter personal prelucrate, în așa fel încât să fie prelucrate doar informațiile relevante și necesare în contextul realizării sarcinilor serviciului e-KYC;

4) principiul integrității datelor, care presupune păstrarea conținutului și interpretarea univocă în condițiile unor acțiuni accidentale. Integritatea datelor se consideră a fi păstrată dacă datele nu au fost denaturate sau distruse;

5) principiul confidențialității informației, care se referă la restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată, în conformitate cu legislația, în scopul neadmiterii ingerinței în viața privată a subiecților datelor cu caracter personal sau cauzării prejudiciilor persoanelor juridice;

6) principiul îndrumării procesului de utilizare a serviciului e-KYC, care garantează accesul operativ la informație al utilizatorului, în limitele competenței stabilite prin actele normative și nivelul de acces;

7) principiul securității informaționale, care presupune asigurarea nivelului integrității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, denaturării, deteriorării, modificării, accesului și utilizării neautorizate. Securitatea serviciului e-KYC presupune rezistența la atacuri, protecția caracterului confidențial al informației, a integrității și pregătirea pentru lucru atât la nivel de sistem, cât și la nivel de date prezentate în această informație;

8) principiul compatibilității serviciului e-KYC cu sistemele informaționale partajate existente în țară;

9) principiul îmbunătățirii continue, care presupune ajustarea serviciului e-KYC la practicile și recomandările internaționale;

10) principiul modularității și scalabilității, ce reprezintă posibilitatea de a dezvolta serviciul e-KYC fără modificarea componentelor create anterior.

Capitolul II

CADRUL NORMATIV-JURIDIC AL SERVICIULUI e-KYC

6. Implementarea serviciului e-KYC este prevăzută de Strategia de reformă a administrației publice din Republica Moldova pentru anii 2023-2030 (*activitatea 1.5.*), aprobată prin Hotărârea Guvernului nr. 126/2023 și se conține în Programul pentru implementarea Strategiei de Reformă a Administrației Publice pentru anii 2023-2026 (*acțiunea 4.1.18*), aprobat prin Hotărârea Guvernului nr. 352/2023.

7. Crearea și funcționarea serviciului e-KYC este reglementată, în particular, de următoarele acte normative:

1) Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere (Monitorul Oficial al Republicii Moldova, 2022, nr. 170-176, art. 317);

- 2) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44);
- 3) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate (Monitorul Oficial al Republicii Moldova, 2018, nr. 295-308, art. 452);
- 4) Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr. 58-66, art. 133);
- 5) Legea nr. 133/2011 privind protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr. 170-175, art. 492);
- 6) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat (Monitorul Oficial al Republicii Moldova, 2006, nr. 79-82, art. 591);
- 7) Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017 (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art. 277);
- 8) Hotărârea Guvernului 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat (Monitorul Oficial al Republicii Moldova, 2018, nr. 157-166, art. 474);
- 9) Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect), aprobat prin Hotărârea Guvernului nr. 211/2019 (Monitorul Oficial al Republicii Moldova, 2019, nr. 132-138, art. 254);
- 10) Regulamentul privind utilizarea, administrarea și dezvoltarea platformei tehnologice comune (MCloud), aprobat prin Hotărârea Guvernului nr. 128/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 47-48, art. 145);
- 11) Regulamentul privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), aprobat prin Hotărârea Guvernului nr. 405/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 147-151, art. 445);
- 12) Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr. 1090/2013 (Monitorul Oficial al Republicii Moldova, 2014, nr. 4-8, art. 2);
- 13) Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr. 708/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 261-267, art. 756);
- 14) Regulamentul privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify), aprobat prin Hotărârea Guvernului nr. 376/2020 (Monitorul Oficial al Republicii Moldova, 2020, nr. 149-151, art. 476);
- 15) Regulamentul privind utilizarea, administrarea și dezvoltarea Portalului guvernamental al unităților de drept, aprobat prin Hotărârea Guvernului nr. 412/2020 (Monitorul Oficial al Republicii Moldova, 2020, nr. 161-164, art. 533);
- 16) Regulamentul privind utilizarea, administrarea și dezvoltarea Portalului guvernamental al cetățeanului, aprobat prin Hotărârea Guvernului nr. 413/2020 (Monitorul Oficial al Republicii Moldova, 2020, nr. 161-164, art. 534);

17) Hotărârea Guvernului 324/2022 cu privire la serviciul guvernamental de identitate și semnătură electronică mobilă (MobiSign) (Monitorul Oficial al Republicii Moldova, 2022, nr. 151-157, art. 382);

18) Reglementarea tehnică „Procese ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006 (Monitorul Oficial al Republicii Moldova, 2006, nr. 95-97, art. 335).

