



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2022

Chișinău

Cu privire la serviciul guvernamental de identitate și semnătură electronică mobilă (MobiSign)

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 instituie serviciul guvernamental de identitate și semnătură electronică mobilă (MobiSign).

2. Se aprobă:

1) Conceptul serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), conform anexei nr. 1;

2) Regulamentul privind modul de funcționare și utilizare a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), conform anexei nr. 2.

3. Se desemnează Instituția Publică Agenția de Guvernare Electronică în calitate de posesor al serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign).

4. Se desemnează Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică în calitate de deținător al serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign).

5. Instituția Publică Agenția de Guvernare Electronică:

1) va asigura crearea, mentenanța corectivă și adaptivă, precum și dezvoltarea continuă a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign);

2) va asigura disponibilitatea aplicației mobile prin publicare pe principalele platforme/magazine online de aplicații mobile.

6. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică:

1) va asigura administrarea și mentenanța preventivă a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign);

2) va asigura prestarea serviciilor de certificare pentru crearea semnăturii electronice avansate calificate prin intermediul serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign);

3) va asigura mijloacele tehnice și/sau de program configurate, utilizate pentru punerea în aplicare a datelor de creare/verificare a semnăturii electronice;

4) va asigura verificarea identității persoanei, recepționarea cererilor de certificare a cheii publice, revocarea certificatului cheii publice și suspendarea serviciului MobiSign prin intermediul:

a) propriilor centre de înregistrări;

b) centrelor multifuncționale ale Instituției Publice Agenția Servicii Publice;

c) misiunilor diplomatice/oficiilor consulare;

d) altor prestatori de servicii de înregistrare.

7. Ministerul Afacerilor Externe și Integrării Europene și Instituția Publică Agenția Servicii Publice, prin intermediul entităților menționate în pct. 6 subpct. 4) lit. b) și c), în condițiile acordului semnat cu Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, vor realiza, fără perceperea unor plăți, prestarea serviciilor de înregistrare în vederea obținerii certificatului calificat al cheii publice.

8. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică va presta, fără perceperea unor plăți, serviciile aferente procesului de certificare a cheii publice, precum și serviciile de creare și verificare a semnăturii electronice prin intermediul serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign).

9. Entitățile publice implicate în procesul de implementare a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) vor întreprinde acțiunile necesare pentru ajustarea cadrului normativ aferent.

10. În scopul implementării prezentei hotărâri, Cancelaria de Stat în comun cu Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică și Instituția Publică Agenția de Guvernare Electronică vor estima anual costurile necesare pentru prestarea și dezvoltarea continuă a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), iar Ministerul Finanțelor,

în conformitate cu prevederile Legii finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014, va propune alocarea în legea bugetului de stat pentru anul respectiv a mijloacelor bugetare necesare în acest sens.

Prim-ministru

NATALIA GAVRILIȚA

Contrasemnează:

Viceprim-ministru
pentru digitalizare

Iurie ȚURCANU

CONCEPTUL
serviciului guvernamental de identitate
și semnătură electronică mobilă (MobiSign)

INTRODUCERE

Ecosistemul de identitate și semnătură electronică este o parte esențială a strategiei digitale a oricărui guvern, către procese digitalizate, sigure, fără hârtie, durabile și cooperarea transfrontalieră sau transorganizațională. Cererea de semnături electronice apare de fiecare dată când este nevoie de a lega o decizie sau o tranzacție de o anumită persoană sau entitate și de a asigura integritatea datelor. Posibilitatea de a conduce toate afacerile și interacțiunile din domeniul digital a devenit mai presantă, deoarece contactul fizic în contextul actual este limitat.

În Republica Moldova, serviciile electronice există în majoritatea sectoarelor guvernamentale și reprezintă un canal de livrare mai ușor și mai convenabil decât canalele tradiționale de prestare a serviciilor publice.

Totuși, de cele mai multe ori, pentru a avea acces la serviciile electronice, persoanele fizice și juridice trebuie să dispună de o identitate electronică, care se bazează pe infrastructura cheilor publice (PKI) națională.

Datele statistice pentru anul 2021 indică faptul că circa 200 mii de persoane dispun de o identitate electronică, care se bazează pe infrastructura cheilor publice (PKI) națională, ceea ce reprezintă circa 9-10% din populația adultă a Republicii Moldova.

Pe lângă lipsa cunoștințelor de utilizare, conștientizarea avantajelor și oportunităților oferite de instrumentelor de semnătură electronică, reticența față de serviciile electronice, un impediment deseori invocat îl reprezintă cheltuielile aferente obținerii și utilizării certificatului calificat al cheii publice. În cele mai dese cazuri, costul de obținere și utilizare a certificatului cheii publice împiedică utilizatorii ocazionali, în special persoanele fizice, să meargă la ghișeu pentru a o obține.

Un factor important care contribuie la creșterea acestui cost este necesitatea deținerii unui dispozitiv fizic care stochează în siguranță cheia privată utilizată pentru a crea semnătura electronică avansată calificată. Există mai multe tipuri de dispozitive de creare a semnăturii electronice, cum ar fi o cartelă SIM, dispozitiv USB specializat sau cartelă criptografică. Toate acestea încorporează un cip criptografic specializat care garantează prin construcția sa secretul cheii private a deținătorului. Utilizarea dispozitivelor fizice specializate de către utilizatori presupune costuri de achiziție și probleme logistice legate de depozitarea, transportul și distribuția acestora, în special deoarece acestea sunt realizate într-un mod reglementat. Dispozitivele fizice au, de asemenea, proprietatea de a fi

pierdute, uzate sau distruse fizic prin neglijență. Utilizarea dispozitivelor fizice implică, de asemenea, o dependență de capacitățile de stocare și algoritmice ale cipului criptografic utilizat. Necesitatea unor modificări ale capacității de stocare sau a algoritmilor implementați de producătorul dispozitivului poate duce la necesitatea de a schimba dispozitivul fizic.

Cercetarea criptografică modernă, omniprezența telefoanelor mobile și practica internațională au arătat că există alternative la fel de sigure pentru păstrarea cheii private care nu necesită dispozitive fizice specializate. O soluție alternativă viabilă, accesibilă și sigură este de a împărți cheia privată în două componente și de a le păstra la ambii participanți în proces: o parte în telefonul mobil sub controlul exclusiv al titularului și o a doua parte la prestatorul de servicii de încredere. Acest lucru asigură imposibilitatea compromiterii cheii private prin compromiterea telefonului mobil în mod individual, dar garantează, de asemenea, controlul deplin al deținătorului asupra procesului de creare a semnăturilor electronice. Cu alte cuvinte, semnătura poate fi creată numai cu participarea ambelor părți la proces, titularul având control asupra procesului, în timp ce prestatorul poate asigura securitatea acestuia, inclusiv prin blocarea utilizării cheii private atunci când PIN-ul este introdus incorect și în mod repetat.

