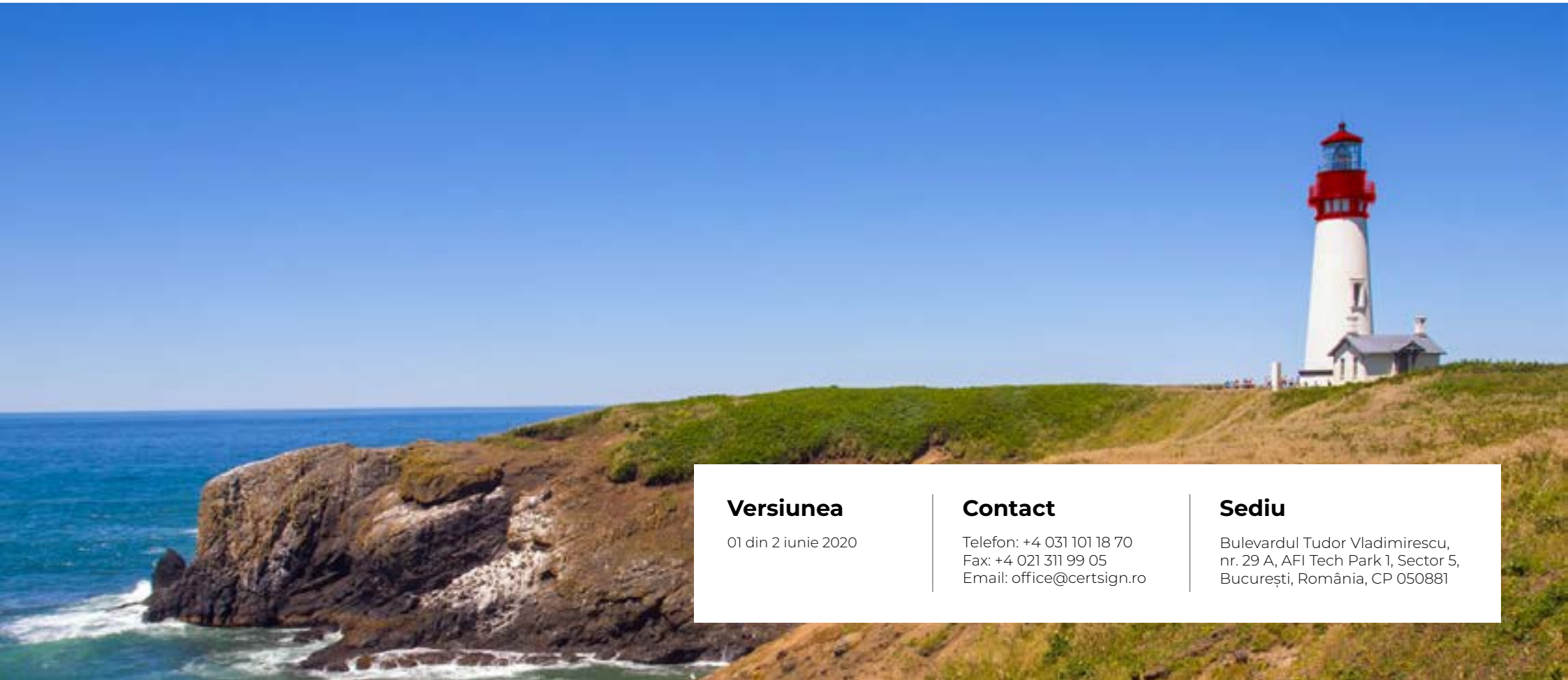
certSIGN

GHID DE BUNE PRACTICI ȘI ASPECTE LEGALE PRIVIND UTILIZAREA SEMNĂTURII ELECTRONICE ÎN ORGANIZAȚII



Versiunea

01 din 2 iunie 2020

Contact

Telefon: +4 031 101 18 70
Fax: +4 021 311 99 05
Email: office@certsign.ro

Sediu

Bulevardul Tudor Vladimirescu,
nr. 29 A, AFI Tech Park 1, Sector 5,
București, România, CP 050881

Acest GHID este proprietatea CERTSIGN SA. Nu puteți utiliza acest document în integralitatea sa sau în parte decât pentru uz personal și necomercial. De asemenea nu îl puteți transmite către terți fără indicarea sursei ca fiind CERTSIGN SA.