Capitolul III

SPAȚIUL FUNCȚIONAL AL SERVICIULUI e-KYC

8. Serviciul e-KYC trebuie să asigure realizarea funcțiilor de bază ale unui sistem informațional prevăzute în cadrul normativ, precum și a funcțiilor specifice care rezultă din destinația sistemului.

9. Serviciul e-KYC are un design modular și poate fi dezvoltat prin implementarea sau integrarea de noi funcționalități specifice activităților de identificare la distanță a persoanelor, ținând cont de capacitățile de reutilizare ale acestora și posibilitățile de îmbunătățire a experienței utilizatorilor în procesul de înregistrare sau solicitare a unui serviciu de către aceștia. În serviciul e-KYC se vor implementa următoarele componente funcționale de bază:

- 1) colectarea datelor pentru identificarea persoanei la distanță:
 - a) completarea formularului de solicitare a identificării la distanță;
 - b) scanarea actului de identitate biometric și preluarea informațiilor din MRZ;
 - c) citirea informațiilor de pe componenta de securitate a actului de identitate prin tehnologia NFC;
 - d) înregistrarea feței solicitantului cu instrucțiuni de verificare afișate pe ecranul solicitantului în timpul apelului video;
 - e) preluarea datelor tehnice și adresa IP a dispozitivului solicitantului.
 - 2) validarea datelor prezentate și stabilirea identității persoanei:
 - a) verificarea autenticității actului de identitate și a datelor pe care le conține cu datele din Registrul de stat al populației;
 - b) conversia în date a imaginilor preluate (crearea amprente faciale) și compararea acestora cu cele din Registrul de stat al populației;
 - c) realizarea verificării biometrice a vitalității feței solicitantului;
 - d) verificarea numărului de telefon sau a adresei de e-mail a solicitantului prin folosirea unui sistem de parole unice (OTP-One Time Password).
 - 3) confirmarea identității și furnizarea în regim automatizat beneficiarilor serviciului e-KYC a atributelor de identitate ale solicitanților;
 - 4) generarea sub formă de document electronic a unei cereri sau solicitări de înregistrare și transmiterea acesteia în regim automatizat către serviciul client;
 - 5) crearea dosarului electronic de evidență.
10. De asemenea, serviciul e-KYC va implementa următoarele funcționalități de sistem:

- 1) schimb de date cu sistemele informaționale externe – realizat prin consumarea interfețelor destinate schimbului reciproc de date prin platforma de

interoperabilitate (MConnect), precum și integrarea sistemelor informaționale partajate (MPass, MSign, MLog, MNotify etc.);

2) înregistrarea, stocarea și păstrarea securizată a datelor colectate (imagini foto/video, amprenta facială, date despre solicitanți etc.) pe o perioadă determinată de timp stabilită conform cadrului normativ aplicabil și/sau în bază de acordului cu beneficiarii serviciului e-KYC;

3) executare proceduri automatizate – funcționalități de declanșare și funcționare în regim automatizat a unui șir de funcționalități ale serviciului e-KYC în vederea utilizării raționale a resurselor server, a lansării serviciilor specifice funcționării acestuia și a furnizării la momentul oportun a datelor pentru utilizatori;

4) administrarea sistemului;

5) asigurarea integrității logice a serviciului e-KYC;

6) asigurarea securității și protecției informației în cadrul serviciului e-KYC;

7) gestionarea copiilor de rezervă;

8) expediere notificări;

9) jurnalizarea evenimentelor de sistem;

10) monitorizarea performanței serviciului e-KYC;

11) suport tehnic și mentenanță.

11. Serviciul e-KYC poate fi dezvoltat prin implementarea de noi funcționalități în conformitate cu prevederile cadrului normativ aplicabil.

