

**DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE
DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ**

**FURNIZAREA UNEI SEMNĂTURI
ELECTRONICE AVANSATE SAU A
UNEI SEMNĂTURI ELECTRONICE
CALIFICATE DE CĂTRE O
INSTITUȚIE SAU AUTORITATE
PUBLICĂ CETĂȚENILOR**

material documentar

aprilie 2025

Materialele elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.
Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă.
Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:
<https://www.cdep.ro/pls/dic/site2015.page?den=dsdl-home1>

Documentare și sinteză: Andra Andronic, consilier parlamentar.
Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

DEFINIREA CONCEPTELOR UTILIZATE

Potrivit articolului 3, punctul 11 al [Regulamentului nr.910/2014](#) al Parlamentului European și Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, **semnătura electronică avansată** reprezintă acea semnătură electronică care îndeplinește cerințele prevăzute la **articolul 26**.

Semnătura electronică calificată înseamnă a semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificate și care se bazează pe un certificat calificat pentru semnăturile electronice (articolul 3, punctul 12).

Certificatul calificat pentru semnătura electronică înseamnă un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa I a Regulamentului (articolul 3, punctul 15).

Serviciul de încredere¹ este definit conform punctului 16 al articolului 3 ca însemnând un serviciu electronic prestat în mod obișnuit **în schimbul unei remunerații**, care constă în:

- (a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective; sau
- (b) crearea, verificarea și validarea certificatelor pentru autentificarea unui site internet; sau
- (c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective.

Articolului 25 al Regulamentului 910/2014 reglementează **efectele juridice ale semnăturilor electronice**:

- (1) Unei semnături electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnăturile electronice calificate.

¹ Precizăm că în [Regulamentul 2024/1183](#) de modificare a Regulamentului (UE) nr.910/2014 în ceea ce privește instituirea cadrului European pentru identitatea digitală, articolul 16 este înlocuit, introducându-se o definiție mai detaliată a atribuțiilor serviciului de încredere.

(2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.

(3) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru este recunoscută drept semnătură electronică calificată în toate celelalte state membre².

Articolul 26³ definește **cerințele** pe care trebuie să le îndeplinească **semnăturile electronice avansate** și anume:

(a) face trimitere exclusiv la semnatar;

(b) permite identificarea semnatarului;

(c) este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său; și

(d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.

Potrivit **articolului 27**, punctul (1), în cazul în care un stat membru solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște semnăturile electronice avansate, semnăturile electronice avansate bazate pe un certificat calificat pentru semnături electronice și semnăturile electronice calificate care întrebunțează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

² Potrivit Regulamentului 2024/1183 de modificare a Regulamentului (UE) nr.910/2014 în ceea ce privește instituirea cadrului European pentru identitatea digitală, la articolul 25, alineatul (3) se abrogă.

³ Regulamentul 2024/1183 modifică articolul 26 în sensul că unicul paragraf devine alineatul (1) și adaugă alineatul (2), care prevede: "Până la 21 mai 2026, Comisia evaluează dacă este necesar să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru semnăturile electronice avansate. Pe baza rezultatului evaluării respective, Comisia poate adopta astfel de acte de punere în aplicare. În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele referitoare la semnăturile electronice avansate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2)".

Statele membre nu solicită o semnătură electronică la un nivel de securitate mai ridicat decât cel al semnăturii electronice calificate pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public (articolul 27, punctul (3)).

EXPLICAȚII TEHNICE

Potrivit [Ghidului de bune practici și aspecte legale privind utilizarea semnăturii electronice în organizații](#) elaborat de certSIGN (2020), **semnătura electronică avansată**, spre deosebire de semnătura electronică, reprezintă un concept care este strâns legat de gradul de încredere pe care cineva se presupune că ar trebui să îl aibă în el. Astfel, semnătura electronică avansată nu se referă la o tehnologie specifică, putându-se realiza prin diferite tehnologii (soluții tehnice și procedurale), cu condiția ca acestea să asigure îndeplinirea celor 4 cerințe din definiția semnăturii electronice avansate.

Practic, un document semnat cu o semnătură electronică avansată, în cazul în care se dovedește că într-adevăr este avansată, adică îndeplinește cele 4 condiții de mai sus, exprimă „cu un nivel ridicat de încredere” actul de voință al semnatarului.