O soluție de identificare mobilă bazată pe infrastructura cheilor publice (PKI) oferă cel puțin același nivel de securitate ca și soluțiile bazate pe dispozitive specializate cu cip. Cu toate acestea, există mai multe avantaje semnificative. De exemplu, nu este nevoie de cititoare de carduri și software-ul corespunzător. Soluțiile mobile sunt, de asemenea, mai ușor și mai convenabil de utilizat, inclusiv din afara teritoriului Republicii Moldova.

În acest sens, se propune instituirea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), care va oferi un grad similar de securitate a cheilor private în comparație cu soluțiile existente bazate pe dispozitive specializate, dar fără a fi necesară utilizarea acestora. Soluția respectivă se bazează pe algoritmi criptografici avansați, iar securitatea unei implementări similare, în unele state din Uniunea Europeană a fost certificată ca avansată calificată și în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, publicat în Jurnalul Oficial al Uniunii Europene L 257 din 28 august 2014.

Capitolul I

DISPOZIȚII GENERALE

1. Serviciul guvernamental de identitate și semnătură electronică mobilă (MobiSign) (în continuare – *serviciul MobiSign*) este o soluție de identitate electronică bazată pe aplicații mobile și are ca obiectiv principal oferirea instrumentului de autentificare și semnare a documentelor electronice, inclusiv

prin intermediul sistemelor informaționale integrate cu serviciul electronic guvernamental integrat de semnătură electronică (MSign) (în continuare – serviciul MSign) și serviciul guvernamental de autentificare și control al accesului (MPass) (în continuare – *MPass*).

2. Serviciul MobiSign este parte componentă a sistemelor informaționale de stat ale Republicii Moldova și reprezintă un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, care are drept scop oferirea unui mecanism eficient, fiabil și modern de identificare electronică și creare a semnăturilor electronice avansat calificate, prin intermediul aplicației mobile.

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

date de identificare personală – set de date care permit stabilirea identității unei persoane fizice;

dispozitivul utilizatorului – orice dispozitiv inteligent (telefon sau tabletă) care se află în posesia utilizatorului compatibil cu aplicația mobilă a serviciului MobiSign;

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

4. Obiective de bază specifice stabilite pentru serviciul MobiSign:

1) implementarea unui model distribuit de identificare și înregistrare a utilizatorilor;

2) facilitarea utilizării identității electronice și creării semnăturii electronice de către cetățenii Republicii Moldova aflați în străinătate;

3) sporirea accesibilității la serviciile de aplicare a semnăturii electronice și implicit la serviciile electronice disponibile;

4) crearea condițiilor pentru înregistrarea la distanță a utilizatorilor și automatizarea procesului de verificare a identității.

5. Principiile de bază ale serviciului MobiSign sunt:

1) principiul legalității, care presupune crearea și exploatarea serviciului MobiSign 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 MobiSign 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 MobiSign;

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 MobiSign, 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 MobiSign 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 MobiSign cu sistemele informaționale partajate existente în țară;

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

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

Capitolul II

CADRUL NORMATIV-JURIDIC AL SERVICIULUI MOBISIGN

6. Implementarea serviciului MobiSign este inclusă în Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr. 235/2021.

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

1) Legea nr. 91/2014 privind semnătura electronică și documentul electronic;

2) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

3) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

4) Legea nr. 133/2011 privind protecția datelor cu caracter personal;

5) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

6) Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010;

7) Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017;

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;

9) Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect), aprobat prin Hotărârea Guvernului nr. 211/2019;

10) Regulamentul privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice, aprobat prin Hotărârea Guvernului nr. 1140/2017;

11) Regulamentul privind utilizarea, administrarea și dezvoltarea platformei tehnologice comune (MCloud), aprobat prin Hotărârea Guvernului nr. 128/2014;

12) Regulamentul privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), aprobat prin Hotărârea Guvernului nr. 405/2014;

13) Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr. 1090/2013;

14) Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr. 708/2014;

15) Regulamentul privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify), aprobat prin Hotărârea Guvernului nr. 376/2020;

16) Regulamentul privind utilizarea, administrarea și dezvoltarea Portalului guvernamental al cetățeanului, aprobat prin Hotărârea Guvernului nr. 413/2020;

17) Reglementarea tehnică „Procese ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;

18) Normele tehnice în domeniul semnăturii electronice avansate calificate, aprobate prin Ordinul directorului Serviciului de Informații și Securitate al Republicii Moldova nr. 69/2016.

Capitolul III

SPAȚIUL FUNCȚIONAL AL SERVICIULUI MOBISIGN

8. Funcțiile de bază ale serviciului MobiSign sunt:

1) înregistrarea identităților electronice și a datelor de identificare personală aferente acestora;

2) furnizarea informațiilor pentru identificarea electronică a persoanei în procesul de autentificare în cadrul sistemelor informaționale;

3) crearea semnăturilor electronice pentru semnarea documentelor electronice.

9. Având în vedere funcțiile sale de bază, serviciul MobiSign va avea următoarele contururi funcționale de bază:

1) Conturul „Spațiul prestatorului de servicii de înregistrare” care asigură următoarele funcții specifice:

- a) verificarea identității persoanei și datelor de identificare personală ale acesteia;
- b) generarea cererii de certificare a cheii publice;
- c) confirmarea identităților electronice și înregistrarea datelor de identificare personală aferente acestora.

2) Conturul „Spațiul operatorului centrului de suport”:

a) acces la datele de înregistrare și de contact ale utilizatorului, disponibile în serviciul MobiSign;

b) acces la istoricul utilizatorului din serviciul MobiSign;

c) suspendarea/restabilirea serviciului MobiSign;

d) revocarea certificatului cheii publice a utilizatorului.

3) Conturul „Spațiul utilizatorului serviciului MobiSign” care asigură următoarele funcții specifice:

a) generarea perechii de chei publice și private;

b) crearea și modificarea codului PIN și/sau setarea metodelor de păstrare sigure a informației - autentificarea biometrică;

c) depunerea cererii pentru eliberarea repetată a certificatului cheii publice;

d) solicitarea suspendării/revocării identității electronice și certificatului cheii publice înregistrate.

4) Conturul „Spațiul de autoservire a utilizatorului serviciului MobiSign”:

a) gestionarea listei dispozitivelor proprii înregistrate pentru utilizarea serviciului MobiSign;

b) vizualizarea istoricului propriu privind utilizarea serviciului MobiSign;

c) înregistrarea identității electronice și a datelor de identificare personală, folosind altă soluție de semnătură electronică.

