REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1502 AL COMISIEI

din 8 septembrie 2015

de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 8 alineatul (3),

întrucât:

(1) Articolul 8 din Regulamentul (UE) nr. 910/2014 prevede că un sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) trebuie să specifice nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv.

(2) Stabilirea unor specificații, standarde și proceduri tehnice minime este esențială pentru a se asigura o înțelegere comună a detaliilor nivelurilor de asigurare a încrederii și interoperabilitatea în procesul de clasificare a nivelurilor naționale de asigurare aferente sistemelor de identificare electronică notificate în funcție de nivelurile de asigurare menționate la articolul 8, astfel cum se prevede la articolul 12 alineatul (4) litera (b) din Regulamentul (UE) nr. 910/2014.

(3) La elaborarea specificațiilor și a procedurilor prevăzute în prezentul act de punere în aplicare s-a ținut cont de standardul internațional ISO/IEC 29115, acesta fiind principalul standard internațional în materie de niveluri de asigurare ale mijloacelor de identificare electronică. Cu toate acestea, conținutul Regulamentului (UE) nr. 910/2014 diferă de standardul internațional menționat, în special în ceea ce privește cerințele în materie de dovedire și verificare a identității, precum și în ceea ce privește modul în care sunt luate în considerare diferențele dintre mecanismele referitoare la identitate din statele membre și instrumentele cu același scop existente în UE. Prin urmare, anexa, deși se bazează pe acest standard internațional, nu ar trebui să facă trimitere la niciun element concret din standardul ISO/IEC 29115.

(4) Prezentul regulament a fost elaborat sub forma unei abordări bazate pe rezultate, aceasta fiind considerată cea mai adecvată, ceea ce se reflectă și în definițiile utilizate pentru a explica termenii și conceptele. Acestea țin seama de obiectivul Regulamentului (UE) nr. 910/2014 în ceea ce privește nivelurile de asigurare ale mijloacelor de identificare electronică. Prin urmare, la stabilirea specificațiilor și a procedurilor prevăzute în prezentul act de punere în aplicare ar trebui să se țină seama cât mai mult posibil de proiectul-pilot pe scară largă STORK, incluzând specificațiile elaborate în cadrul acestuia, precum și de definițiile și de conceptele din standardul ISO/IEC 29115.

(5) În funcție de contextul în care trebuie să fie verificat un element de dovedire a identității, sursele sigure pot avea diverse forme, cum ar fi, printre altele, registrele, documentele și organismele. Sursele sigure pot diferi de la un stat membru la altul, chiar și în contexte similare.

(6) La elaborarea cerințelor în materie de dovedire și verificare a identității ar trebui să se țină seama de diferitele sisteme și practici, garantându-se, în același timp, un grad de asigurare suficient de ridicat încât să se formeze încrederea necesară. Prin urmare, acceptarea procedurilor utilizate anterior pentru un alt scop decât emiterea de mijloace de identificare electronică ar trebui să fie condiționată de confirmarea faptului că aceste proceduri îndeplinesc cerințele prevăzute pentru nivelul de asigurare corespunzător.

([1]) JO L 257, 28.8.2014, p. 73.

(7) De obicei sunt utilizați anumiți factori de autentificare, cum ar fi secretele partajate, dispozitivele fizice și caracteristicile fizice. Cu toate acestea, ar trebui să fie încurajată utilizarea unui număr mai mare de factori de autentificare, în special proveniți din categorii diferite, pentru a spori securitatea procesului de autentificare.

(8) Prezentul regulament nu ar trebui să afecteze drepturile de reprezentare ale persoanelor juridice. Cu toate acestea, anexa ar trebui să prevadă cerințe privind legăturile dintre mijloacele de identificare electronică ale persoanelor fizice și juridice.

(9) Ar trebui recunoscută importanța sistemelor de asigurare a securității informațiilor și a sistemelor de gestionare a serviciilor, la fel ca și importanța utilizării metodologiilor recunoscute și a aplicării principiilor incluse în seriile de standarde ISO/IEC 27000 și ISO/IEC 20000.

(10) Ar trebui, de asemenea, să fie luate în considerare bunele practici în ceea ce privește nivelurile de asigurare din statele membre.