12. Interfața utilizator a serviciului e-KYC:

1) va oferi o interfață ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori prin intermediul unei aplicații mobile și cu un funcțional redus prin intermediul unei aplicații web. Interfața utilizator a serviciului e-KYC va reprezenta un design grafic, echilibrat, distinct și adaptabil pentru majoritatea dispozitivelor utilizate (smartphone, tabletă, calculator desktop, notebook);

2) va furniza o interfață în limbile română (implicit), engleză și rusă. Pentru facilitarea utilizatorilor, soluția informatică va dispune de un sistem de ajutor contextual online (versiunea în limba română – obligatorie) la nivelul fiecărei interfețe utilizator;

3) va furniza o interfață personalizată fiecărei categorii de utilizatori și aplicații în funcție de categoriile utilizatorilor (drepturile și rolurile acestora).

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SERVICIULUI e-KYC

13. Proprietarul serviciului e-KYC este statul.

14. Posesorul și deținătorul serviciului e-KYC este Instituția publică „Agenția de Guvernare Electronică” (în continuare - posesor).

15. Administratorul tehnic al serviciului e-KYC este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare - deținător), care exercită inclusiv rolul de prestator de servicii de încredere calificat.

16. Utilizatorii serviciului e-KYC:

solicitantul – persoană fizică a cărei identitate urmează să fie dovedită pentru a deveni utilizator sau beneficiar al unui serviciu, inclusiv al unui serviciu de încredere calificat, prestat în conformitate cu Legea 124/2022;

beneficiarul serviciului e-KYC – prestator de servicii, care deține sisteme informaționale și prestează solicitanților anumite servicii (servicii de încredere, servicii publice, servicii notariale, servicii financiar-bancare etc.), inclusiv în mod digital.

Capitolul V

SPAȚIUL INFORMAȚIONAL AL SERVICIULUI e-KYC

17. Totalitatea obiectelor informaționale de bază, care reprezintă resursa informațională a serviciului e-KYC, se determină în funcție de destinația acestuia și include:

- 1) solicitantul;
- 2) beneficiarul serviciului e-KYC;
- 3) dispozitivul utilizatorului;
- 4) solicitarea de identificare;
- 5) rezultatul verificării;
- 6) solicitarea de înregistrare.

18. Identificatorul obiectului informațional „solicitantul” este numărul de identificare de stat al persoanei fizice (IDNP).

19. Identificatorul obiectului informațional „beneficiarul serviciului e-KYC” este numărul de identificare de stat al persoanei juridice (IDNO), după caz numărul de identificare de stat al persoanei fizice (IDNP).

20. Identificatorul obiectului informațional „dispozitivul utilizatorului” constituie un cod unic de identificare, transmis în procesul de înregistrare a dispozitivului în cadrul serviciului e-KYC.

21. Identificatorul obiectului informațional „solicitarea de identificare” este constituit de un cod unic de identificare, atribuit de serviciul e-KYC.

22. Identificatorul obiectului informațional „rezultatul verificării” este constituit de un cod unic de identificare, atribuit de serviciul e-KYC.

23. Identificatorul obiectului informațional „solicitarea de înregistrare” este constituit de un cod unic de identificare, atribuit de serviciul e-KYC.

24. Obiectele informaționale împrumutate – „persoana fizică” și „persoana juridică” – sunt inițial înregistrate și identificate în alte resurse informaționale de stat, respectiv Registrul de stat al populației și Registrul de stat al unităților de drept, pentru care nemijlocit în serviciul e-KYC se mențin numai numerele de identificare – în acest caz nu se admite modificarea identificatorului. Toate datele suplimentare necesare sunt accesibile din Registrul de stat al populației sau Registrul de stat al unităților de drept, iar în caz de necesitate – sunt completate sau accesate din alte sisteme informaționale de stat.

25. Obiectele informaționale reprezintă totalitatea de date care le caracterizează:

- 1) datele obiectului informațional „solicitantul”:
 - a) numele și prenumele;