5) Conturul „Administrare și Control”, care asigură următoarele funcții:

a) administrarea serviciului MobiSign;

b) asigurarea integrității logice a serviciului MobiSign;

c) gestionarea rolurilor operatorilor;

d) asigurarea securității și protecției informației în cadrul serviciului MobiSign;

e) gestionarea copiilor de rezervă;

f) jurnalizarea evenimentelor de sistem;

g) monitorizarea performanței serviciului MobiSign;

h) suportul tehnic și mentenanța.

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SERVICIULUI MOBISIGN

10. Proprietarul serviciului MobiSign este statul.

11. Posesorul serviciului MobiSign este Instituția Publică Agenția de Guvernare Electronică (în continuare – *posesor*).

12. Deținătorul și administratorul tehnic al serviciului MobiSign este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică (în continuare – *deținător*), care exercită inclusiv rolul de prestator de servicii de certificare.

13. Utilizatorii serviciului MobiSign sunt titularii certificatelor cheii publice, identificați și înregistrați de către prestatorul de servicii de certificare sau un prestator de servicii de înregistrare, care beneficiază de funcționalitățile de identificare electronică și creare a semnăturii electronice.

14. Prestatorul de servicii de înregistrare este persoana care prestează servicii privind verificarea identității solicitantului, înregistrarea și transmiterea cererii de certificare a cheii publice către prestatorul de servicii de certificare din numele solicitantului semnăturii electronice, și are acces la funcționalitățile serviciului MobiSign destinate înregistrării cererii de certificare a cheii publice și verificării identității solicitantului.

Capitolul V

SPAȚIUL INFORMAȚIONAL AL SERVICIULUI MOBISIGN

15. Totalitatea obiectelor informaționale de bază, care reprezintă resursa informațională a serviciului MobiSign, se determină în funcție de destinația acestuia și include:

- 1) utilizatorul serviciului MobiSign;
- 2) prestatorul de servicii de înregistrare;
- 3) dispozitivul utilizatorului;
- 4) solicitarea de înregistrare;
- 5) solicitarea de autentificare;
- 6) solicitarea de semnare;
- 7) certificatul cheii publice.

16. Identificatorul obiectului informațional „utilizatorul serviciului MobiSign” este numărul de identificare de stat al persoanei fizice (IDNP).

17. Identificatorul obiectului informațional „prestatorul de servicii de înregistrare” este numărul de identificare de stat al persoanei juridice (IDNO), după caz numărul de identificare de stat al persoanei fizice (IDNP).

18. Identificatorul obiectului informațional „dispozitivul utilizatorului” constituie un cod unic de identificare, transmis în procesul de înregistrare a dispozitivului în cadrul serviciului MobiSign.

19. Identificatorul obiectului informațional „solicitarea de înregistrare” este constituit de un cod unic de identificare, atribuit de serviciul MobiSign.

20. Identificatorul obiectului informațional „solicitarea de autentificare” este constituit de un cod unic de identificare, atribuit de serviciul MobiSign.

21. Identificatorul obiectului informațional „solicitarea de semnare” este constituit de un cod unic de identificare, atribuit de serviciul MobiSign.

22. Identificatorul obiectului informațional „certificatul cheii publice” este constituit de un număr de serie unic, atribuit de către infrastructura unică a cheii publice (PKI) a Guvernului.

23. Obiectele informaționale „solicitarea de autentificare” și „solicitarea de semnare” sunt păstrate temporar în cadrul serviciului MobiSign din rațiuni tehnologice pentru facilitarea proceselor de autentificare, respectiv de semnare a documentelor electronice, după care în regim automatizat se șterg.

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

- 1) datele obiectului informațional „utilizatorul serviciului MobiSign”:
 - a) numele și prenumele;
 - b) IDNP;
 - c) datele de contact (telefon, adresa poștei electronice (e-mail) etc.).
- 2) datele despre obiectul informațional „prestatorul de servicii de înregistrare”:
 - a) denumire, după caz numele și prenumele;
 - b) IDNO, după caz IDNP;
 - c) datele de contact (telefon, adresa poștei electronice (e-mail) etc.).
- 3) datele despre obiectul informațional „dispozitivul utilizatorului”:
 - a) denumirea;
 - b) ID – număr de identificare;
 - c) cheile dispozitivului.
- 4) datele despre obiectul informațional „solicitarea de înregistrare”:
 - a) ID – număr de identificare;
 - b) conținutul solicitării stabilit conform cadrului normativ.
- 5) datele despre obiectul informațional „solicitarea de autentificare”:
 - a) ID – număr de identificare;
 - b) ID - dispozitivul utilizatorului;
- 6) datele despre obiectul informațional „solicitarea de semnare”:
 - a) ID – număr de identificare;
 - b) ID - dispozitivul utilizatorului;

- c) documentele spre semnare.
- 7) datele despre obiectul informațional „certificatul cheii publice”:
 - a) ID - număr de identificare;
 - b) conținutul certificatului stabilit conform cadrului normativ.

25. Scenariile de bază ale serviciului MobiSign reprezintă o listă a evenimentelor aferente obiectelor informaționale gestionate, și anume:

- 1) în cazul înregistrării identității utilizatorului serviciului MobiSign:
 - a) la prestatorul de servicii de certificare sau la prestatorul de servicii de înregistrare:
 - solicitantul descarcă pe propriul dispozitiv, aplicația mobilă a serviciului MobiSign;
 - pentru stabilirea identității, solicitantul prezintă un act de identitate, datele căruia sunt verificate de prestatorul de servicii de certificare sau prestatorul de servicii de înregistrare în conformitate cu datele de identificare ale solicitantului actualizate și disponibile în cadrul Registrului de stat al populației;
 - după stabilirea identității, solicitantul în cadrul aplicației serviciului MobiSign scanează codul QR expus;
 - generarea perechii de chei pentru semnare;
 - împărțirea cheii private în 2 părți cu salvarea unei părți a cheii în dispozitivul utilizatorului în formă criptată cu ajutorul PIN-ului și/sau a biometriei și transmiterea spre înregistrare a celeilalte părți a cheii la prestatorul de servicii de certificare;
 - semnarea și înregistrarea certificatului cheii publice;
 - în cazul înregistrării la prestatorul de servicii de înregistrare, acesta realizează verificarea identității solicitantului, înregistrarea și transmiterea cererii de certificare a cheii publice către prestatorul de servicii de certificare din numele solicitantului semnăturii electronice, în conformitate cu regulamentul aprobat de către prestator de servicii de certificare și avizat de către organul competent în domeniul semnăturii electronice.
 - b) folosind altă soluție de semnătură electronică, fără necesitatea prezenței fizice la un prestator de servicii de înregistrare:
 - solicitantul descarcă pe propriul dispozitiv, aplicația mobilă a serviciului MobiSign;
 - selectează din aplicația mobilă a serviciului MobiSign, modalitatea de înregistrare folosind altă soluție de semnătură electronică al cărei utilizator este;
 - solicitantul introduce datele de verificare și datele sale contact;
 - semnează cererea de certificare a cheii publice prin intermediul serviciului MSign;
 - generarea perechii de chei pentru autentificare și semnare;
 - împărțirea cheii private în 2 părți cu salvarea unei părți a cheii în dispozitivul utilizatorului în formă criptată cu ajutorul PIN-ului și/sau a biometriei și

transmiterea spre înregistrare a celeilalte părți a cheii la prestatorul de servicii de certificare;

semnarea și înregistrarea certificatului cheii publice.

