

Lege **privind cadrul național de interoperabilitate**

CAPITOLUL I

Art. 1

Prezenta lege stabilește drepturile și obligațiile operatorilor sistemelor informatice prin care se oferă servicii publice electronice în vederea accelerării tranziției către Societatea Informațională și Economia Bazată pe Cunoaștere.

Art. 2

În înțelesul prezentei legi, următorii termeni se definesc astfel:

- a) interoperabilitate – capacitatea sistemelor informatice de a comunica și schimba date într-un mod consistent și eficient;
- b) Sistem Unic Național de Autentificare (SUNA) – sistem informatic care permite autentificarea sigură a utilizatorilor serviciilor publice electronice;
- c) date de autentificare – pereche formată din nume de utilizator și parola sau, alternativ, un certificat digita;
- d) Depozitar Național de Documente (DND) – sistem informatic care permite stocarea securizată a documentelor persoanelor fizice și juridice.

Art. 3

Principiile avute în vedere sunt:

- e) creșterea eficienței și eficacității sistemelor informatice prin care se oferă servicii publice electronice;
- f) creșterea eficienței utilizării fondurilor publice;
- g) creșterea conformatului cetățeanului;
- h) creșterea securității sistemelor informatice ale administrației publice locale și centrale;
- i) reutilizarea resurselor implicate în cadrul sistemelor informatice;
- j) îmbunătățirea colaborării între instituțiile administrației publice;
- k) maturitate, suport în piață și popularitate;
- l) promovarea accesibilității web;
- m) facilitarea colaborării la nivel european și internațional.

Art. 4

(1) Pentru transpunerea în practică a cadrului de interoperabilitate propus se formează Grupul de Lucru pentru Interoperabilitate (GLI), format din reprezentanți ai:

- a) Ministerului Comunicațiilor și Societății Informaționale;
- b) Agenției pentru Serviciile Societății Informaționale;
- c) Institutului Național de Cercetare-Dezvoltare în Informatică;

(2) Grupul de lucru va funcționa sub coordonarea Ministerului Comunicațiilor și Societății Informaționale.

CAPITOLUL II Sistemul Unic Național de Autentificare (SUNA)

Art. 5

În termen de 90 de zile de la data intrării în vigoare a prezentei legi, Ministerul Comunicațiilor și Societății Informaționale va asigura implementarea și operaționalizarea SUNA.

Art. 6

SUNA va permite autentificarea certă și sigură a utilizatorilor pe baza datelor de autentificare ale acestora.

Art. 7

Orice persoană fizică sau juridică va putea solicita prin mijloace electronice eliberarea datelor de autentificare.

Art. 8

Datele de autentificare vor fi transmise solicitantului după verificarea identității acestuia pe baza documentelor de identitate.

Art. 9

Datele de autentificare vor putea fi transmise direct solicitantului sau prin poșta recomandată cu confirmare de primire.

Art. 10

Titularul datelor de autentificare are obligația de a solicita revocarea acestora în cazul în care:

- a) a pierdut datele de autentificare;
- b) are motive să creadă că datele de autentificare au ajuns la cunoștința unui terț neautorizat.

Art. 11

Titularul are obligația să protejeze datele de autentificare proprii și să le prezinte exclusiv SUNA, prin interfața web securizată.

Art. 12

Operatorii sistemelor informatice prin care se oferă servicii publice electronice au obligația ca, în termen de 90 de zile de la data intrării în vigoare a prezentei legi, să asigure interconectarea sistemelor informatice cu SUNA, asigurând acces imediat și nediscriminatoriu tuturor utilizatorilor, pe baza datelor de autentificare, în urma validării realizate prin SUNA.

Art. 13

Toate sistemele informatice prin care se oferă servicii publice electronice, operaționalizate ulterior datei intrării în vigoare a prezentei legi, vor asigura componenta de autentificare exclusiv prin interconectarea cu SUNA.

CAPITOLUL III Depozitarul Național de Documente (DND)**Art. 14**

În termen de 90 de zile de la data intrării în vigoare a prezentei legi, Ministerul Comunicațiilor și Societății Informaționale va asigura implementarea și operaționalizarea DND.