Provocarea constă însă în a demonstra îndeplinirea celor 4 cerințe aferente articolului 26, iar acest lucru este posibil doar în măsura în care tehnologia utilizată (soluția tehnică și procedurile aferente) este echivalentă tehnologiei pentru semnătura calificată descrisă în Regulamentul 910/2014.

Semnătura electronică calificată, spre deosebire de conceptul de semnătură electronică avansată, este o semnătură electronică în care se specifică tehnologia (soluția tehnică și procedurală) utilizată pentru a fi creată, respectiv un dispozitiv de creare a semnăturilor electronice calificat și un certificat calificat pentru semnăturile electronice, care sunt definite în detaliu, potrivit definițiilor prezentate mai sus, la care se adaugă o serie considerabilă de cerințe precizate în Regulamentul 910/2014 și mai departe în actele de punere în aplicare a Regulamentului.

Această tehnologie cu care este creată semnătura calificată este atât de detaliată și bine reglementată, încât semnătura calificată este de fapt o semnătură avansată FOARTE UȘOR DE DEMONSTRAT/CERTĂ.

Semnătura calificată este UNICUL tip de semnătură avansată pentru care Regulamentul 910/2014 precizează în mod complet tehnologia (soluția tehnică și procedurală) utilizată pentru crearea ei.

Una dintre concluziile importante este că teoretic, pot exista o multitudine de tehnologii (soluții tehnice și procedurale) de creare a unei semnături electronice, respectiv a unei semnături electronice avansate.

În mod evident, din motive de costuri și de ușurință și pentru interoperabilitate în implementarea proceselor de digitalizare în organizație și între organizații, organizațiile vor trebui să decidă să se limiteze la cât mai puține astfel de tehnologii pentru crearea și respectiv acceptarea semnăturilor electronice.

Decizia stabilirii tehnologiei utilizate de către o organizație se poate lua prin raportare la cerințele art. 27 din Regulamentul 910/2014, care face referire la semnăturile electronice în cadrul serviciilor publice, dar conținutul articolului poate fi utilizat și de către o organizație privată.

Conform Regulamentului 910/2014, **semnătura electronică calificată este singura menționată de Regulament ca având efectul juridic al unei semnături olografe**. Acest lucru se datorează faptului că semnătura calificată este UNICUL tip de semnătură avansată pentru care Regulamentul 910/2014 precizează în mod complet tehnologia (soluția tehnică și procedurală) utilizată pentru crearea ei. Conform Regulamentului 910/2014, nici unei semnături electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnăturile electronice calificate.

SITUAȚIA DIN ROMÂNIA

[Legea nr.214/2014](#) stabilește cadrul juridic intern de aplicare directă a Regulamentului (UE) nr.910/2014 și de preluare în ordine juridică internă a măsurilor lăsate la latitudinea statelor membre, prin clarificarea anumitor aspecte ale sigiliului electronic, a mărcii temporale și a documentelor electronice cărora li s-a aplicat o semnătură electronică, o marcă temporală sau un sigiliu electronic.

Articolul 3 reglementează regimul juridic al semnăturilor electronice, după cum urmează:

(1) Toate tipurile de semnătură electronică prevăzute în Regulamentul (UE) nr. 910/2014 sau în prezenta lege produc efecte juridice și pot fi utilizate ca mijloace de probă în fața instanțelor de judecată.

(2) Actul juridic în format electronic, semnat cu tipul de semnătură electronică prevăzut de lege sau cu semnătura electronică calificată, produce aceleași efecte juridice ca același act juridic în format letric.

(3) Valabilitatea semnăturii electronice se verifică în raport cu condițiile pe care trebuie să le îndeplinească la momentul semnării documentului electronic, iar expirarea valabilității certificatului în baza căruia a fost aplicată semnătura nu afectează valabilitatea sau efectele documentului semnat. Prevederile prezentului alineat sunt valabile și în cazul semnăturilor electronice avansate care nu se bazează pe un certificat pentru semnătură electronică, ci folosesc alte tehnologii.

(4) Perioada maximă de valabilitate a certificatului pentru semnătura electronică avansată se stabilește de emitentul certificatului pentru o perioadă de maximum 2 ani. Autoritatea de supraveghere și reglementare în domeniu este responsabilă pentru stabilirea perioadelor de valabilitate în cazul semnăturilor electronice avansate care nu se bazează pe un certificat pentru semnătură electronică, ci folosesc alte tehnologii.