(11) Certificarea de securitate informatică bazată pe standarde internaționale este un instrument important de verificare a conformității produselor cu cerințele în materie de securitate prevăzute în prezentul act de punere în aplicare.

(12) Comitetul menționat la articolul 48 din Regulamentul (UE) nr. 910/2014 nu a emis un aviz în termenul stabilit de președintele acestuia,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

(1) Nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică emise în cadrul unui sistem de identificare electronică notificat se stabilesc prin raportare la specificațiile și procedurile prevăzute în anexă.

(2) Specificațiile și procedurile prevăzute în anexă se utilizează pentru a preciza nivelul de asigurare al mijloacelor de identificare electronică emise în cadrul unui sistem de identificare electronică notificat, prin determinarea fiabilității și a calității următoarelor elemente:

(a) înscrierea, astfel cum se prevede în secțiunea 2.1 din anexa la prezentul regulament, în temeiul articolului 8 alineatul (3) litera (a) din Regulamentul (UE) nr. 910/2014;

(b) gestionarea mijloacelor de identificare electronică, astfel cum se prevede în secțiunea 2.2 din anexa la prezentul regulament, în temeiul articolului 8 alineatul (3) literele (b) și (f) din Regulamentul (UE) nr. 910/2014;

(c) autentificarea, astfel cum se prevede în secțiunea 2.3 din anexa la prezentul regulament, în temeiul articolului 8 alineatul (3) litera (c) din Regulamentul (UE) nr. 910/2014;

(d) gestionarea și organizarea, astfel cum se prevede în secțiunea 2.4 din anexa la prezentul regulament, în temeiul articolului 8 alineatul (3) literele (d) și (e) din Regulamentul (UE) nr. 910/2014.

(3) În cazul în care un mijloc de identificare electronică emis în cadrul unui sistem de identificare electronică notificat îndeplinește o cerință aferentă unui nivel de asigurare superior, se consideră că respectivul mijloc îndeplinește cerința echivalentă aferentă nivelului de asigurare inferior.

(4) Cu excepția cazului în care se prevede altfel în partea relevantă a anexei, pentru a corespunde nivelului de asigurare vizat trebuie îndeplinite toate elementele enumerate în anexă pentru un anumit nivel de asigurare a mijloacelor de identificare electronică emise în cadrul unui sistem de identificare electronică notificat.

Articolul 2

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 8 septembrie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

ANEXĂ

Specificațiile tehnice și procedurile pentru nivelurile de asigurare scăzut, substanțial și ridicat ale mijloacelor de identificare electronică emise în cadrul unui sistem de identificare electronică notificat

1. Definițiile aplicabile

În sensul prezentei anexe, se aplică următoarele definiții:

1. „sursă sigură" înseamnă orice sursă, indiferent de formă, în privința căreia se poate avea încredere că furnizează date, informații și/sau dovezi exacte care pot fi utilizate pentru dovedirea identității;

2. „factor de autentificare" înseamnă un factor în privința căruia s-a confirmat că are legătură cu o persoană și care se încadrează în una dintre următoarele categorii:

   (a) „factor de autentificare bazat pe posesie" înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze că se află în posesia acestuia;

   (b) „factor de autentificare bazat pe cunoștințe" înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze cunoașterea informației în cauză;

   (c) „factor de autentificare inerent" înseamnă un factor de autentificare care se bazează pe o caracteristică fizică a unei persoane fizice și în cazul căruia subiectul trebuie să demonstreze că prezintă respectiva caracteristică fizică;

3. „autentificare dinamică" înseamnă un proces electronic care utilizează criptografia sau alte tehnici pentru a oferi un mijloc de a crea, la cerere, o dovadă electronică a faptului că subiectul controlează datele de identificare sau se află în posesia acestora, dovadă care se modifică la fiecare autentificare a subiectului în sistemul care verifică identitatea subiectului;

4. „sistem de management al securității informațiilor" înseamnă un set de procese și proceduri menite să gestioneze la niveluri acceptabile riscurile legate de securitatea informațiilor.

2. Specificații și proceduri tehnice

Elementele specificațiilor și ale procedurilor tehnice prevăzute în prezenta anexă se utilizează pentru a determina modul în care se aplică cerințele și criteriile prevăzute la articolul 8 din Regulamentul (UE) nr. 910/2014 în cazul mijloacelor de identificare electronică emise în cadrul unui sistem de identificare electronică.