2) în cazul autentificării în cadrul sistemelor informaționale:

a) utilizatorul accesează interfața web a serviciului MPass;

b) din soluțiile de autentificare disponibile în cadrul serviciului MPass, utilizatorul selectează serviciul MobiSign;

c) utilizatorul introduce codul PIN sau folosește autentificarea biometrică pentru a confirma autentificarea în aplicația serviciului MobiSign;

d) după ce serviciul MobiSign finalizează procesul de autentificare, serviciul MPass primește confirmarea de autentificare.

3) în cazul semnării unui document în format electronic:

a) după ce accesează interfața web a serviciului MSign, utilizatorul selectează soluția de semnare serviciul MobiSign;

b) utilizatorul introduce codul PIN pentru aprobarea semnării documentului sau documentelor în interfața aplicației serviciului MobiSign;

c) după ce serviciul MobiSign finalizează procesul de semnare, serviciul MSign primește documentele finale semnate.

26. În cadrul serviciului MobiSign procesul de autentificare și semnare are loc exclusiv la inițiativa și sub controlul utilizatorului, securitatea cheii private fiind asigurată de faptul că sunt implicate de fiecare dată ambele părți: aplicația serviciului MobiSign instalată pe dispozitivul utilizatorului și serviciul MobiSign gestionat de către deținătorul serviciului MobiSign. În același timp, în cadrul tuturor scenariilor de utilizare, fiecare parte nu poate să restabilească întreaga cheie privată.

27. Serviciul MobiSign va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud).

28. Serviciul MobiSign va interacționa cu următoarele sisteme informaționale:

1) platforma de interoperabilitate (MConnect) – pentru schimbul de date cu registrele și sistemele informaționale de stat;

2) serviciul guvernamental de autentificare și control al accesului (MPass) – pentru identificarea electronică în cadrul sistemelor informaționale;

3) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea electronică a documentelor electronice;

4) serviciul electronic guvernamental de jurnalizare (MLog) – pentru jurnalizarea evenimentelor;

5) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea utilizatorilor;

6) portalul guvernamental al cetățeanului – pentru autoservirea în cadrul serviciului MobiSign.

Capitolul VI

SPAȚIUL TEHNOLOGIC AL SERVICIULUI MOBISIGN

29. La dezvoltarea serviciului MobiSign 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.

30. 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.

31. Serviciul MobiSign va utiliza serviciile de certificare și componentele aplicative oferite în cadrul infrastructurii unice a cheii publice a Guvernului.

32. Serviciul MobiSign este bazat pe algoritmi criptografici avansați, simetrici și asimetrici. Principiul de bază de funcționare al acestuia constă în faptul utilizării cheii private distribuite pentru algoritmi asimetrici RSA, care presupune generarea unei perechi de chei pe dispozitivul mobil al utilizatorului și a unei alte perechi de chei pe dispozitivul securizat al prestatorului serviciilor de certificare.

33. Utilizând resursele dispozitivului utilizatorului are loc declanșarea procesului de generare a perechii de chei și divizarea cheii private. O componentă a cheii private este păstrată exclusiv sub controlul utilizatorului în formă criptată în baza PIN-ului introdus de utilizator.

34. Cheia privată generată pe partea deținătorului serviciului MobiSign se creează utilizând mijloace tehnice de program asigurându-se accesul la aceasta exclusiv la solicitarea utilizatorului. Ca urmare a generării perechilor de chei, utilizând tehnologiile criptografice în baza algoritmului RSA de partajare a cheii private și a fuziunii cheilor publice generate separate pe dispozitivul utilizatorului și modulul de securitate hardware (HSM), are loc calcularea unei cheii publice combinate, pentru care se asigură certificarea în modul stabilit de cadrul normativ în domeniul semnăturii electronice.

35. În procesul aplicării semnăturii electronice, utilizatorul în mod expres confirmă aplicarea semnăturii electronice prin introducerea PIN-ului secret,

definit la generarea perechii de chei pentru semnare, care poate fi schimbat doar de către utilizator.

36. Serviciul MobiSign 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.

37. 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.

38. Interfața aplicațiilor mobile ale serviciului MobiSign se va adapta automat la diverse rezoluții de afișare și va fi disponibilă în limbile română, rusă și engleză.

39. Având în vedere locul și rolul serviciului MobiSign 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

40. Securitatea informațională presupune protecția serviciului MobiSign, 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.

41. 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 MobiSign va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus.

42. Serviciul MobiSign asigură următoarele obiective de securitate:

- 1) autentificarea – garantează că zonele restricționate ale serviciului MobiSign 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 MobiSign nu pot fi accesate de o parte terță neautorizată;

4) integritatea – garantează că datele înregistrate în serviciul MobiSign nu au fost modificate sau alterate de o parte terță neautorizată;

5) nonrepudierea – garantează că datele înregistrate în serviciul MobiSign nu pot fi negate mai târziu.

43. Suplimentar mecanismelor de securitate specifice platformei tehnologice guvernamentale comune (MCloud), serviciul MobiSign dispune de următoarele mecanisme:

1) distribuirea aplicației mobile exclusiv prin intermediul platformelor/magazinelor online de aplicații mobile;

2) semnarea aplicației mobile cu cheia privată la compilarea acesteia;

3) comunicare sigură (transferuri de date) între serverele web, aplicație mobilă și utilizatori – schimbul de informații confidențiale este securizat;

4) instrument de jurnalizare – 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 MobiSign 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 MobiSign 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 identitate și semnătură electronică mobilă.

Implementarea serviciului MobiSign va permite implementarea unui model distribuit de identificare și înregistrare a utilizatorilor cu implicarea unui număr semnificativ de prestatori de servicii de înregistrare cu o acoperire geografică mare, cu efort și costuri logistice reduse.