(5) Prin excepție de la alin. (4), certificatul pentru semnătură electronică avansată emis conform legii de către Ministerul Afacerilor Interne și înscris pe cartea electronică de identitate este valabil pentru o perioadă de maximum 5 ani.

(6) Înscrierile în formă electronică, reglementate potrivit art. 267 din Legea nr. 134/2010 privind Codul de procedură civilă, republicată, cu modificările și completările ulterioare, sunt asimilate documentelor electronice, astfel cum acestea sunt definite de Regulamentul (UE) nr. 910/2014.

Potrivit articolului 4, para. (1), documentul electronic semnat cu o semnătură electronică calificată este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătură privată, în condițiile art. 25 alin. (2) din Regulamentul (UE) nr. 910/2014. Semnătura electronică calificată produce aceleași efecte juridice ca semnătura olografă.

În cazul în care, potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată care, în condițiile prezentei legi, produce aceleași efecte precum semnătura olografă (articolul 4, para. (3)).

Articolul 16 stabilește la para. (3), lit (a), că **verificarea identității unei persoane în vederea eliberării unui certificat calificat, respectiv a unui certificat pentru semnătură electronică avansată se poate face (...) de către prestatorul de servicii de încredere, pe baza actului de identitate, a pașaportului sau a permisului de ședere** emis de autoritățile competente, în original, al solicitantului și prin prezența fizică a solicitantului în fața unui reprezentant al prestatorului de servicii de încredere calificate, care trebuie să aibă un contract cu respectivul prestator de servicii de încredere și să fie desemnat și pregătit de acesta să efectueze activități de identificare a persoanei. **Litera (b) stabilește verificarea identității unei persoane pe baza unui certificat calificat pentru semnătură electronică sau pentru sigiliu electronic calificat, valid la momentul identificării, emis de un prestator de servicii de încredere calificate.** Articolul 16 prevede și alte mijloace de identificare valabile.

Articolul 24 reglementează utilizarea semnăturii electronice de către autoritățile și instituțiile publice. La para. (1) se stabilește că actele emise în format electronic de autoritățile și instituțiile publice sunt semnate cu o semnătură electronică calificată sau cu o semnătură electronică avansată creată cu un certificat digital emis de o autoritate sau o instituție publică din România.

Paragraful (4) reglementează că Serviciul de Telecomunicații Speciale, în calitate de prestator de servicii de încredere calificate acreditat conform Regulamentului (UE) nr. 910/2014, furnizează servicii de încredere calificate, cu titlu **gratuit**, în scopul îndeplinirii atribuțiilor funcționale, exclusiv personalului autorizat din cadrul autorităților și instituțiilor publice beneficiare, în conformitate cu prevederile Legii nr. 92/1996 privind organizarea și funcționarea Serviciului de Telecomunicații Speciale, cu modificările și completările ulterioare.

Totodată, instituțiile din domeniul securității naționale furnizează servicii de încredere calificate pentru sistemele electronice închise gestionate de acestea, iar certificatele calificate sau certificatele pentru semnătură avansată emise de aceste organe sunt recunoscute și

folosite pentru nevoi proprii și un set definit de participanți în baza acordurilor încheiate, pentru realizarea schimbului de date intern, sau între acestea și instituțiile din domeniul apărării, ordinii publice și securității naționale, precum și pentru semnarea corespondenței digitale și realizarea schimbului de corespondență digitală (para. (5)).

De asemenea, precizăm că odată cu data cu intrarea în vigoare la data de 06.05.2021 a [Ordonanței de Urgență nr.36/2021](#), este permisă semnarea electronică a tuturor documentelor din sfera relațiilor de muncă.

Potrivit actului normativ, angajatorul și salariatul pot opta să folosească, la încheierea contractului individual de muncă, a actelor adiționale la acesta, la întocmirea tuturor înscrisurilor/documentelor din domeniul relațiilor de muncă rezultate la încheierea contractului individual de muncă, pe parcursul executării acestuia sau la încetarea contractului individual de muncă, semnătura electronică avansată sau semnătura electronică calificată, însoțită de marca temporală electronică sau marca temporală electronică calificată și sigiliul electronic calificat al angajatorului în condițiile stabilite prin regulamentul intern și/sau contractul colectiv de muncă aplicabil.