2.1. *Înscrierea*

2.1.1. Cererea și înregistrarea

Nivelul de asigurare	Elementele necesare
Scăzut	1. Asigurarea faptului că solicitantul este la curent cu termenii și condițiile legate de utilizarea mijloacelor de identificare electronică. 2. Asigurarea faptului că solicitantul are cunoștință de măsurile de prevedere recomandate în materie de securitate a mijloacelor de identificare electronică. 3. Colectarea datelor de identitate relevante necesare pentru dovedirea și verificarea identității.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.1.2. Dovedirea și verificarea identității (persoană fizică)

Nivelul de asigurare	Elementele necesare
Scăzut	1. Se poate presupune că persoana este în posesia unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică și care reprezintă identitatea pretinsă. 2. Se poate presupune că dovezile sunt autentice sau că ele există în conformitate cu o sursă sigură, iar dovezile par să fie valabile. 3. Se știe dintr-o sursă sigură că identitatea pretinsă există și se poate presupune că persoana care pretinde a avea identitatea respectivă corespunde acelei identități.
Substanțial	Trebuie să fie îndeplinite cerințele aferente nivelului scăzut, plus una dintre alternativele enumerate la punctele 1-4: 1. S-a verificat că persoana este în posesia unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică și care reprezintă identitatea pretinsă; și dovezile au fost verificate pentru a se stabili că sunt autentice sau se știe, în conformitate cu o sursă sigură, că ele există și că se referă la o persoană reală; și au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor dovezi pierdute, furate, suspendate, revocate sau expirate; sau 2. Un document de identitate este prezentat în cadrul unui proces de înregistrare în statul membru în care a fost eliberat documentul, iar acesta pare să se refere la persoana care îl prezintă; și au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor documente pierdute, furate, suspendate, revocate sau expirate; sau 3. În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare echivalentă cu cele prevăzute în secțiunea 2.1.2 pentru nivelul de asigurare substanțial, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului [1] sau de un organism echivalent; sau 4. În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare substanțial sau ridicat și luând în considerare riscurile unei modificări ale datelor de identificare personală în cauză, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare substanțial sau ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent.

Nivelul de asigurare	Elementele necesare
Ridicat	Trebuie să fie îndeplinite cerințele de la punctul 1 sau 2: 1. Trebuie să fie îndeplinite cerințele aferente nivelului substanțial, plus una dintre alternativele enumerate la literele a-c: (a) În cazul în care s-a verificat că persoana este în posesia unor dovezi de identificare fotografice sau biometrice recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică, iar elementele respective reprezintă identitatea pretinsă, atunci dovezile sunt verificate pentru a se stabili dacă sunt valabile în conformitate cu o sursă sigură; și prin intermediul unei comparații între una sau mai multe caracteristici fizice ale solicitantului și o sursă sigură se constată că persoana în cauză are identitatea pretinsă; sau (b) În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare echivalentă cu cele prevăzute în secțiunea 2.1.2 pentru nivelul de asigurare ridicat, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent; și se iau măsuri pentru a demonstra că rezultatele procedurilor anterioare rămân valabile; sau (c) În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare ridicat și luând în considerare riscurile unei modificări ale datelor de identificare ale persoanei în cauză, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent; și se iau măsuri pentru a demonstra că rezultatele acestei proceduri anterioare de emitere a unui mijloc de identificare electronică notificate rămân valabile. SAU 2. În cazul în care solicitantul nu prezintă dovezi de identificare fotografice sau biometrice recunoscute, se aplică exact procedurile folosite la nivel național în statul membru al entității responsabile de înregistrare pentru obținerea acestor dovezi de identificare fotografice sau biometrice recunoscute.

([1]) Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

2.1.3. Dovedirea și verificarea identității (persoană juridică)

Nivelul de asigurare	Elementele necesare
Scăzut	1. Identitatea pretinsă a persoanei juridice este demonstrată pe baza unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică.