Nu puteți distribui, publica sau comercializa conținutul acestui Ghid fără consimțământul expres și prealabil al CERTSIGN SA.

Acest Ghid conține opinia CERTSIGN SA cu privire la semnătura electronică și nu vă puteți întemeia deciziile sau comportamentul pe conținutul acestuia și nu puteți considera CERTSIGN SA răspunzător pentru cele exprimate în document sau dacă v-ați întemeiat deciziile pe acesta. Există opinii și puncte de vedere diferite, cu privire la conceptele prezentate în acest document.

Scopul acestui Ghid este acela de a facilita înțelegerea conceptului de semnătură electronică și a efectelor acesteia, astfel cum CERTSIGN SA le-a înțeles având în vedere legislația și tehnologiile existente până în acest moment în domeniul semnăturii electronice.

CUPRINS

1. INTRODUCERE
pg. 4
CITEȘTE

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE
pg. 5
DOCUMENTEAZĂ-TE

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR
pg. 15
DESCOPERĂ

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE
pg. 24
AFLĂ CUM

5. VALOAREA LEGALĂ A DOCUMENTELOR ELECTRONICE SEMNATE ELECTRONIC
pg. 41
CONSULTĂ LEGILE

6. ANEXE
pg. 50
CITEȘTE

1. INTRODUCERE

Ghidul de bune practici și aspecte legale privind utilizarea semnăturii electronice în organizații prezintă posibilitățile de folosire a semnăturilor electronice în România. Face o analiză a cadrului legislativ european, Regulamentul UE nr. 910/2014 și actele de punere în aplicare a acestuia, norme legale direct aplicabile în fiecare stat membru al Uniunii Europene.

Ghidul are în vedere o abordare completă, acoperind atât aspecte teoretice cât și aspecte practice, de utilizare a semnăturilor într-o organizație.

Documentul pornește de la definițiile diferitelor tipuri de semnături electronice, formatele de semnături, așa cum sunt ele stabilite la nivelul UE, și diferențele dintre acestea.

Conține informații privind modul în care se pot verifica semnăturile electronice și ce trebuie să aibă în vedere o organizație atunci când hotărăște să utilizeze sau să accepte documente semnate electronic.

Sunt făcute recomandări cu privire la tipurile de semnături electronice ce pot fi utilizate, principalele considerente analizat fiind: simplitate în folosire, nivelul de recunoaștere automat, în România și la nivelul UE, precum și ușurința în dovedirea valorii legale.

Din 2006, certSIGN are o experiență solidă cu privire la aspectele tehnice și legislative ce țin de documentele digitale și semnăturile electronice.

Experiența națională este întărită de activitatea internațională în zona serviciilor de încredere: prezența în comitetul tehnic ETSI care gestionează standardele cu privire la semnătură electronică și servicii de încredere, participarea la teste de interoperabilitate a semnăturilor electronice sau membru al Cloud Signature Consortium (CSC).

Echipa ce a contribuit la elaborarea acestui ghid are peste 20 de ani de experiență în domeniul criptografiei, serviciilor de încredere, precum și în și domeniul juridic.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.1 DEFINIȚII CONFORM REGULAMENTULUI 910/2014

2.1.1 SEMNĂTURA ELECTRONICĂ

Regulamentul 910/2014 definește, la art. 3, pct. 10:

▸ „semnătură electronică” înseamnă date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;

iar la pct. 9:

▸ „semnatar” înseamnă o persoană fizică care creează o semnătură electronică.

DE REȚINUT

▸ Semnătura electronică este un termen foarte larg, care nu are nicio legătură cu gradul de încredere pe care cineva se presupune că ar trebui să îl aibă în el; adică o cerință de genul „documentul trebuie semnat electronic” are un efect foarte scăzut, din punct de vedere al gradului în care o parte interesată se poate baza pe acel document că reprezintă într-adevăr actul de voința al semnatarului;

Practic

- ▸ simpla precizare a numelui semnatarului la sfârșitul unui document electronic se încadrează la definiția semnăturii electronice, sau
- ▸ atașarea unei poze a semnăturii olografe, sau chiar a pozei semnatarului la un document se încadrează în definiție, sau
- ▸ un scan după un document semnat olograf de semnatar atașat la un e-mail se încadrează în definiție etc.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.1 DEFINIȚII CONFORM REGULAMENTULUI 910/2014

2.1.1 SEMNĂTURA ELECTRONICĂ

▸ „Semnătura electronică” este un concept abstract, nu se bazează pe nici o tehnologie specifică, ea se poate realiza prin diferite tehnologii, așa cum se vede și din exemplele de mai sus.