O precizare importantă este că, pentru orice document pentru care Codul muncii stabilește că forma scrisă este obligatorie, se consideră cerința îndeplinită dacă documentul este întocmit în formă electronică semnat cu semnătură electronică avansată sau calificată. Aceste documente se arhivează de către angajator cu respectarea prevederilor Legii Arhivelor Naționale nr.16/1996.

Totodată, angajatorul poate utiliza semnătura electronică avansată sau calificată la întocmirea documentelor din domeniul relațiilor de muncă sau securității și sănătății în muncă în relația cu instituțiile publice.

Deși angajatorul poate suporta costurile aferente folosirii semnăturii electronice (vezi articolul IV, para. (2)), salariatul nu poate fi obligat să folosească semnătura electronică avansată sau calificată.

De subliniat, părțile trebuie să folosească același tip de semnătură (fie semnătura olografă, adică de mână, fie cea electronică avansată, fie cea electronică calificată) la toate documentele încheiate.

Menționăm că [Proiectul privind introducerea cărții electronice de identitate și a semnăturii digitale](#), prezentat pe site-ul Comisiei Europene, își propune sprijinirea tranziției și adoptarea cărții electronice de identitate (e-ID card) de către cetățenii români, investiția fiind considerată esențială pentru facilitarea interacțiunii digitale între entitățile publice/private și cetățeni.

Investiția constă în livrarea a 5 milioane de cărți electronice de identitate pe parcursul implementării planului național de redresare și reziliență.

Cartea electronică de identitate va stoca două certificate digitale:

i) unul care va face posibilă autentificarea pentru utilizarea serviciilor online ale administrației publice, utilizabil din momentul emiterii cărții electronice de identitate și

ii) **unul opțional pentru semnătura electronică calificată emisă de furnizori de servicii de certificare calificați, disponibil pentru a fi achiziționat de către cetățeni.**

Punerea în aplicare a investiției va fi finalizată până în 30 iunie 2026, componentele tehnice și de infrastructură necesare pentru emiterea cărții de identitate electronice fiind finalizate și operaționalizate.

EXEMPLE DE BUNE PRACTICI

În **Portugalia**, [semnătură digitală](#) are aceeași valabilitate juridică ca cea olografă, fiind compatibilă cu orice software care permite semnătura digitală. O semnătură digitală are asociate certificate digitale care garantează identitatea persoanei care semnează un document digital. În acest context, **statul portughez garantează certificarea semnăturilor digitale** realizate cu ajutorul unui card de identitate sau a unei chei mobile digitale (CMD).

Prin intermediul aplicației [Autenticação.gov](#) (pentru computere) sau aplicației mobile [gov.pt](#), cetățenii portughezi pot beneficia de următoarele servicii aferente cardurilor lor electronice de identitate:

- semnarea documentelor digitale cu [Cartão de Cidadão](#)⁴ (cardul de cetățean, reprezentând un document de identificare fizică care conține un cip/ card inteligent, cu ajutorul căruia deținătorul cardului poate fi identificat ca cetățean portughez în fața oricărei entități publice sau private, în persoană sau la distanță/ digital) sau [Chave Móvel Digital](#)⁵ (CMD - cheia mobilă digitală reprezentând un mijloc de autentificare și de obținere a semnăturii digitale certificate de statul portughez)
- personalizarea semnăturii digitale;
- vizualizarea adresei și schimbarea adresei înscrise în cardul de cetățean;
- modificarea codurilor PIN aferente cardului;
- verificarea valabilității certificatelor digitale aferente cardului de cetățean;
- includerea unor informații importante pentru utilizator, precum: contacte de utilizat în caz de urgență, grupa de sânge, alergii, etc;
- vizualizarea și imprimarea datelor personale aferente cardului.

Utilizarea semnăturii electronice avansate este asociată [documentelor digitale cu attribute profesionale](#).

În vederea utilizării semnăturii digitale avansate, profesioniștii calificați trebuie să procedeze la asocierea atributelor profesionale prin intermediul [Sistemului de certificare a atributelor profesionale](#) (SCAP). Atributele profesionale pot fi: de afaceri, ale liderilor politici, ale aleșilor locali, ale angajaților etc. Autentificarea, și în acest caz, se realizează prin intermediul cardului de cetățean și CMD-ului.