Nivelul de asigurare	Elementele necesare
	2. Dovezile par să fie valabile și se poate presupune că sunt autentice sau că există în conformitate cu o sursă sigură, în cazul în care includerea unei persoane juridice în sursa sigură este voluntară și este reglementată de un acord între persoana juridică și sursa sigură. 3. Sursa sigură nu are cunoștință că persoana juridică ar avea un statut care să o împiedică să acționeze ca persoană juridică.
Substanțial	Trebuie să fie îndeplinite cerințele aferente nivelului scăzut, plus una dintre alternativele enumerate la punctele 1-3: 1. Identitatea pretinsă a persoanei juridice este demonstrată pe baza unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică, incluzând denumirea, forma de organizare și (dacă este cazul) numărul de înregistrare al persoanei juridice; și dovezile sunt verificate pentru a se stabili dacă sunt autentice sau dacă se știe că există în conformitate cu o sursă sigură, în cazul în care includerea persoanei juridice în sursa sigură este obligatorie pentru ca persoana juridică să își poată desfășura activitatea în sectorul său; și au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei juridice să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor documente pierdute, furate, suspendate, revocate sau expirate; sau 2. În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare echivalentă cu cele prevăzute în secțiunea 2.1.3 pentru nivelul de asigurare substanțial, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent; sau 3. În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare substanțial sau ridicat, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare substanțial sau ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent.
Ridicat	Trebuie să fie îndeplinite cerințele aferente nivelului substanțial, plus una dintre alternativele enumerate la punctele 1-3: 1. Identitatea pretinsă a persoanei juridice este demonstrată pe baza unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică, incluzând denumirea, forma de organizare și cel puțin un identificator unic care desemnează persoana juridică la nivel național; și dovezile au fost verificate pentru a se stabili că sunt valabile în conformitate cu o sursă sigură; sau

Nivelul de asigurare	Elementele necesare
	2. În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare echivalentă cu cele prevăzute în secțiunea 2.1.3 pentru nivelul de asigurare ridicat, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent; și se iau măsuri pentru a demonstra că rezultatele acestei proceduri anterioare rămân valabile; sau 3. În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare ridicat, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent și se iau măsuri pentru a demonstra că rezultatele acestei proceduri anterioare de emitere a unui mijloc de identificare electronică notificate rămân valabile.

2.1.4. Legătura dintre mijloacele de identificare electronică ale persoanelor fizice și juridice

După caz, pentru legătura dintre mijloacele de identificare electronică ale unei persoane fizice și mijloacele de identificare electronică ale unei persoane juridice (denumită în continuare „legătura"), se aplică următoarele condiții:

1. Trebuie să fie posibilă suspendarea și/sau retragerea unei legături. Ciclul de viață al unei legături (de exemplu, activarea, suspendarea, reînnoirea, revocarea) este administrat în conformitate cu procedurile recunoscute la nivel național.

2. Persoana fizică al cărei mijloc de identificare electronică este legat de mijlocul de identificare electronică al unei persoane juridice poate delega exercitarea legăturii către o altă persoană fizică, pe baza unor proceduri recunoscute la nivel național. Cu toate acestea, persoana fizică care deleagă rămâne responsabilă.

3. Legătura se efectuează după cum urmează:

Nivelul de asigurare	Elementele necesare
Scăzut	1. Dovedirea identității persoanei fizice care acționează în numele persoanei juridice este verificată ca fiind efectuată la nivelul scăzut sau la un nivel superior acestuia. 2. Legătura a fost stabilită pe baza unor proceduri recunoscute la nivel național. 3. Sursa sigură nu are cunoștință că persoana fizică ar avea un statut care să o împiedică să acționeze în numele persoanei juridice.
Substanțial	Punctul 3 de la nivel scăzut, plus: 1. Dovedirea identității persoanei fizice care acționează în numele persoanei juridice este verificată ca fiind efectuată la nivelul substanțial sau ridicat.

Nivelul de asigurare	Elementele necesare
	2. Legătura a fost stabilită pe baza unor proceduri recunoscute la nivel național, ceea ce a avut drept rezultat înregistrarea legăturii într-o sursă sigură. 3. Legătura a fost verificată pe baza informațiilor dintr-o sursă sigură.
Ridicat	Punctul 3 de la nivelul scăzut și punctul 2 de la nivelul substanțial, plus: 1. Dovedirea identității persoanei fizice care acționează în numele persoanei juridice este verificată ca fiind efectuată la nivelul ridicat. 2. Legătura a fost verificată pe baza unui identificator unic care desemnează persoana juridică, utilizat în contextul național; și pe baza informațiilor care desemnează în mod unic o persoană fizică dintr-o sursă autorizată.