Soluția nu exclude, de asemenea, posibilitatea de a implementa 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. O astfel de posibilitate va fi evaluată ulterior la un nivel tehnic adecvat pentru a menține un grad ridicat de asigurare a identificării corecte a solicitantului și pentru a preveni o posibilă fraudă în acest proces.

Pentru utilizarea serviciului MobiSign, atât de pe teritoriul Republicii Moldova, cât și din străinătate, utilizatorul va avea nevoie de dispozitivul său inteligent (telefon sau tabletă) și conexiune la internet.

Implementarea serviciului MobiSign, se va realiza cu suportul financiar al Programului Națiunilor pentru Dezvoltare (PNUD) Moldova.

Anexa nr. 2
la Hotărârea Guvernului nr.

REGULAMENT
privind modul de funcționare și utilizare a serviciului guvernamental de
identitate și semnătură electronică mobilă (MobiSign)

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind modul de funcționare și utilizare a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) (în continuare – *Regulament*) este elaborat în vederea reglementării modului de organizare și funcționare a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) (în continuare – *serviciul MobiSign*).

2. Serviciul MobiSign este organizat astfel încât să asigure că procesele de înregistrare a identităților electronice, identificare electronică în cadrul sistemelor informaționale și creare a semnăturii electronice, să fie simple, eficiente, accesibile și transparente.

3. Noțiunile utilizate în prezentul Regulament sunt corespunzătoare definițiilor de la pct. 3 din anexa nr. 1.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII,
EXPLOATĂRII ȘI UTILIZĂRII SERVICIULUI MOBISIGN

4. Subiecții din domeniul creării, exploatării și utilizării serviciului MobiSign sunt numiți în capitolul IV al anexei nr.1 din hotărâre.

5. Posesorul are următoarele atribuții:

- 1) asigură condițiile organizatorice, juridice și financiare pentru implementarea serviciului MobiSign;
- 2) stabilește scopurile și funcționalitățile serviciului MobiSign, în conformitate cu prezenta hotărâre;
- 3) stabilește în comun cu deținătorul măsurile tehnice și organizatorice de protecție și securitate a serviciului MobiSign;
- 4) aprobă, după coordonarea cu deținătorul, termenii și condițiile de utilizare a serviciului MobiSign și politica de confidențialitate;
- 5) asigură mentenanța corectivă și adaptivă, precum și dezvoltarea continuă a serviciului MobiSign prin adăugarea de noi componente ce pot fi utilizate de utilizatori;

6) organizează activități de instruire și promovare privind utilizarea serviciului MobiSign;

7) exercită alte atribuții necesare asigurării bunei funcționări a serviciului MobiSign.

6. Posesorul are dreptul:

1) să elaboreze și să dezvolte, prin intermediul Cancelariei de Stat, în baza competențelor sale, cadrul normativ cu privire la serviciul MobiSign;

2) să propună soluții de perfecționare și eficientizare a procesului de funcționare a serviciului MobiSign, precum și să le pună în aplicare în colaborare cu deținătorului serviciului MobiSign.

7. Posesorul este obligat:

1) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor în conformitate cu cadrul normativ aplicabil;

2) să utilizeze informația disponibilă în serviciul MobiSign doar în scopurile stabilite de prezentul Regulament și cadrul normativ aplicabil.

8. Deținătorul are următoarele atribuții:

1) asigură prestarea serviciilor de înregistrare și certificare a cheii publice și serviciilor aferente, conform cadrului normativ aplicabil;

2) asigură mijloacele tehnice și/sau de program configurate, utilizate pentru punerea în aplicare a datelor de creare/verificare a semnăturii electronice;

3) asigură administrarea și mentenanța preventivă a serviciului MobiSign;

4) stabilește în comun cu posesorul măsurile tehnice și organizatorice de protecție și securitate a serviciului MobiSign;

5) controlează procesul de înregistrare și prelucrare a datelor în cadrul serviciului MobiSign;

6) asigură securitatea și protecția datelor;

7) asigură înregistrarea, soluționarea și înlăturarea erorilor, disfuncționalităților și incidentelor care afectează funcționarea normală a serviciului MobiSign;

8) exercită alte atribuții necesare asigurării bunei funcționări a serviciului MobiSign.

9. Deținătorul are dreptul:

1) să solicite de la utilizatori, în cazul detectării erorilor și omisiunilor, actualizarea și corectarea informației furnizate;

2) să propună soluții pentru perfecționarea și eficientizarea procesului de funcționare a serviciului MobiSign, precum și să le pună în aplicare după aprobarea acestora.

10. Deținătorul este obligat:

- 1) să realizeze verificarea identității persoanei și recepționarea cererilor de certificare a cheii publice cu scopul prestării serviciilor de certificare a cheii publice, inclusiv prin intermediul unor părți terțe, desemnate în conformitate cu cadrul normativ aplicabil;
- 2) să asigure atribuirea rolurilor și drepturilor de acces la interfețele serviciului MobiSign și datele acestuia;
- 3) să asigure funcționarea neîntreruptă a serviciului MobiSign în conformitate cu cadrul normativ aplicabil;
- 4) să acorde suportul necesar utilizatorilor care au acces la serviciul MobiSign;
- 5) să informeze utilizatorii despre modificările condițiilor tehnice de funcționare a acestuia;
- 6) să efectueze măsurile organizatorice și tehnice necesare asigurării protecției și confidențialității informației stocate în baza de date a serviciului MobiSign, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;
- 7) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu cadrul normativ în materie de protecția datelor cu caracter personal;
- 8) să asigure prestarea serviciilor în conformitate cu cadrul normativ aplicabil, și termenii și condițiile de prestare a serviciilor;
- 9) să asigure accesul securizat la informația conținută în serviciul MobiSign, respectarea condițiilor de securitate și a regulilor de exploatare a acestuia.

11. Utilizatorul are dreptul:

- 1) să depună cererea de certificare a cheii publice, revocare a certificatului cheii publice și suspendare a serviciului MobiSign la prestatorul de servicii de certificare sau la prestatorul de servicii de înregistrare;
- 2) să transmită cererea de certificare a cheii publice semnată electronic, la adresa electronică a deținătorului;
- 3) să descarce gratuit aplicația mobilă a serviciului MobiSign de pe platformele mobile;
- 4) să acceseze funcționalitățile serviciului MobiSign în conformitate cu prezentul Regulament și termenele și condițiile de utilizare aferente;
- 5) să seteze unele preferințe de interacțiune cu serviciul MobiSign și sistemele aferente;
- 6) să acceseze spațiul informațional al serviciului MobiSign, în limitele rolului atribuit;

7) să exercite dreptul de acces la datele cu caracter personal și dreptul de intervenție asupra datelor cu caracter personal în conformitate cu prevederile legislației din domeniul protecției datelor cu caracter personal;

8) să solicite și să primească de la deținător asistență metodologică și practică de utilizare a serviciului MobiSign;

9) să înainteze posesorului sau deținătorului propuneri privind modificarea actelor normative care reglementează funcționarea serviciului MobiSign;

10) să înainteze posesorului sau deținătorului propuneri privind îmbunătățirea și sporirea eficacității funcționării serviciului MobiSign.