Art. 15

Orice persoană înregistrată în SUNA va beneficia de un spațiu de stocare securizat, în care va putea păstra documente proprii, în format electronic.

Art. 16

Accesul la documentele stocate în DND se va face după autentificarea în SUNA.

Art. 17

Operatorii sistemelor informatice prin care se oferă servicii publice electronice care implică comunicarea de informații către contribuabil au obligația ca, în termen de 90 de zile de la data intrării în vigoare a prezentei legi, să asigure interconectarea sistemelor informatice cu DND, asigurând transmiterea informațiilor în format electronic, semnate în condițiile Legii 455/2001, în spațiul rezervat solicitantului.

Art. 18

Operatorii sistemelor informatice prin care se oferă servicii publice electronice au obligația ca, în termen de 90 de zile de la data intrării în vigoare a prezentei legi să informeze MCSI cu privire la sistemele operate. Această informare se va face în baza unui formular ce va fi stabilit în normele tehnice și metodologice de aplicare a prezentei legi.

CAPITOLUL IV Cadrul tehnic de interoperabilitate

Art. 19

MCSI va asigura, în cadrul Sistemului Electronic Național, toate informațiile și mecanismele pentru identificarea și accesarea eficientă a tuturor serviciilor publice electronice disponibile la nivel național.

Art. 20

(1) GLI va elabora normele tehnice și metodologice privind cadrul național de interoperabilitate prin care se vor asigura:

- a) utilizarea serviciilor publice electronice direct din interfața proprie a Sistemului Electronic Național;
- b) schimbul de informații dintre două sau mai multe sisteme informatice ale administrației publice prin intermediul unui nod central;
- c) accesarea, de către un sistem informatic a datelor și informațiilor stocate în registrele naționale unice;

(2) Normele tehnice și metodologice vor face referire la standardele internaționale relevante.

Art. 21

În termen de 90 de zile de la publicarea normelor tehnice și metodologice, operatorii sistemelor informatice prin care se oferă servicii publice electronice și instituțiile responsabile cu gestionarea registrelor naționale unice vor lua măsurile necesare pentru a asigura:

- a) acceptarea și procesarea solicitărilor transmise de cetățeni prin intermediul Sistemului Electronic Național;
- b) acceptarea și procesarea solicitărilor primite din partea unui alt sistem informatic prin care se oferă servicii publice electronice;
- c) transmiterea de solicitări către alte sisteme, în cazul în care poziția operatorilor acestora este necesară pentru soluționarea unei cereri primite din partea cetățenilor;
- d) preluarea automată a informațiilor deja existente în cadrul registrelor naționale unice în vederea eliminării introducerii repetate a datelor.

Art. 22

Nerespectarea prevederilor art. 19 se sancționează cu amendă contravențională de la 50.000 lei la 100.000 lei.

Art. 23

Constatarea și sancționarea contravențiilor prevăzute la art.22 se realizează de persoane desemnate din cadrul MCSI.

CAPITOLUL V Dispoziții finale

Art. 24

În termen de 60 de zile de la intrarea în vigoare a prezentei legi, MCSI va elabora normele tehnice și metodologice de aplicare care vor fi aprobate prin ordin emis de ministrul comunicațiilor și societății informaționale.

Art. 25

Prezenta lege intră în vigoare în termen de 3 de zile de la data publicării în Monitorul Oficial al României, Partea I.

Norme tehnice și metodologice privind Cadru Național de Interoperabilitate (CNI)

CNI cuprinde politicile și specificatiile de ordin tehnic pentru a atinge interoperabilitatea între sistemele informatice, produsele-program, aplicațiile sau serviciile accesibile prin Sistemul Electronic Național.

CNI stabilește condițiile minim necesare pentru facilitarea procesului de comunicare, securității, a schimbului de date și informații dintre: administrație și administrație la nivel național (G2G), administrație și cetățean (G2C, C2G), administrație și mediul privat (G2B, B2G), administrația română și alte administrații ale statelor membre sau instituții UE (G2UE, UE2G).