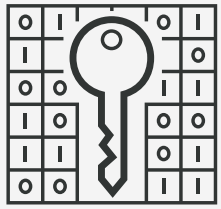
▸ Un tip concret de tehnologie pentru crearea unei semnături electronice este semnătura digitală care este bazată pe criptarea cu chei publice generate cu ajutorul unei Infrastructuri cu chei publice - PKI (Public Key Infrastructure). Semnătura digitală atașată unui document este de fapt rezultatul criptării acelui document, mai precis al unui hash al acestuia cu o cheie așa numită privată pe care se presupune că numai semnatarul o are. Această criptare poate fi decriptată cu o cheie publică, unică asociată acelei chei private.

Cheia publică este cunoscută tuturor, în acest fel oricine poate verifica semnătura documentului. Dacă poate decripta valoarea hash înseamnă că documentul a fost semnat cu cheia privată asociată cheii publice și se poate stabili originea semnăturii.

Cel care verifică o semnătură calculează, la rândul lui, hash-ul documentului.

Daca hash-ul calculat de cel care verifica semnătura este identic cu cel transmis de cel care a semnat, înseamnă ca documentul nu a fost modificat între timp. Cheia publică este încorporată într-un așa numit certificat digital care garantează legătura dintre persoana fizică semnatară și perechea cheie publică - cheie privată.

Certificatul digital este emis de un prestator de servicii de încredere, el garantând această asociere într-un grad mai mare sau mai mic de încredere.



2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.1 DEFINIȚII CONFORM REGULAMENTULUI 910/2014

2.1.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ

Regulamentul 910/2014 definește, la art. 3, pct. 11:

▸ „semnătură electronică avansată” înseamnă o semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26;

Conform art. 26: O semnătura electronică avansată îndeplinește următoarele cerințe:

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.

Iar art. 3 pct. 13 prevede:

▸ „date de creare a semnăturilor electronice” înseamnă date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică.

DE REȚINUT

▸ „Semnătura electronică avansată”, spre deosebire de semnătura electronică, este un concept care este strâns legat de gradul de încredere pe care cineva se presupune că ar trebui să îl aibă în el;

▸ 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;

▸ „Semnătura electronică avansată” este un concept abstract, nu se referă la o tehnologie specifică, se poate realiza prin diferite tehnologii (soluții tehnice și procedurale) și aceste tehnologii trebuie să asigure îndeplinirea celor 4 cerințe din definiția semnăturii electronice avansate;

▸ PROVOCAREA ESTE ÎNSĂ DE A DEMONSTRA ÎNDEPLINIREA CELOR 4 CONDIȚII ȘI ACEST LUCRU NU ARE CUM SĂ FIE POSIBIL DECÂT DACĂ TEHNOLOGIA RESPECTIVĂ (SOLUȚIE TEHNICĂ ȘI PROCEDURILE AFERENTE) ESTE ECHIVALENTĂ TEHNOLOGIEI PENTRU SEMNĂTURA CALIFICATĂ DESCRISĂ ÎN REGULAMENTUL 910/2014.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.1 DEFINIȚII CONFORM REGULAMENTULUI 910/2014

2.1.3 SEMNĂTURA ELECTRONICĂ CALIFICATĂ

Regulamentul 910/2014 definește, la art. 3, pct. 12:

▸ „semnătură electronică calificată” înseamnă o semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificat și care se bazează pe un certificat calificat pentru semnăturile electronice;

și mai departe:

23. „dispozitiv de creare a semnăturilor electronice calificat” înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în **anexa II**; (a se vedea în **Anexele** de la prezentul ghid)

22. „dispozitiv de creare a semnăturilor electronice” înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;