12. Utilizatorul este obligat:

1) să utilizeze funcționalitățile serviciului MobiSign, în conformitate cu prezentul Regulament și regulile de utilizare aferente;

2) să prezinte un act de identitate în procesul de verificare a identității și depunere a cererii de certificare a cheii publice;

3) să creeze codul PIN și/sau să seteze metodele de păstrare sigure a informației – autentificarea biometrică;

4) să respecte condițiile tehnice de utilizare a serviciului MobiSign;

5) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe la dispozitivul său;

6) să nu folosească dispozitive care utilizează sisteme de operare neautorizate de producătorul dispozitivului;

7) să asigure autenticitatea și veridicitatea datelor de contact incluse în serviciul MobiSign.

13. Prestatorul de servicii de înregistrare are dreptul:

1) să acceseze spațiul informațional al serviciului MobiSign, în limitele rolului atribuit;

2) să solicite și să primească de la deținător asistență metodologică și practică de utilizare a serviciului MobiSign în procesul de verificare a identității solicitanților și recepționare a cererilor de certificare a cheii publice, de revocare a certificatului cheii publice și de suspendare a serviciului MobiSign.

14. Prestatorul de servicii de înregistrare este obligat:

1) să verifice datele din actul de identitate prezentat de solicitant cu datele recepționate din Registrul de stat al populației;

2) să asigure corectitudinea, autenticitatea, actualitatea și veridicitatea datelor introduse în serviciul MobiSign;

3) să ofere suport solicitantului în procesul depunerii cererii de certificare a cheii publice și înregistrare în serviciul MobiSign;

4) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

5) să utilizeze funcționalitățile serviciului MobiSign, în conformitate cu prezentul Regulament și regulile de utilizare aferente;

6) să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor.

Capitolul III

ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI

15. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul serviciului MobiSign se efectuează de către subiecții acestuia, cu respectarea strictă a cerințelor față de asigurarea securității informației și a prevederilor legislației din domeniul protecției datelor cu caracter personal.

16. În conformitate cu prevederile cadrului normativ aplicabil, certificatul cheii publice și informația cu privire la certificatul cheii publice atașat semnăturilor electronice avansate calificate sunt păstrate de către prestatorul de servicii de certificare cel puțin 15 ani de la data revocării sau expirării certificatului.

17. La expirarea termenului prevăzut la pct. 16, certificatul cheii publice și informația cu privire la certificatul cheii publice atașat semnăturilor electronice avansate calificate sunt radiate, cu înregistrarea evenimentelor corespunzătoare.

18. Măsurile de protecție și securitate a datelor din serviciul MobiSign reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a serviciului MobiSign și se actualizează de către toți subiecții serviciului MobiSign.

19. Securitatea informațională a serviciului MobiSign se asigură prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al serviciului MobiSign și a procedurilor operaționale.

20. Obiecte ale asigurării protecției și securității informației din serviciul MobiSign se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

1) baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date și alte aplicații care asigură funcționarea serviciului MobiSign;

2) sistemele de comunicații electronice, rețele, servere, calculatoare și alte mijloace tehnice de prelucrare a informației.

21. Protecția informației din serviciul MobiSign la nivel de deținător se efectuează prin următoarele metode:

- 1) asigurarea măsurilor de protecție a datelor, prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date guvernamentale;
- 2) excluderea accesului neautorizat la datele din serviciul MobiSign;
- 3) prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau care cauzează defecțiuni în funcționarea complexului tehnic și de program;
- 4) efectuarea periodică planificată a copiilor de rezervă ale datelor și fișierelor mijloacelor de program;
- 5) efectuarea tuturor măsurilor pentru asigurarea restabilirii și continuității funcționării serviciului MobiSign în cazul incidentelor.

22. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

23. Pentru asigurarea funcționalității eficiente și neîntrerupte a serviciului MobiSign, schimbul informațional de date al serviciului MobiSign este asigurat în regim non-stop.

24. Utilizatorii serviciului MobiSign sunt autorizați să acceseze doar funcționalitățile și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia.

25. Funcționarea serviciului MobiSign se suspendă de către deținător, cu informarea subiecților prin mijloacele tehnice disponibile, în caz de apariție a uneia dintre următoarele situații:

- 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al serviciului MobiSign;
- 2) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea serviciului MobiSign;
- 3) în cazul apariției dificultăților tehnice ce fac imposibilă utilizarea și funcționarea în condiții optime a serviciului MobiSign.

26. Suspendarea funcționării serviciului MobiSign se efectuează asigurându-se un impact minim asupra calității serviciilor livrate utilizatorilor.

Capitolul IV RĂSPUNDEREA

27. Subiecții în ale căror atribuții intră administrarea serviciului MobiSign, introducerea datelor, furnizarea informațiilor și asigurarea funcționării serviciului MobiSign poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

28. Toți subiecții serviciului MobiSign poartă răspundere conform legislației pentru prelucrarea, divulgarea și transmiterea informației ce conține date cu caracter personal persoanelor terțe, contrar prevederilor legislației.

NOTA INFORMATIVĂ

la proiectul hotărârii Guvernului cu privire la serviciul guvernamental de identitate și semnătură electronică mobilă (MobiSign)

1. Denumirea autorului proiectului

Proiectul hotărârii Guvernului este elaborat de către Viceprim-ministrul pentru digitalizare, cu suportul Instituției publice „Agenția de Guvernare Electronică” și Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”.

2. Condițiile ce au impus elaborarea proiectului și finalitățile urmărite

Astăzi oamenii trăiesc într-o lume în schimbare rapidă, în care fluxul de informații, idei și cunoștințe de pe tot globul are un impact profund asupra modului în care funcționează lumea. Guvernele din întreaga lume se confruntă cu provocarea acestei transformări și cu nevoia de a reinventa sistemele publice pentru a furniza servicii, informații și cunoștințe eficiente și rentabile prin tehnologiile informației și comunicațiilor.

Un factor cheie în această transformare este implementarea identității și semnăturii electronice – o componentă esențială a infrastructurii pe care se va construi viitorul sistemelor de e-guvernare și de e-servicii private. Un ID electronic cu capacitate deplină de a face acțiuni obligatorii din punct de vedere legal online – oriunde și oricând – oferă un avantaj imens atât cetățenilor, companiilor, cât și guvernelor.