Principiile care stau la baza Cadrului Național de Interoperabilitate sunt:

1. **Relevanța și integralitate** – standardele și specificatiile care alcătuiesc CNI trebuie să fie relevante ariilor de interoperabilitate: Interconnection, Data Integration, Information Access, Security, and Metadata; acestea vor fi abordate într-un mod concentrat și coordonat.
2. **Maturitate, suport în piață și popularitate** – standardele și specificatiile care alcătuiesc CNI trebuie să fie recunoscute la nivel european sau de facto ca mature, larg răspândite în industria IT, să fie larg suportate de platformele tehnologice dominante la nivel european, pachetele software și aplicațiile private existente pe piața unică.
3. **Standarde deschise** - standardele și specificatiile care alcătuiesc CNI trebuie să fie deschise, pe cât este posibil. Standardele care sunt neutre din punct de vedere al producătorului sau al produsului vor fi favorizate față de alternativele proprietar.
4. **Promovarea accesibilității web** – standardele și specificatiile care alcătuiesc CNI trebuie să fie aliniate cu standardele de Internet larg acceptate (ex: W3C, IETF, OASIS etc), în vreme ce Internetul va fi canalul principal pentru furnizarea serviciilor și informațiilor prin mijloace electronice și pentru schimbul de date și informații.
5. **Reutilizarea politicilor, specificatiilor și standardelor deja existente în domeniul interoperabilității** – politicile, standardele și specificatiile care alcătuiesc CNI trebuie să fie în concordanță cu politicile, standardele și specificatiile deja existente, acolo unde este necesar, sau relevant.

Obiectivele urmărite prin elaborarea și implementarea Cadrului Național de Interoperabilitate sunt:

1. Asigurarea unor interfețe web standardizate și accesibile pentru furnizarea și pentru accesarea serviciilor și informațiilor publice electronice;
2. Standardizarea, adoptarea și promovarea utilizării XML ca standard actual pentru schimbul de date între serviciile publice electronice;
3. Standardizarea, adoptarea, utilizarea și rafinarea modelelor utilizate de structurare a datelor (metadata), după necesități, conform standardului ISO 15836:2009, sau altor standarde ISO sau internaționale, deschise sau publice (ex: ISO 20775:2009, ISO25577:2008 etc);
4. Alinierea la standardele și specificațiile tehnice utilizate în Internet, dezvoltate de organizații de specialitate acceptate și la nivel european (W3C, ISSS, OASIS, IETF etc); urmărirea alinierii sistemelor de furnizare a serviciilor publice electronice la aceste standarde sau specificații;
5. Adoptarea, sprijinirea și utilizarea standardelor “deschise” și a specificațiilor larg utilizate și sprijinite de către piața privată pentru a reduce costurile totale pentru întreținerea și dezvoltarea serviciilor publice electronice;
6. Promovarea beneficiilor ce reies din utilizarea tehnologiilor deschise;
7. Revizuirea politicilor, standardelor și specificațiilor implementate deja în sistemele existente de furnizare a serviciilor publice electronice, în vederea alinierii lor la cele existente nivel european, larg răspândite în industria IT și larg suportate de platformele tehnologice, pachetele software și aplicații, cele mai utilizate în sectorul public.

Din punct de vedere funcțional Cadrul Național de Interoperabilitate are în vedere următoarele:

1. Implementarea autentificării unice în cadrul sistemelor administrației publice;
2. Accesarea unificată a serviciilor publice electronice;
3. Definirea bazelor de date primare și a modului de interconectare a acestora;
4. Definirea mecanismelor de colaborare între sistemele administrației publice;
5. Interoperabilitatea cu sistemele similare la nivel european;
6. Definirea standardelor de securitate pentru sistemele administrației publice.

1. Implementarea autentificării unice în cadrul sistemelor administrației publice. O bariera semnificativă în dezvoltarea și utilizarea serviciilor publice electronice o reprezintă mecanismele de obținere/ transmitere a datelor de acces în cadrul sistemelor informatice. La nivel național, de-a lungul timpului, au fost implementate o serie de servicii publice electronice însă rata de creștere a numărului de utilizatori a fost scăzută. O cauză majoră o reprezintă faptul că un cetățean care dorește să acceseze un serviciu public electronic trebuie să obțină în prealabil credențialele de acces (nume utilizator+parola/ certificat digital) de la operatorul sistemului (de ex. primăria localității în care are domiciliu), înlocuindu-se astfel un drum la ghișeu (pentru obținerea unei autorizații) cu un alt drum la ghișeu (pentru obținerea parolei de acces).