2.2. *Gestionarea mijloacelor de identificare electronică*

2.2.1. Caracteristicile și concepția mijloacelor de identificare electronică

Nivelul de asigurare	Elementele necesare
Scăzut	1. Mijlocul de identificare electronică utilizează cel puțin un factor de autentificare. 2. Mijlocul de identificare electronică este conceput în așa fel încât emitentul să ia măsuri rezonabile pentru a se asigura că este utilizat numai sub controlul sau în posesia persoanei căreia îi aparține.
Substanțial	1. Mijlocul de identificare electronică utilizează cel puțin doi factori de autentificare din categorii diferite. 2. Mijlocul de identificare electronică este conceput în așa fel încât să se poată presupune că este utilizat numai sub controlul sau în posesia persoanei căreia îi aparține.
Ridicat	Nivelul substanțial, plus: 1. Mijlocul de identificare electronică este protejat împotriva copierii și a manipulării frauduloase, precum și împotriva atacatorilor cu potențial ridicat de atac. 2. Mijlocul de identificare electronică este conceput astfel încât să poată fi protejat în mod fiabil de către persoana căreia îi aparține împotriva utilizării de către alte persoane.

2.2.2. Emiterea, livrarea și activarea

Nivelul de asigurare	Elementele necesare
Scăzut	După emitere, mijlocul de identificare electronică este livrat prin intermediul unui mecanism grație căruia să se poate presupune că acesta ajunge numai la persoana căreia îi este destinat.
Substanțial	După emitere, mijlocul de identificare electronică este livrat prin intermediul unui mecanism grație căruia să se poate presupune că acesta ajunge numai în posesia persoanei căreia îi aparține.
Ridicat	În cadrul procesului de activare se verifică dacă mijlocul de identificare electronică a ajuns numai în posesia persoanei căreia îi aparține.

2.2.3. Suspendarea, revocarea și reactivarea

Nivelul de asigurare	Elementele necesare
Scăzut	1. Este posibil ca un mijloc de identificare electronică să fie suspendat și/sau revocat în timp util și în mod eficace. 2. Existența unor măsuri luate în scopul prevenirii suspendării, a revocării și/sau a reactivării neautorizate. 3. Reactivarea are loc numai în cazul în care cerințele în materie de asigurare stabilite înainte de suspendare sau revocare continuă să fie îndeplinite.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.2.4. Reînnoirea și înlocuirea

Nivelul de asigurare	Elementele necesare
Scăzut	Având în vedere riscurile unei modificări ale datelor de identificare personală, reînnoirea sau înlocuirea trebuie să îndeplinească aceleași cerințe de asigurare ca dovedirea și verificarea identității inițiale sau să se bazeze pe un mijloc de identificare electronică valabil cu un nivel de asigurare identic sau superior.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	Nivelul scăzut, plus: În cazul în care reînnoirea sau înlocuirea se bazează pe un mijloc de identificare electronică, datele de identitate sunt verificate prin raportare la o sursă sigură.

2.3. *Autentificarea*

Această secțiune se concentrează pe amenințări asociate cu utilizarea mecanismului de autentificare și enumeră cerințele pentru fiecare nivel de asigurare. În această secțiune controalele trebuie să fie interpretate în așa fel încât să fie proporționale cu riscurile aferente nivelului în cauză.

2.3.1. Mecanismul de autentificare

Tabelul de mai jos indică cerințele pentru fiecare nivel de asigurare cu privire la mecanismul de autentificare prin care persoana fizică sau juridică utilizează un mijloc de identificare electronică pentru a-și confirma identitatea unui beneficiar.

Nivelul de asigurare	Elementele necesare
Scăzut	1. Eliberarea datelor de identificare personală este precedată de verificarea fiabilă a mijlocului de identificare electronică și a valabilității acestuia. 2. În cazul în care datele de identificare personală sunt stocate ca parte a mecanismului de autentificare, informațiile respective sunt securizate împotriva pierderii și a compromiterii, inclusiv prin analizarea lor offline. 3. În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puțin probabil ca activități cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicațiilor de către un atacator cu potențial de atac scăzut consolidat să poată submina mecanismele de autentificare.