Ecosistemul de identitate și semnătură electronică este o parte esențială a strategiei digitale a oricărui guvern, către procese digitalizate, sigure, fără hârtie, durabile și cooperarea transfrontalieră sau transorganizațională. Cererea de semnături electronice apare de fiecare dată când este nevoie de a lega o decizie sau o tranzacție de o anumită persoană sau entitate și de a asigura integritatea datelor. Posibilitatea de a conduce toate afacerile și interacțiunile din domeniul digital a devenit mai presantă, deoarece contactul fizic în contextul actual este limitat.

În Republica Moldova, serviciile electronice există în majoritatea sectoarelor guvernamentale și reprezintă un canal de livrare mai ușor și mai convenabil decât canalele tradiționale de prestare a serviciilor publice.

Totuși, de cele mai multe ori, pentru a avea acces la serviciile electronice, persoanele fizice și juridice trebuie să utilizeze semnături electronice calificate, care se bazează pe infrastructura cheilor publice (PKI) națională. Deși PKI este disponibil în Moldova din septembrie 2006, semnăturile electronice și implicit identitățile electronice, sunt folosite de un grup destul de restrâns de persoane care sunt conștiente de avantajul acestora. Companiile sunt obligate să le utilizeze pentru raportarea electronică și, opțional, pentru facturarea electronică sau semnarea contractelor, în timp ce funcționarii publici au obligația de a utiliza semnăturile electronice pentru declarațiile de avere și a intereselor personale și în alte scopuri specifice atribuțiilor pe care le exercită.

Datele statistice pentru anul 2021 indică faptul că există circa 200 mii de utilizatori activi de semnături electronice, care reprezintă sub 10% din populația adultă a Republicii Moldova.

Prin definiție, o identitate electronică bazată pe o semnătură electronică avansată calificată permite interacțiunea electronică securizată între cetățeni, mediul de afaceri și autoritățile publice. Pe lângă lipsa cunoștințelor de utilizare, conștientizarea avantajelor și oportunităților oferite de utilizarea semnăturilor electronice, reticența față de instrumentele electronice, un impediment deseori invocat îl reprezintă cheltuielile aferente obținerii și utilizării certificatului cheii publice. În cele mai dese cazuri, costul de obținere și utilizare a certificatului cheii publice împiedică utilizatorii ocazionali, în special persoanele fizice, să meargă la ghișeu pentru a o obține.

Un factor important care contribuie la creșterea acestui cost este necesitatea deținerii unui dispozitiv fizic care stochează în siguranță cheia privată utilizată pentru a crea semnătura electronică avansată calificată. Există mai multe tipuri de dispozitive de creare a semnăturii electronice, cum ar fi o cartelă SIM, dispozitiv USB specializat sau cartelă criptografică. Toate acestea încorporează un cip criptografic specializat care garantează prin construcția sa secretul cheii private a deținătorului. Utilizarea dispozitivelor fizice specializate de către utilizatori presupune costuri de achiziție și probleme logistice

legate de depozitarea, transportul și distribuția acestora, în special deoarece acestea sunt realizate într-un mod reglementat. Dispozitivele fizice au, de asemenea, proprietatea de a fi pierdute, uzate sau distruse fizic prin neglijență. Utilizarea dispozitivelor fizice implică, de asemenea, o dependență de capacitățile de stocare și algoritmice ale cipului criptografic utilizat. Necesitatea unor modificări ale capacității de stocare sau a algoritmilor implementați de producătorul dispozitivului poate duce la necesitatea de a schimba dispozitivul fizic.

Cercetarea criptografică modernă, omniprezența telefoanelor mobile și practica internațională au arătat că există alternative la fel de sigure pentru păstrarea cheii private care nu necesită dispozitive fizice specializate. O soluție alternativă viabilă, accesibilă și sigură este de a împărți cheia privată în două componente și de a le păstra la ambii participanți în proces: o parte în telefonul mobil sub controlul exclusiv al titularului și o a doua parte la prestatorul de servicii de încredere. Acest lucru asigură imposibilitatea compromiterii cheii private prin compromiterea telefonului mobil în mod individual, dar garantează, de asemenea, controlul deplin al deținătorului asupra procesului de creare a semnăturilor electronice. Cu alte cuvinte, semnătura poate fi creată numai cu participarea ambelor părți la proces, titularul având control asupra procesului, în timp ce prestatorul poate asigura securitatea acestuia, inclusiv prin blocarea utilizării cheii private atunci când PIN-ul este introdus incorect și în mod repetat.

O soluție de identificare mobilă bazată pe infrastructura cheilor publice (PKI) oferă același nivel de securitate ca și soluțiile bazate pe dispozitive specializate cu cip. Cu toate acestea, există mai multe avantaje semnificative. De exemplu, nu este nevoie de cititoare de carduri și software-ul corespunzător. Soluțiile mobile sunt, de asemenea, mai ușor și mai convenabil de utilizat, inclusiv din afara teritoriului Republicii Moldova.

În acest sens, se propune instituirea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), care va oferi un grad similar de securitate a cheilor private în comparație cu soluțiile existente bazate pe dispozitive sau pe medii criptografice, dar fără a fi necesară utilizarea acestora. Soluția respectivă se bazează pe algoritmi criptografici avansați, iar securitatea unei implementări similare, în unele state din Uniunea Europeană a fost certificată ca avansată calificată și în conformitate cu Regulamentul european privind identificarea electronică și serviciile de încredere (eIDAS). Soluția implementează algoritmi criptografici în software pe partea utilizatorului, care permit evoluția rapidă a algoritmilor prin actualizări periodice, dacă este necesar.

Prin eliminarea necesității dispozitivelor criptografice specializate, inclusiv a costurilor logistice asociate acestora, soluția permite implementarea unui model distribuit de identificare și înregistrare a utilizatorilor. În acest model, operatorii prestatorilor serviciilor de înregistrare desemnați, fiind autentificați într-un modul dedicat înregistrării și asistenței utilizatorilor soluției, pot verifica datele personale ale unui utilizator și pot confirma identitatea acestuia pentru a efectua procesul de certificare a cheii publice. Operatorii pot opera în cadrul mai multor organizații care ar acoperi din punct de vedere teritorial, atât cererile de pe teritoriul Republicii Moldova (spre exemplu Centrele multifuncționale ale Instituției publice „Agenția Servicii Publice”), cât și din diaspora (misiunile diplomatice și oficiile consulare).

Soluția nu exclude, de asemenea, posibilitatea de a implementa 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. O astfel de posibilitate va fi evaluată ulterior la un nivel tehnic adecvat pentru a menține un grad ridicat de asigurare a identificării corecte a solicitantului și pentru a preveni o posibilă fraudă în acest proces.