În acest context se impune implementarea unui sistem integrat la nivel național pentru autentificarea în cadrul soluțiilor informatice ale administrației, astfel încât un cetățean să poată accesa un serviciu public electronic imediat ce acesta este oferit de administrație, în baza datelor de autentificare unice.

Implementarea va avea în vedere preluarea credențialelor utilizate în momentul de față de către un cetățean și înlocuirea cu un set unic de date de autentificare, totul realizându-se transparent pentru utilizator. Astfel, după implementarea sistemului de autentificare unică, administrația publică va avea obligația de a interconecta toate soluțiile proprii cu acest modul centralizat, realizându-se preluarea conturilor utilizator.

Sistemul de autentificare unică va include conectori către celelalte servicii publice electronice și orice soluție informatică nouă (prin care se va oferi un serviciu public) va putea exploata aceste extensii (conectori).

Propunerea ofera doua 3 avantaje majore:

- a. Un cetatean va avea acces imediat la orice serviciu public electronic, fara a fi nevoie sa-si faca cate un cont pentru fiecare aplicatie;
- b. Datele de acces vor fi securizate, nefiind vizibile la nivelul aplicatiei prin care se ofera serviciul public (modulul centralizat va "intoarce" aplicatiei profilul utilizatorului in urma autentificarii pe un canal securizat);
- c. Economii in dezvoltarea sistemelor (prin reutilizarea componentei de autentificare).

2. Accesarea unificata a serviciilor publice electronice. In momentul de fata un cetatean care doreste sa accesez un anumit serviciu public electronic trebuie sa stie cu precizie ce pagini web sa acceseze si unde (in cuprinsul paginii web) se regaseste "punctul de intrare" catre serviciul public cautat. In conditiile in care exista deja o aplicatie care gestioneaza solicitarile cetatenilor se justifica consolidarea unui punct central de acces catre toate acestea. Astfel, pe baza interfetelor Sistemului Electronic National orice sistem informatic prin care se ofera servicii publice electronice va putea sa-si expune formularele standardizate. Mai mult, Sistemul Electronic National va facilita accesul la aceste servicii indrumand cetateanul catre formularul cautat (devenind un fel de "ghid" in lumea virtuala). Toate administratiile publice vor avea obligatia conectarii sistemelor existente si a migrarii formularelor in Sistemul Electronic National.

Din punct de vedere tehnic, integrarea se realizeaza pe baza unor scheme XML publice iar efortul de migrare este redus comparativ cu dezvoltarea aplicatiei propriu-zise. Pricipalele avantaje ale acestei abordari sunt:

- a. Facilitarea simplificarii proceselor administrative prin identificarea caracteristicilor comune si standardizarea acestora;
- b. Utilizarea formularelor standardizate la nivel national / comunitar (unde este posibil);
- c. Cresterea numarului de utilizatori prin consolidarea Punctului Central de Acces la Servicii Publice Electronice.

3. Definirea bazelor de date primare si a modului de interconectare a acestora.

Dezvoltarea "insulara" (neconectata) a serviciilor publice electronice a condus la situatia in care fiecare sistem informatic gestioneaza propria baza de date, de cele mai multe ori neactualizata si continand date pe care nu le genereaza institutia care opereaza aplicatia. Astfel, baze de date similare (cum ar fi identitatea persoanelor fizice sau juridice) nu ofera aceleasi informatii iar evolutia este intens divergenta. Se impune definirea unui set canonic de baze de date, impreuna cu responsabilitatile aferente (institutiile responsabile cu gestionarea si actualizarea informatiei) si mijlocele de acces

electronic la acestea. Aceste baze de date vor fi interconectate, modificarile efectuate (de institutia responsabila) la nivelul uneia dintre acestea propagandu-se eficient la nivel national. Principalele avantaje ale acestei masuri sunt:

- a. asigurarea consistentei si veridicitatii informatiei tranzactionate;
- b. posibilitatea implementarii eficiente a instrumentelor de gestionare a informatiilor persoanelor fizice si juridice de-a lungul intregului ciclu de viata;
- c. nivel crescut de securitate;
- d. scaderea costurilor implementarii sistemelor informatice noi, bazele de date fiind mai putin aglomerate.