15. „certificat calificat pentru semnătură 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 se vedea în **Anexele** de la prezentul ghid)

14. „certificat pentru semnătura electronică” înseamnă o atestare electronică care face legătura între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele sau pseudonimul persoanei respective;

20. „prestator de servicii de încredere calificat” înseamnă un prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;

19. „prestator de servicii de încredere” înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;

17. „serviciu de încredere calificat” înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;

16. „serviciu de încredere” înseamnă 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;

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.1 DEFINIȚII CONFORM REGULAMENTULUI 910/2014

2.1.3 SEMNĂTURA ELECTRONICĂ CALIFICATĂ

DE REȚINUT

▸ 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 așa cum se poate vedea în definițiile prezentate mai sus și în Anexe 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.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ VS CALIFICATĂ

Așa cum rezultă din definițiile și observațiile din secțiunea 2.1, NU se poate face o comparație între semnătura electronică avansată și cea calificată. E ca și cum ne-am propune să comparăm termenii „automobil" cu „Dacia Duster" sau „medicament" cu „aspirină" sau „mamifer" cu „tigru". „Semnătura avansată" reprezintă un concept abstract pe când "Semnătura calificată" reprezintă semnătura electronică bine definită de tehnologia concretă, utilizată pentru a fi creată.

Semnătura calificată este o semnătură electronică pentru care se precizează tehnologia (soluția tehnică și procedurală) utilizată. Și această tehnologie este demonstrabil, doar în baza prevederilor Regulamentului 910/2014 și ale actelor de punere în aplicare ale acestuia, că îndeplinește cele 4 cerințe pentru semnătura electronică avansată, așa cum se poate vedea și în **Tabelul 1** Semnătura calificată.

Tabel 1. Semnătura calificată

CERINȚE ART. 26 DIN REGULAMENTUL 910/2014	**(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;	**(d)** este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.
SEMNĂTURA ELECTRONICĂ CALIFICATĂ	**DA**, pentru că se bazează pe și conține certificatul calificat, care face trimitere exclusiv la semnatar, conform Anexei I la Regulamentul 910/2014, punctul c.	**DA**, pentru că se bazează pe și conține certificatul calificat, care se emite în condițiile prevăzute la art. 24 (1) din Regulamentul 910/2014.	**DA**, pentru că se bazează pe QSCD care îndeplinește această cerință conform Anexei II la Regulamentul 910/2014, punctul 1.	**DA**, pentru ca se utilizează certificate digitale, adică tehnologie cu chei publice care asigură integritatea datelor semnate, **dar cu condiția utilizării de către semnatar a formatelor standardizate prevăzute de Regulamentul 910/2014 și Decizia 1506/2015**.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ VS CALIFICATĂ

Cu privire la cerința de la punctul b , „permite identificarea semnatarului”, art. 24, alin.1 din Regulamentul 910/2014 prevede reguli clare pentru prestatorul calificat cu privire la identificarea în vederea emiterii certificatelor calificate:

„**(1)** Atunci când emite un certificat calificat pentru un serviciu de încredere, un prestator de servicii de încredere calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat.

Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în conformitate cu dreptul intern:

(a) de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau

(b) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice și care îndeplinesc cerințele stabilite la articolul 8 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”; sau

(c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu dispozițiile de la litera **(a)** sau **(b)**; sau

(d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică.

Nivelul de asigurare echivalent este confirmat de un organism de evaluare a conformității.”

Îndeplinirea acestor condiții de către prestatorul calificat fac ca punctul b din art. 26 să fie îndeplinit cu certitudine în cazul semnăturii calificate.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ VS CALIFICATĂ

În sprijinul argumentelor aduse vine materialul realizat de ENISA (The European Union Agency for Cybersecurity) **Security guidelines on the appropriate use of qualified electronic signatures**, Guidance for users, Version 2.0, Final, December 2016:

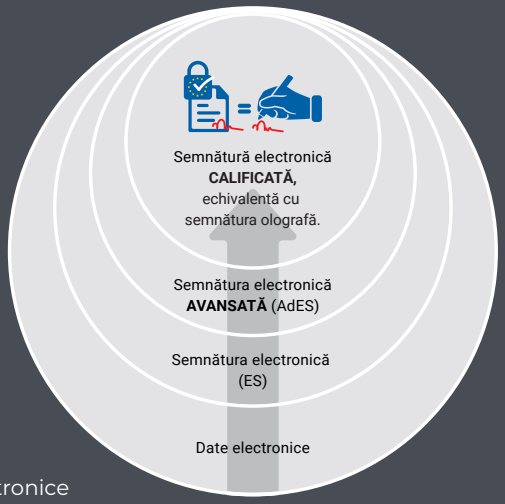


Figura 1 Tipuri de semnături electronice

Figura 1 Tipuri de semnături electronice, extrasă din Ghid („Fig. 3 - Types of electronic signatures"), este cât se poate de sugestivă, arătând în mod clar că semnătura calificată (QES) este un tip de semnătură avansată CERTĂ/ DOVEDITĂ datorită specificațiilor sale tehnice și a mecanismelor tehnice și procedurale precizate în clar prin Regulamentul 910/2014.

Întrebarea atunci este: ce alte exemple de semnături avansate create prin tehnologii concrete s-ar putea da?

De exemplu, art. 27 din Regulamentul 910/2014 face referire la „semnătura avansată bazată pe certificat calificat". Putem avea semnătură avansată bazată pe certificat necalificat și pe dispozitiv necalificat de creare a semnăturii electronice? Sau putem avea semnătură avansată bazată pe o altă tehnologie decât cea bazată pe certificate?

Teoretic da, dar cu condițiile specificate în **Tabelul 2** - tot ce este cu roșu revine în sarcina semnatarului să dovedească și, respectiv destinatarului/persoanei care se bazează pe acel document să verifice că era corect LA MOMENTUL SEMNĂRII.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ VS CALIFICATĂ

Tabel 2. Alte tipuri de semnături electronice

CERINȚE ART. 26 DIN REGULAMENTUL 910/2014	**(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;	**(d)** Este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.
SEMNĂTURA ELECTRONICĂ BAZATĂ PE CERTIFICAT CALIFICAT (FĂRĂ DISPOZITIV CALIFICAT)	**DA**, pentru că se bazează pe și conține certificatul calificat, care face trimitere exclusiv la semnatar, conform Anexei 1 la Regulamentul 910/2014, punctul c.	**DA**, pentru că se bazează pe și conține certificatul calificat, care se emite în condițiile prevăzute la art. 24 (1).	Trebuie ca persoana interesată să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea utilizată pentru gestionarea accesului la datele de creare a semnăturii.	**DA**, pentru că se utilizează certificate digitale, adică tehnologie cu chei publice care asigură integritatea datelor semnate, **dar cu condiția utilizării de către semnatar a formatelor standardizate prevăzute de Regulamentul 910/2014 și Decizia 1506/2015.**
SEMNĂTURA ELECTRONICĂ BAZATĂ PE CERTIFICAT NECALIFICAT ȘI CREATĂ FOLOSIND DISPOZITIV CALIFICAT	Trebuie ca persoana interesată să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea în care s-a emis respectivul certificat necalificat.	Trebuie ca persoana interesată să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea în care s-a emis respectivul certificat necalificat și a procedurilor de identificare utilizate la momentul emiterii certificatului necalificat.	**DA**, pentru că se bazează pe QSCD care îndeplinește această cerința conform Anexei II la Regulamentul 910/2014, punctul 1.	**DA**, pentru că se utilizează certificate digitale, adică tehnologie cu chei publice care asigură integritatea datelor semnate, **dar cu condiția utilizării formatelor standardizate prevăzute de Regulamentul 910/2014 și Decizia 1506/2015.**
SEMNĂTURA ELECTRONICĂ BAZATĂ PE CERTIFICAT NECALIFICAT ȘI FĂRĂ DISPOZITIV CALIFICAT	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea în care s-a emis respectivul certificat necalificat.	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea în care s-a emis respectivul certificat necalificat și a procedurilor de identificare utilizate la momentul emiterii certificatului necalificat.	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de modalitatea utilizată pentru gestionarea accesului la datele de creare a semnăturii.	**DA**, pentru că se utilizează certificate digitale, adică tehnologie cu chei publice care asigură integritatea datelor semnate, **dar cu condiția utilizării formatelor standardizate prevăzute de Regulamentul 910/2014 și Decizia 1506/2015.**
SEMNĂTURA ELECTRONICĂ BAZATĂ PE ALTE MECANISME DECÂT SEMNĂTURA DIGITALĂ	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de mecanismul utilizat.	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de mecanismul utilizat.	Trebuie ca semnatarul să poată demonstra această cerință LA MOMENTUL SEMNĂRII, în funcție de mecanismul utilizat.	Trebuie ca semnatarul să poată demonstra această cerință, în funcție de mecanismul utilizat.