Pentru utilizarea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) atât de pe teritoriul Republicii Moldova, cât și din străinătate, utilizatorul va avea nevoie de dispozitivul său inteligent (telefon sau tabletă) și conexiune la internet. Totodată, este de menționat că utilizarea serviciului MobiSign nu generează impedimente pentru utilizator de a utiliza pe același dispozitiv și serviciile de „semnătură mobilă” furnizate de companiile telefonie mobilă.

Pentru a spori accesibilitatea la serviciile electronice, disponibile atât în sectorul public, cât și în sectorul privat, pentru utilizarea aplicației mobile a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) se propune oferirea acesteia fără perceperea unor plăți de la persoane, total nelimitată și posibil de a fi descărcată pe dispozitivele inteligente moderne.

Prin intermediul acestui serviciu, va fi posibilă autentificarea în sisteme informaționale și semnarea electronică a documentelor electronice și de pe calculator. Pentru aceste activități, utilizatorul va utiliza dispozitivul mobil pe care este instalată aplicația mobilă corespunzătoare serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) și calculatorul.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul nu conține norme de armonizare a legislației naționale cu legislația Uniunii Europene.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul cuprinde reglementări care au ca obiectiv instituirea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), aprobarea Conceptului serviciului respectiv și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), desemnarea posesorului și obligației unor entități de a asigura verificarea identității persoanei și transmiterea cererii de certificare a cheii publice către Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”. Proiectul descrie drepturile și obligațiile subiecților serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), interacțiunea cu alte sisteme informaționale de stat etc.

5. Fundamentarea economico-financiară

Implementarea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign), se va realiza cu suportul financiar al Programului Națiunilor pentru Dezvoltare (PNUD) Moldova, costul estimat fiind de aproximativ 1,0 mln lei.

Administrarea și dezvoltarea continuă a serviciului MobiSign nu va necesita alocarea de resurse suplimentare din bugetul de stat și se va realiza din contul și limita alocațiilor bugetare planificate deja în bugetul Cancelariei de Stat pentru anul 2022 și incluse în CBTM 2022-2024 (aproximativ 8,7 mil. lei), pentru asigurarea întreținerii infrastructurii PKI a Guvernului.

Potențiali beneficiari ai serviciului MobiSign sunt toate persoanele fizice ce au atins vârsta de 18 ani - cetățeni ai Republicii Moldova sau cetățeni străini cărora le-a fost atribuit un numărul de identificare de stat al persoanei fizice (IDNP). Astfel, grupul țintă a utilizatorilor serviciului MobiSign este populația adultă, aflată în țară și peste hotare, și care conform datelor statistice ar depăși cifra de 2 mln. de persoane.

Având în vedere rata de adopție redusă în rândul populației (sub 10% din populația adultă) a soluțiilor de semnătură electronică disponibile și ținând cont că identitatea electronică este un element esențial al oricărui ecosistem de e-guvernare, conform pct. 8 din proiectul hotărârii este propus ca serviciile aferente procesului de certificare a cheii publice, precum și serviciile de creare și verificare a semnăturii electronice prin intermediul serviciului MobiSign să fie furnizate fără perceperea unor plăți.

Serviciul MobiSign pe lângă faptul că simplifică obținerea și utilizarea semnăturii electronice are menirea de a simplifica și procesul de stabilire a identității persoanei (solicitant a semnăturii electronice), și de depunere a cererii de certificare a cheii publice. Având în vedere că efortul operațional pentru activitățile respective este unul relativ redus și de regulă va fi conex altor servicii prestate de către prestatorii de servicii ce vor avea calitatea de prestatori de servicii de înregistrare nu se impune necesitatea planificării unor cheltuieli în acest sens. Este de menționat că o rată ridicată de adopție a identității electronice în rândul cetățenilor Republicii Moldova va contribui la creșterea numărului de utilizatori de servicii publice electronice, inclusiv ce apelează la instrumente de autoservire electronică, ceea ce cu siguranță va asigura reducerea rândurilor la prestatorii de servicii publice, diminuând astfel presiunea pe front-office-ul acestora.

La dezvoltarea serviciului guvernamental de identitate și semnătură electronică mobilă (MobiSign) se va ține cont de arhitectura tehnologică existentă și economiile ce pot fi generate prin reutilizarea infrastructurii conexă serviciilor de certificare din posesia Instituției publice „Serviciul Tehnologia

Informației și Securitate Cibernetică”, găzduirea soluției pe platforma tehnologică guvernamentală comună (MCloud) și integrarea acesteia cu sistemele informaționale partajate relevante - MPass, MSign, MLog, etc.).

6. Modul de încorporare a actului în cadrul normativ în vigoare

Proiectul de hotărâre a Guvernului se integrează organic în cadrul normativ în vigoare și se întemeiază pe competențele Guvernului stabilite în art.22 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

7. Avizarea și consultarea publică a proiectului

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, pe pagina web oficială a Cancelariei de Stat (www.cancelaria.gov.md), secțiunea – Transparența decizională a fost asigurată plasarea:

anunțului privind inițiativa de elaborare a proiectului, precum și proiectului, împreună cu Nota informativă.

Proiectul este înregistrat de către Cancelaria de Stat cu numărul unic 141/CS/AGE/2022 și este supus avizării de către toate autoritățile și instituțiile a căror avizare este necesară.

8. Constatările expertizei de compatibilitate

Proiectul nu este elaborat în scopul armonizării legislației naționale cu legislația UE, exceptându-se astfel de la efectuarea expertizei de compatibilitate.

9. Constatările expertizei juridice

Proiectul este supus expertizei juridice (*avizele Ministerului Justiției nr. 04/2441 din 16.03.2022 și Aviz nr. 04/3347 din 11.04.2022*), obiecțiile și propunerile fiind luate în considerare la definitivarea acestuia.

10. Constatările expertizei anticorupție

Proiectul este supus expertizei anticorupție (*scrisoarea nr. 06/2-2185 din 13.04.2022*) și nu conține factori de risc care să genereze apariția riscurilor de corupție.

11. Constatările altor expertize

Proiectul nu cade sub incidența altor expertize necesare de a fi efectuate în condițiile Legii nr.100/2017 cu privire la actele normative, dat fiind faptul că nu reglementează activitatea de întreprinzător, nu conține reglementări cu impact asupra bugetului public național sau a unor componente din cadrul acestuia și nu prevede reorganizări și reforme structurale sau instituționale ale autorităților ori ale instituțiilor publice. Prin urmare, proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr.23/2019.

Viceprim-ministru pentru digitalizare

Iurie ȚURCANU