4. Definirea mecanismelor de colaborare intre sistemele administratiei publice.

Aceiasi dezvoltarea "insulara" (neconectata) a serviciilor publice electronice enuntata mai sus a condus la situatia in care un sistem informatic raspunde la un singur tip de cerere din partea cetatenilor. Astfel, in situatia in care un cetatean solicita o autorizatie care implica avize de la doua sau mai multe institutii trebuie sa adreseze punctual solicitarea tuturor entitatilor implicate. Solutia propusa presupune implementarea si operationalizarea unei "mase turnante" care sa canalizeze automat solicitarea clientului catre toate institutiile implicate. Acest mecanism va fi implementat in cadrul ASSI si in prima faza va gestiona solicitarile precizate in Directiva privind Serviciile. Principalele avantaje sunt:

- a. capitalizarea sinergiilor inerente prin interconectarea fluxurilor de avizare din cadrul institutiilor responsabile;
- b. orientarea administratiei catre cetatean, acesta netrebuind sa cunosca in detaliu mecanismele administratiei (acestea se vor regasi in cadrul Registrului National al Responsabilitatilor, creat si operat de ASSI); concret, intreg circuitul de avizare devine transparent pentru utilizator.

5. Interoperabilitatea cu sistemele similare la nivel european.

Interoperabilitatea solutiilor informatice prin care se ofera servicii publice in context european este o tema intens dezbatuta la nivelul uniunii, dovada numarul mare de proiecte in acest domeniu. In acest context vor fi dezvoltate toate componentele enumerate anterior: autentificarea (incluzand un modul dedicat interoperabilitatii PKI) si lucrul colaborativ intre institutii cu atributii similare in diferite tari.

6. Definirea standardelor de securitate pentru sistemele administratiei publice.

Deoarece sistemele administratiei publice gestioneaza date cu caracter personal, se impune definirea unor standarde precise, pe tipuri de sisteme, de-a lungul dimensiunilor

precizate anterior. Astfel, din punct de vedere al autentificarii solutiile posibile includ utilizarea perechii (nume utilizator + parola) sau certificat digital, in timp ce solutia propriu zisa trebuie sa includa o componenta de securitate importanta (pentru fiecare tip de sistem, in functie de tipul de date gestionate si tranzactionate, se vor elabora norme tehnice si metodologice cu privire la nivelul de securitate al sistemul si al aplicatiei).

Cadrul de implementare

Pentru transpunerea în practică a Cadrului de Interoperabilitate propus se formează Grupul de Lucru pentru Interoperabilitate, format din reprezentanți ai:

- Ministerului Comunicațiilor și Societății Informaționale;
- Agenției pentru Serviciile Societății Informaționale;
- Ministerului Administrației și Internelor;
- Ministerului Finanțelor Publice;
- Ministerului Justiției și Libertăților Cetățenești.

Grupul de lucru va funcționa sub coordonarea MCSI.

Acțiuni, responsabilități și termene

Acțiune	Responsabil	Termen
Implementarea sistemului de autentificare unică și a depozitarului de documente	ASSI APL/APC	2009
Migrarea serviciilor publice electronice la nivelul Punctului Central de Acces	ASSI APL/APC	2010
Implementarea bazelor de date unice	MCSI, ASSI, MJLC, MFP, MAI	2010
Implementarea Punctului de Contact Unic electronic	ASSI	2009
Extinderea Punctului de Contact Unic electronic către toate serviciile publice	MCSI, ASSI, MAI, MFP, MJLC	2011
Asigurarea interoperabilității la nivel european	MCSI, ASSI	2010
Implementarea standardelor de securitate la nivelul sistemelor informatice ale APL/APLC	MCSI, ASSI, MAI, APL, APC	2010