2. DEFINIȚII ȘI DIFERENȚE ÎNTRE DIFERITELE TIPURI DE SEMNĂTURI ELECTRONICE CE SE POT UTILIZA ÎNTR-O ORGANIZAȚIE

2.2 SEMNĂTURA ELECTRONICĂ AVANSATĂ VS CALIFICATĂ

DE REȚINUT

▸ Semnătura calificată este o semnătură avansată certă/dovedită datorită tehnologiei și standardelor, pe care se bazează, precizate concret de Regulamentul 910/2014;

▸ Este foarte important de reținut că **O SEMNĂTURĂ ELECTRONICĂ NE-CALIFICATĂ NU ESTE IMPLICIT AVANSATĂ**;

o semnătură electronică ne-calificată înseamnă că este o semnătură electronică creată prin altă tehnologie decât cea a semnăturii calificate; în funcție de acea tehnologie, semnătura poate să fie sau nu avansată;

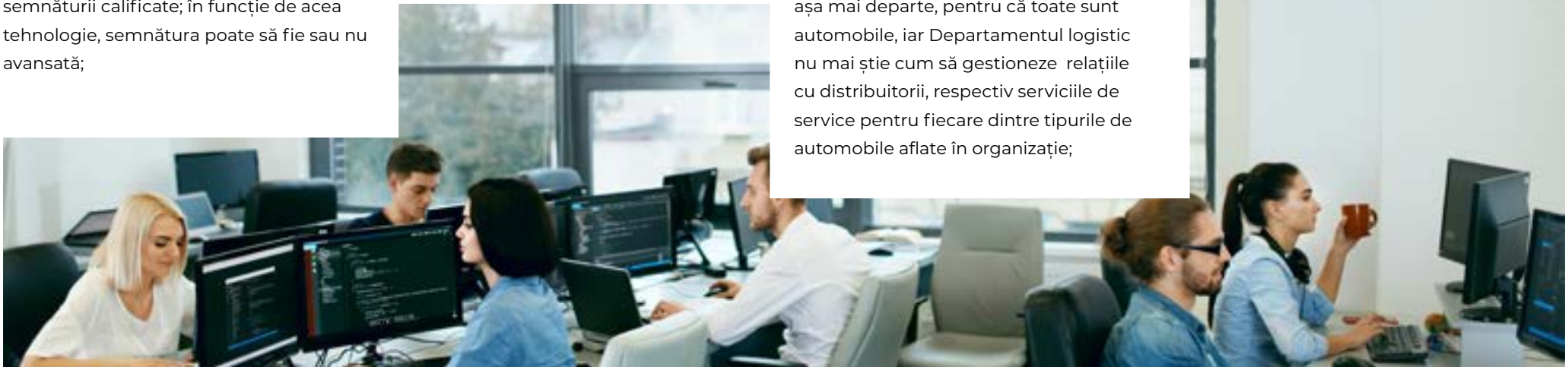
▸ Când într-un anumit context se face referire la semnătura avansată fără a se preciza tehnologia (soluția tehnică și procedurală) pe care se bazează, atunci poate fi vorba de ORICE tehnologie, inclusiv cea utilizată de semnătură calificată;

▸ Deci există, teoretic, o multitudine de tipuri de semnături avansate concrete, câte tehnologii care îndeplinesc cele 4 condiții de la art. 26 ar putea fi identificate;

▸ De aceea, o organizație care își propune să accepte/utilizeze „semnătura avansată” fără să precizeze și tehnologia/tehnologiile cu care se creează, pe care le acceptă/utilizează, va avea mari probleme atât în ceea ce privește crearea semnăturilor electronice, cât mai ales, în verificarea acestora;