- b) IDNP;
- c) datele de contact (telefon, adresa poștei electronice (e-mail) etc.).
- 2) datele despre obiectul informațional „beneficiarul serviciului e-KYC”:
 - a) denumire, după caz numele și prenumele;
 - b) IDNO, după caz IDNP;
 - c) date de contact (telefon, adresa poștei electronice (e-mail) etc.);
 - d) sistemul informațional integrat cu serviciul e-KYC și date despre acesta.
- 3) datele despre obiectul informațional „dispozitivul utilizatorului”:
 - a) denumirea;
 - b) ID – numărul de identificare;
 - c) adresa IP și datele tehnice ale dispozitivului solicitantului.
- 4) datele despre obiectul informațional „solicitarea de identificare”:
 - a) ID – numărul de identificare;
 - b) date despre solicitant;
 - c) conținutul solicitării;
 - d) data și ora inițierii procesului de identificare;
 - e) date despre actul de identitate utilizat în procesul identificării;
 - f) imaginile faciale preluate în procesul identificării;
 - g) imaginile video înregistrate în procesul identificării;
 - h) rezultatul verificării identității de la distanță;
 - i) date despre alte probe colectate în procesul de identificare;
 - j) consimțământul solicitantului;
 - k) date despre beneficiarul serviciului e-KYC.
- 5) datele despre obiectul informațional „rezultatul verificării”:
 - a) ID – numărul de identificare;
 - b) verdictul verificării identității la distanță (reușit sau nereușit);
 - c) motivele care au generat verdictul „nereușit”;
 - d) data la care a fost emis verdictul;
 - e) rezultatul verificării identității la distanță trimisă serviciului client.
- 6) datele despre obiectul informațional „solicitarea de înregistrare”:
 - a) ID – numărul de identificare;
 - b) numele și prenumele solicitantului;
 - c) IDNP;
 - d) conținutul solicitării;
 - e) consimțământul solicitantului;
 - f) date despre destinatarul solicitării;
 - g) alte date relevante.

26. Scenarul de bază al serviciului e-KYC reprezintă o listă a evenimentelor aferente obiectelor informaționale gestionate, și anume:

- 1) inițierea procesului de identificare la distanță:
solicitantul trebuie să dispună de un act de identitate biometric și un dispozitiv care are o cameră funcțională și acceptă tehnologia NFC;
- solicitantul vizualizează informațiile despre procesul de identificare a persoanei la distanță;

după care examinează și acceptă termenii și condițiile de utilizare a serviciului e-KYC;

descarcă și instalează aplicațiile necesare.

2) colectarea datelor pentru identificare:

solicitantul completează formularul solicitării;

pentru identificarea solicitantului acesta scanează actul de identitate prin recunoașterea optică a zonei MRZ și citirea prin NFS a datelor înscrise pe componenta de securitate a actului de identitate biometric;

solicitantul oferă consimțământul în vederea parcurgerii procesului de identificare și asupra scopului identificării, precum și pentru realizarea de fotografii, capturi de imagini și/sau colectare de date ale sale și ale actului de identitate;

serviciul e-KYC, în mod automatizat preia date suplimentare din surse externe (registre de stat, registre private etc.);

serviciul e-KYC asigură efectuarea înregistrărilor foto și video;

serviciul e-KYC realizează interacțiunea cu solicitantul pentru detectarea biometrică a vitalității feței solicitantului din imaginile preluate (Biometric Liveness Detection).

3) validarea datelor colectate, la această etapă serviciul e-KYC în mod automatizat:

verifică autenticitatea actului de identitate și a datelor pe care le conține cu datele din Registrul de stat al populației;

realizează conversia în date a imaginilor preluate (crearea amprente faciale) și compararea acestora cu cele din Registrul de stat al populației. Verificarea identității solicitantului este efectuată pe baza potrivirii feței și a detectării biometrice a vitalității feței solicitantului printr-un algoritm de învățare profundă. În timpul sesiunii de verificare a identității, se face o comparație între un instantaneu luat dintr-un flux video selfie cu imaginea persoanei preluată din Registrul de stat al populației, după caz citită de pe componenta de securitate a actului de identitate, pentru a determina vitalitatea feței solicitantului;

verifică numărul de telefon și/sau adresa de e-mail a solicitantului prin folosirea unui sistem de parole unice (OTP-One Time Password);

efectuează verificarea autenticității și consistenței altor date colectate în procesul de identificare la distanță, prin compararea acestora cu datele din surse externe de date (registre de stat, registre private etc.).

4) verificarea automatizată de către serviciul e-KYC a datelor colectate în vederea stabilirii identității solicitantului, după caz, datele furnizate în procesul de identificare sunt verificate suplimentar de către un operator.

5) serviciul e-KYC după stabilirea identității persoanei, remite în mod automatizat beneficiarului serviciului e-KYC confirmarea identificării solicitantului la distanță și attributele de identitate ale acestuia.

6) generarea sub formă de document electronic a unei cereri sau solicitări de înregistrare și transmiterea acesteia în regim automatizat către serviciul client (pas optional – stabilit în baza acordului cu beneficiarul serviciului e-KYC).

7) crearea dosarului electronic de evidență.