Trebuie să precizăm că în Portugalia, **statul nu oferă accesul complet gratuit la semnătura electronică calificată** pe baza Cartão de Cidadão. Astfel, pentru utilizarea certificatelor digitale puse la dispoziție de statul portughez cetățenilor, sunt necesari următorii pași:

⁴ Cardul de cetățean a înlocuit mai multe documente, reunind într-un singur document informațiile privind identificarea civilă, fiscală, privind securitatea socială și utilizarea Serviciului Național de Sănătate. De asemenea, cu ajutorul cardului de cetățean se poate și vota, eliminându-se astfel utilizarea cardului de alegător.

⁵ Cheia mobilă digitală se asociază unui număr de telefon mobil, unui document de identificare a unei persoane, respectiv cardului de cetățean sau a cărții de identitate; în cazul cetățenilor străini, cheia mobilă este asociată pașaportului sau permisului de ședere.

- activarea certificatelor digitale, incluse pe cip-ul cardului de cetățean/ cărții de identitate, acest proces fiind gratuit;
- **achiziționarea de către utilizator a unui cititor de carduri inteligent conectat la computer;**
- furnizarea, în regim de gratuitate de către statul portughez, a unui software middle-ware specific, care permite interacțiunea dintre card, cititor și aplicații.

În cazul CMD-ului, activarea este gratuită și se poate face online (pentru cei care dețin deja Cartão de Cidadão și certificate digitale activate), prin apel video sau direct la ghișeu.

În concluzie, deși statul portughez nu oferă un acces complet gratuit la semnătura digitală (referindu-ne aici la necesitatea achiziționării cititorului de carduri de către utilizatori), facilitează accesul la semnătura electronică calificată prin includerea certificatelor pe card-ul de cetățean, furnizează software-ul necesar precum și sistemul Chave Móvel Digital.

În cazul **Franței**, **semnătura electronică avansată** (nivelul 2) este cel mai des folosită de către companii/ întreprinderi⁶. Prin utilizarea unei chei private care este accesibilă numai persoanei care semnează, precum smartphone-ul, este posibilă: identificarea semnatarului, asocierea semnăturii cu autorul acesteia, garantarea integrității documentului semnat. În unele cazuri, semnatarului i se cere să încarce actul de identitate pe platforma furnizorului de semnătură electronică, care apoi poate efectua verificări și îl poate autentifica. Acest tip de semnătură este, de exemplu, utilizat pe scară largă pentru a semna o factură electronică (dematerializată), un contract de muncă, un contract de vânzare imobiliară sau un contract de asigurare de viață.

Semnătura electronică avansată bazată pe un certificat de semnătură electronică calificat (nivel 3) permite asigurarea identității semnatarului printr-un proces specific, bazându-se pe utilizarea unui certificat de semnătură electronică calificat care îndeplinește cerințele regulamentului eIDAS, emis de un furnizor de servicii de încredere. Pentru stabilirea acestui certificat, furnizorul de servicii trebuie să verifice identitatea semnatarului. Acest lucru se poate face, de exemplu, în timpul unei întâlniri fizice față în față cu un agent

⁶ <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>

calificat, cum ar fi un agent [La Poste](#), sau prin utilizarea unui serviciu certificat de verificare a identității la distanță.

Semnătura electronică calificată (nivelul 4) necesită următoarele formalități:

- achiziționarea unui certificat de semnătură electronică, la fel ca și pentru semnătura electronică avansată bazată pe un certificat de semnătură electronică calificată (nivel 3), astfel încât identitatea semnatarului să fie validată în prealabil (fizic sau la distanță, în funcție de anumite condiții), de o autoritate de certificare sau de un furnizor de servicii de emitere a unui certificat de semnătură electronică calificat (potrivit regulamentului eIDAS);
- un dispozitiv calificat de creare a semnăturii electronice; acest token (cheie USB, card inteligent, smartphone), certificat de [ANSSI](#) (Agenția Națională pentru Securitatea Sistemelor Informaționale) sau de o altă autoritate europeană de securitate și apărare a sistemelor informatice, este emis numai persoanelor fizice. Întreprinderile pot semna numai prin intermediul unui reprezentant, persoană fizică, autorizat în mod corespunzător.

Potrivit Codului Civil, doar semnătură electronică calificată reprezintă echivalentul unei semnături olografe.