▸ Ar fi ca și cum ar emite o decizie în care ar spune: „Organizația noastră folosește automobile pentru deplasarea echipei de vânzari.” Și atunci un vânzător cere o Dacia, altul un Ferari, altul o Tesla și așa mai departe, pentru că toate sunt automobile, iar Departamentul logistic nu mai știe cum să gestioneze relațiile cu distribuitorii, respectiv serviciile de service pentru fiecare dintre tipurile de automobile aflate în organizație;

▸ Totuși, Regulamentul 910/2014, referitor la semnăturile electronice în cadrul serviciilor publice, recomandă utilizarea tehnologiei bazată pe chei publice, sau în cazul în care se utilizează alte tehnologii, impune condiții clare care trebuie îndeplinite de acele tehnologii, așa cum vom arăta când vom detalia formatele de semnătură electronică.



3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.1 FORMATE DE SEMNĂTURĂ ELECTRONICĂ CONFORM REGULAMENTULUI 910/2014 ȘI A ACTELOR DE PUNERE ÎN APLICARE ALE ACESTUIA ȘI OBLIGAȚIILE ORGANIZAȚIILOR PUBLICE ÎN LEGĂTURĂ CU ACESTE FORMATE

Una dintre concluziile importante ale capitolului precedent este că, teoretic, pot exista o multitudine de tehnologii (soluții tehnice și procedurale) de creare de semnătură electronică, respectiv semnătură electronică avansată.

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 la care dintre tehnologii să se limiteze o organizație se poate lua luând în considerare 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 o organizație privată:

“**Articolul 27**
Semnăturile electronice în cadrul serviciilor publice

(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 întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

(2) În cazul în care un stat membru solicită o semnătură electronică avansată bazată pe un certificat calificat 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 bazate pe un certificat calificat și semnăturile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

(3) 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.

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru semnături electronice avansate. În cazul în care o semnătură electronică avansată îndeplinește respectivele standarde, se presupune că aceasta respectă cerințele referitoare la semnăturile electronice avansate menționate în prezentul articol alineatele (1) și (2) și la articolul 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(5) Până la 18 septembrie 2015 și ținând cont de practicile, standardele și actele juridice ale Uniunii existente, Comisia definește, prin intermediul unor acte de punere în aplicare, formate de referință ale semnăturilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

Actul de aplicare la care se face referire la alineatele (4) și (5) este DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1506 A COMISIEI din 8 septembrie 2015 de stabilire a specificațiilor referitoare la formatele semnăturilor și sigiliilor electronice avansate care trebuie recunoscute de către organismele din sectorul public în temeiul articolului 27 alineatul (5) și al articolului 37 alineatul (5) 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, care prevede următoarele:

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.1 FORMATE DE SEMNĂTURĂ ELECTRONICĂ CONFORM REGULAMENTULUI 910/2014 ȘI A ACTELOR DE PUNERE ÎN APLICARE ALE ACESTUIA ȘI OBLIGAȚIILE ORGANIZAȚIILOR PUBLICE ÎN LEGĂTURĂ CU ACESTE FORMATE

Articolul 1

Statele membre care prevăd utilizarea unei semnături electronice avansate sau a unei semnături electronice avansate bazate pe un certificat calificat, astfel cum se menționează la articolul 27 alineatele (1) și (2) din Regulamentul (UE) nr. 910/2014, recunosc semnăturile electronice avansate în formatele XML, CMS sau PDF la nivelul de conformitate B, T sau LT și fișierele-container cu semnătură asociată dacă semnăturile în cauză respectă specificațiile tehnice enumerate în anexă." - a se vedea **Anexa** la Decizia de punere în aplicare (UE) 2015/1506 a Comisiei.

Din această **anexa** rezultă că, în conformitate cu Regulamentul 910/2014, statele membre trebuie să recunoască formatele de semnătură avansată care respectă unul dintre standardele:

- PAdES - se referă la semnătura în documentele de tip PDF;

- Cades - se referă la semnătura pentru orice tip de document electronic, care se încapsulează într-un fișier de tip CMS (sau PKCS7) atașat sau detașat documentului care este semnat;

- XAdES - se referă la semnătura pentru fișierele în format XML.