Capitolul VI

SPAȚIUL TEHNOLOGIC AL SERVICIULUI e-KYC

27. La dezvoltarea serviciului e-KYC se va aplica arhitectura multi-nivel (având cel puțin următoarele nivele – baza de date, logica de aplicație și interfața cu utilizatorul) și principiile agile. Utilizarea unei astfel de arhitecturi și principii va permite o cuplare redusă între componente, în care responsabilitățile fiecărei componente sunt specializate, precum și implementarea iterativă, operarea modificărilor și flexibilitate în implementare.

28. Spațiul informațional va utiliza standarde deschise și va fi compatibil cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

29. Serviciul e-KYC va utiliza soluții de identificare video care folosesc tehnologia IA pentru a minimiza riscul de fraudă. De asemenea, în scopul descurajarea activităților frauduloase și furnizării probelor în cadrul procedurilor judiciare, serviciul e-KYC va păstra datele colectate în procesul de identificare a persoanei.

30. Serviciul e-KYC va putea fi ușor de scalat, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

31. Sistemul de comunicații se va baza pe infrastructura și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării redundante la internet. Infrastructura existentă va fi planificată în mod corespunzător, pentru a oferi nivelele adecvate de performanță și capacitate.

32. Interfațele de utilizare ale serviciului e-KYC se vor adapta automat la diverse rezoluții de afișare și vor fi disponibile în limbile română, rusă și engleză.

33. Interfațele de utilizare ale platformei e-KYC vor fi implementate folosind tehnologii progresive pentru aplicații web și vor fi funcționale pe dispozitivele mobile.

34. Având în vedere locul și rolul serviciului e-KYC în cadrul serviciilor electronice, este necesară o disponibilitate înaltă și accesul neîntrerupt la acesta. Din acest motiv, întreaga soluție va fi construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână).

Capitolul VII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

35. Securitatea informațională presupune protecția serviciului e-KYC, la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

36. Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Personalul implicat în utilizarea și administrarea serviciului e-KYC va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus.

37. Serviciul e-KYC asigură următoarele obiective de securitate:

- 1) autentificarea – garantează că zonele restricționate ale serviciului e-KYC vor fi accesibile doar utilizatorilor cu o identitate verificată;
- 2) autorizarea – garantează că utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;
- 3) confidențialitatea – garantează că datele înregistrate în serviciul e-KYC nu pot fi accesate de o parte terță neautorizată;
- 4) integritatea – garantează că datele înregistrate în serviciul e-KYC nu au fost modificate sau alterate de o parte terță neautorizată;
- 5) non-repudierea – garantează că datele înregistrate în serviciul e-KYC nu pot fi negate mai târziu.

38. O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității sistemului și pentru monitorizarea activității utilizatorilor. Orice acțiune a utilizatorilor se documentează în registre electronice speciale, arătând momentul și utilizatorul care a efectuat acțiunea. Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate. Serviciul e-KYC jurnalizează evenimentele de business critice prin intermediul serviciului electronic guvernamental de jurnalizare (MLog). Acțiunile care sunt jurnalizate prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) pot fi configurate în opțiunile de administrare. Serviciul e-KYC jurnalizează local evenimente ce țin de buna funcționare a sistemului.

ÎNCHEIERE

Prezentul Concept conține descrierea principalelor aspecte organizaționale, metodologice și tehnologice în conformitate cu care este concepută și implementată soluția de identificare și verificare a identității persoanei la distanță.

Implementarea soluției crează condițiile necesare pentru înregistrarea utilizatorilor la distanță prin mecanisme parțial automatizate sau complet automatizate care ar verifica datele transmise de către solicitanții de semnătură, inclusiv fotografii și înregistrări video, pe baza înregistrărilor de stat și a altor surse de date de verificare.

Serviciul e-KYC își propune să fie unul flexibil și adaptabil, ținând cont de sursele de date emergente și de progresele tehnologice, cum ar fi generarea în timp real a videoclipurilor false etc. Prin implementarea diferitelor criterii bazate pe cazuri de utilizare, accesul solicitantului la dovezi și nivelurile de asigurare necesare, sistemul asigură o abordare personalizată a verificării identității. În plus, soluția va calcula un scor total de risc folosind coeficienți configurabili și își păstrează capacitatea de a se opune întregului proces, dacă este necesar.

Totodată, implementarea serviciului e-KYC generează oportunitatea de identificare și verificare a identității persoanelor străine posesoare a unui act de identitate biometric emis de către un alt stat.