Mai greu de pus în aplicare și mai costisitoare, semnăturile calificate sunt în general rezervate documentelor în care autentificarea este esențială, de exemplu în cazul actelor notariale (notari, executori judecătorești etc.).

Comisia Europeană furnizează o [listă a furnizorilor de servicii de încredere calificați](#) în conformitate cu Regulamentul eIDAS. Crearea unei semnături electronice avansate necesită mai întâi obținerea unui certificat de semnătură electronică.

Certificatele de semnătură electronică calificată în sensul Regulamentului nr. 910/2014 sunt emise de furnizori de servicii de certificare electronică calificați⁷.

ANSSI nu emite astfel de certificate, lista produselor și serviciilor calificate de ANSSI putând fi accesată [aici](#). Menționăm că certificatul de semnătură electronică califi-

⁷ <https://cyber.gouv.fr/obtenir-un-certificat-de-signature-electronique>

cat este legat de persoana fizică care îl utilizează și nu de o funcție. Același certificat poate fi, așadar, utilizat pentru semnarea mai multor documente în numele unor entități diferite, în contextul unor funcții diferite, atâta timp cât emitentul certificatului sau entitatea de care este atașat deținătorul nu a limitat utilizarea certificatului la un context anume (acest lucru va fi specificat, după caz, în condițiile generale de utilizare).

Ghișeul unic pentru facilitarea procedurilor întreprinderilor centralizează 56 de formulare administrative (Certas), existând astfel posibilitatea efectuării declarațiilor obligatorii online privind înregistrarea, modificarea administrativă, depunerea bilanțurilor anuale, încetarea activității. Spre exemplu, formularul pentru înființarea unei întreprinderi necesită o semnătură electronică simplă. Iar pentru formalitățile legate de depunerea bilanțului anual sau încetarea activității, este necesară o semnătură electronică calificată. Cea mai simplă soluție este utilizarea serviciului gratuit de autentificare [FranceConnect+](#) pentru conectarea la ghișeul unic.

FranceConnect facilitează autentificarea sigură a identității. Atunci când este utilizat în contextul semnării electronice, nivelul specific al semnăturii electronice (simplă, avansată sau calificată) va depinde de cerințele serviciului online și de nivelul de securitate necesar pentru tranzacția respectivă.

FranceConnect+ este conceput pentru a oferi un nivel de securitate mai ridicat, fiind adesea asociat cu semnăturile electronice avansate și calificate.

Menționăm că pentru a utiliza France Connect+, utilizatorii trebuie să aibă peste 15 ani, să fie înregistrați în Registrul național de identificare al persoanelor fizice (RNIPP) al INSEE și să aibă o identitate digitală din lista de identități disponibile pe France Connect+.

În concluzie:

Din informațiile disponibile, nu am identificat nicio țară europeană care să ofere în mod complet gratuit cetățenilor săi o semnătură electronică avansată.

Deși unele țări pot facilita accesul sau pot avea inițiative pentru a reduce costurile semnăturii electronice, obținerea unei semnături electronice avansate sau calificate implică de obicei costuri asociate cu:

- certificatul digital calificat, acesta fiind emis de furnizori de servicii de încredere acreditați contra cost.
- dispozitivul securizat de creare a semnăturii (QSCD), uneori fiind necesar un token USB sau un smart card, care poate fi achiziționat uneori contra cost;
- serviciile furnizorului de semnătură electronică; platformele care oferă servicii de semnare electronică oferă servicii remunerate, deși unele pot oferi perioade de încercare gratuite sau funcționalități limitate gratuite.

Regulamentul eIDAS al Uniunii Europene stabilește un cadru legal pentru semnăturile electronice, asigurând recunoașterea lor transfrontalieră, dar nu impune gratuitatea acestor servicii.

Unele țări pot implementa scheme sau programe specifice pentru anumite categorii de cetățeni sau în anumite contexte (de exemplu, pentru accesul la servicii guvernamentale online). Există furnizori de servicii de încredere care oferă soluții de semnare electronică, dar acestea sunt de obicei contra cost.

Deși utilizarea semnăturii electronice este încurajată în Europa pentru digitalizarea serviciilor, în prezent nu există o țară care oferă semnătura electronică avansată/ calificată în regim de gratuitate cetățenii săi.

Alte informații utile privind utilizarea semnăturii electronice (eSignature legality Guide) pot fi găsite [aici](#), în funcție de țara selectată.