Nivelul de asigurare	Elementele necesare
Substanțial	Nivelul scăzut, plus: 1. Eliberarea datelor de identificare personală este precedată de verificarea fiabilă a mijlocului de identificare electronică și a valabilității acestuia printr-o autentificare dinamică. 2. În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puțin probabil ca activități cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicațiilor de către un atacator cu potențial de atac moderat să poată submina mecanismele de autentificare.
Ridicat	Nivelul substanțial, plus: În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puțin probabil ca activități cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicațiilor de către un atacator cu potențial de atac ridicat să poată submina mecanismele de autentificare.

2.4. *Gestionarea și organizarea*

Toți participanții care prestează un serviciu legat de identificarea electronică în context transfrontalier (denumiți în continuare „prestatori") trebuie să dispună de practici și politici de management al securității informațiilor, de abordări în materie de gestionare a riscurilor și de alte controale recunoscute, astfel încât organismelor de guvernanță pentru sistemele de identificare electronică din statele membre respective să li se ofere asigurarea că există și se utilizează practici eficace. În întreaga secțiune 2.4, toate cerințele/elemente trebuie înțelese ca fiind proporționale cu riscurile aferente nivelului în cauză.

2.4.1. Dispoziții generale

Nivelul de asigurare	Elementele necesare
Scăzut	1. Prestatorii oricărui serviciu operațional care face obiectul prezentului regulament sunt o autoritate publică sau o entitate juridică recunoscută ca atare de legislația națională a unui stat membru, având o structură organizatorică bine-definită și fiind pe deplin operațională din toate punctele de vedere relevante pentru prestarea serviciilor. 2. Prestatorii respectă toate cerințele legale care le revin în legătură cu operarea și furnizarea serviciilor, inclusiv în ceea ce privește tipurile de informații care ar putea fi cerute, modul în care se efectuează dovedirea identității, informațiile care pot fi păstrate și perioada pentru care pot fi păstrate. 3. Prestatorii sunt în măsură să își demonstreze capacitatea de a-și asuma riscul răspunderii pentru daune, precum și faptul că dispun de suficiente resurse financiare pentru a continua operațiunile și prestarea serviciilor. 4. Prestatorii sunt răspunzători de îndeplinirea oricăruia dintre angajamentele externalizate către o altă entitate, precum și de conformitatea cu politica sistemului, ca și când prestatorii ar fi îndeplinit ei înșiși sarcinile respective. 5. Sistemele de identificare electronică care nu au fost înființate prin legislația națională trebuie să aibă un plan eficace pentru cazul încetării serviciului. Un astfel de plan trebuie să prevadă încetarea ordonată a serviciului sau continuarea prestării sale de către un alt prestator, modul în care autoritățile competente și utilizatorii finali sunt informați, precum și detalii cu privire la modul în care ar trebui să fie protejate, reținute și distruse înregistrările în conformitate cu politica sistemului.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.4.2. Anunțurile publicate și informațiile pentru utilizatori

Nivelul de asigurare	Elementele necesare
Scăzut	1. Existența unei definiții publicate a serviciului, care să includă toți termenii, toate condițiile și toate tarifele aplicabile, inclusiv eventualele limitări ale utilizării acestuia. Definiția serviciului include o politică privind protecția vieții private. 2. Trebuie instituite o politică și proceduri adecvate pentru a se asigura că utilizatorii serviciului sunt informați într-o manieră fiabilă și la timp cu privire la orice modificare a definiției serviciului și a oricăreia dintre clauzele, condițiile și măsurile de protecție a vieții private pentru serviciul în cauză. 3. Trebuie instituite politici și proceduri adecvate care să asigure răspunsuri integrale și corecte la solicitările de informații.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.4.3. Managementul securității informațiilor

Nivelul de asigurare	Elementele necesare
Scăzut	Există un sistem eficace de management al securității informațiilor, pentru gestionarea și controlul riscurilor la adresa securității informației.
Substanțial	Nivelul scăzut, plus: Sistemul de management al securității informațiilor respectă standarde sau principii dovedite de gestionare și control al riscurilor la adresa securității informației.
Ridicat	La fel ca pentru nivelul substanțial.

2.4.4. Păstrarea evidențelor

Nivelul de asigurare	Elementele necesare
Scăzut	1. Înregistrarea și păstrarea informațiilor relevante prin utilizarea unui sistem eficace de gestionare a evidențelor, ținând seama de legislația aplicabilă și de bunele practici în ceea ce privește protecția și păstrarea datelor. 2. Păstrarea, în măsura în care acest lucru este permis de legislația națională sau de alte dispoziții administrative naționale, și protejarea evidențelor atât timp cât acestea sunt necesare în scopuri de audit și de investigare a cazurilor de încălcare a securității și în scopuri de păstrare a datelor, după care acestea trebuie distruse în mod securizat.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.4.5. Infrastructură și personal

Tabelul de mai jos prezintă cerințele în materie de infrastructură și personal și, după caz, în materie de subcontractanți care îndeplinesc sarcini care intră sub incidența prezentului regulament. Conformitatea cu fiecare cerință trebuie să fie proporțională cu nivelul de risc aferent nivelului de asigurare oferit.

Nivelul de asigurare	Elementele necesare
Scăzut	1. Existența unor proceduri care să garanteze că personalul și subcontractanții sunt suficient de bine formați, calificați și experimentați în ceea ce privește abilitățile necesare pentru a îndeplini rolurile care le revin. 2. Existența unui număr suficient de angajați și de subcontractanți pentru a funcționa în mod adecvat și a asigura resurse serviciului în conformitate cu politicile și procedurile sale. 3. Infrastructura utilizată pentru prestarea serviciilor este monitorizată continuu și protejată împotriva pagubelor provocate de evenimente de mediu, a accesului neautorizat și a altor factori care pot influența securitatea serviciului. 4. Prin infrastructura utilizată pentru prestarea serviciului se asigură că accesul la zonele unde se păstrează sau se prelucrează informații personale, criptografice sau alte informații sensibile este limitat la personalul autorizat sau la subcontractanți.
Substanțial	La fel ca pentru nivelul scăzut.
Ridicat	La fel ca pentru nivelul scăzut.

2.4.6. Controalele tehnice

Nivelul de asigurare	Elementele necesare
Scăzut	1. Existența unor controale tehnice proporționale pentru a gestiona riscurile la adresa securității serviciilor, asigurând protejarea confidențialității, a integrității și a disponibilității informațiilor prelucrate. 2. Canalele de comunicare electronice utilizate pentru a face schimb de date cu caracter personal sau de informații sensibile sunt protejate împotriva interceptării, a manipulării și a reproducerii. 3. Accesul la materialele criptografic sensibile, dacă acestea sunt utilizate pentru emiterea mijloacelor de identificare electronică și de autentificare, se limitează la rolurile și aplicațiile care necesită neapărat accesul. Este necesar să se asigure că aceste materiale nu sunt niciodată stocate pe durate mai lungi sub formă de text simplu. 4. Există proceduri pentru a se asigura că securitatea se menține în timp și că există capacitatea de a reacționa la schimbările nivelurilor de risc, la incidente și încălcări ale securității. 5. Toate suporturile care conțin informații personale, criptografice sau alte informații sensibile sunt stocate, transportate și eliminate în condiții de siguranță și în mod securizat.
Substanțial	La fel ca pentru nivelul scăzut, plus: Materialele criptografice sensibile, dacă sunt utilizate pentru emiterea mijloacelor de identificare electronică și de autentificare, sunt protejate împotriva manipulărilor frauduloase
Ridicat	La fel ca pentru nivelul substanțial.

2.4.7. Conformitatea și auditul

Nivelul de asigurare	Elementele necesare
Scăzut	Existența unor audituri interne periodice, al căror domeniu de aplicare include toate aspectele relevante pentru prestarea serviciilor furnizate, pentru a se asigura respectarea politicii relevante.

Nivelul de asigurare	Elementele necesare
Substanțial	Existența unor audituri interne sau externe periodice independente, al căror domeniu de aplicare include toate aspectele relevante pentru prestarea serviciilor furnizate, pentru a se asigura respectarea politicii relevante.
Ridicat	1. Existența unor audituri externe periodice independente, al căror domeniu de aplicare include toate aspectele relevante pentru prestarea serviciilor furnizate, pentru a se asigura respectarea politicii relevante. 2. În cazul în care un program este gestionat direct de către un organism guvernamental, acesta este auditat în conformitate cu legislația națională.