Analizând standardele referite pentru fiecare dintre cele trei formate de semnătură, rezultă faptul că toate acestea se creează utilizând semnătura digitală adică tehnologia bazată pe criptare cu chei publice, respectiv certificate digitale.

Coroborând prevederile art. 27 ale Regulamentului 910/2104 și art. 1 Decizia de punere în aplicare 1506/2015 concluzia este că, din perspectiva Regulamentului, o organizație publică are următoarele opțiuni:

- Să aleagă să utilizeze/accepte o semnătură electronică bazată pe certificat necalificat (într-unul din formatele PDF, CMS și/sau XML), cu condiția să dovedească faptul că este avansată, DAR conform art. 27 este OBLIGATĂ să accepte și:

  - semnătura electronică avansată bazată pe orice tip de certificat digital (în formatul corespunzător ales PDF, CMS și/ sau XML), care de asemenea trebuie să se dovedească că este avansată la momentul semnării;

  - semnătura electronică bazată pe certificat calificat (în formatul corespunzător ales PDF, CMS și/sau XML), care de asemenea trebuie să se dovedească că este avansată;

  - semnătura calificată (în formatul corespunzător ales PDF, CMS și/sau XML) - care am arătat în capitolul precedent că este CERTĂ că este avansată

- Să aleagă să utilizeze/accepte o semnătură electronică bazată pe certificat calificat (într-unul din formatele PDF, CMS și/sau XML), cu condiția să dovedească faptul că este avansată, DAR conform art. 27 este OBLIGATĂ să accepte și:

  - semnătura calificată (în formatul corespunzător ales PDF, CMS și/ XML) - care am arătat în capitolul precedent că este CERTĂ că este avansată;

- Să aleagă să utilizeze/accepte doar semnătura electronică calificată (într-unul din formatele PDF, CMS și/sau XML).

Desigur, o organizație privată poate să nu fie supusă obligațiilor precizate mai sus, dar ele pot fi o referință pentru organizațiile private, mai ales că, probabil, toate emit și documente care sunt destinate organismelor publice.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.1 FORMATE DE SEMNĂTURĂ ELECTRONICĂ CONFORM REGULAMENTULUI 910/2014 ȘI A ACTELOR DE PUNERE ÎN APLICARE ALE ACESTUIA ȘI OBLIGAȚIILE ORGANIZAȚIILOR PUBLICE ÎN LEGĂTURĂ CU ACESTE FORMATE

Mai trebuie precizat că Decizia de punere în aplicare 1506/2015 prevede la art. 2, alin. (1) și posibilitatea utilizării de alte formate decât cele precizate mai sus, cu condiția să existe posibilitatea de validare a acestor formate:

„(1) Statele membre care prevăd utilizarea unei semnături electronice avansate sau a unei semnături electronice avansate bazate pe un certificat calificat, astfel cum se menționează la articolul 27 alineatele (1) și (2) din Regulamentul (UE) nr. 910/2014, recunosc semnăturile electronice în formate diferite de cele menționate la articolul 1 din prezenta decizie dacă statul membru în care este stabilit prestatorul de servicii de încredere utilizate de semnatar oferă altor state membre posibilități de validare a semnăturilor care, atunci când este posibil, sunt adecvate pentru prelucrarea automată.”

Conform acestui articol, dacă o organizație publică solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online, aceasta este OBLIGATĂ să accepte și o semnătura electronică avansată în formate diferite de formatele PDF, CMS și/sau XML dacă statul membru în care este stabilit prestatorul de servicii de încredere utilizate de semnatar oferă a posibilități de validare a semnăturilor.

DE REȚINUT

Dacă o instituție sau autoritate publică alege totuși să accepte semnătura avansată și într-un alt format decât cele trei specificate de Regulamentul 910/2014, atunci conform art. 27 (1) este obligată să accepte orice semnătură avansată în formatele și metodele definite în Decizia de punere în aplicare 1506/2015, semnătura electronică bazată pe certificat calificat, precum și semnătura calificată.

Pornind totuși de la premiza că formatele de semnături definite de Decizia de punere în aplicare 1506/2015 sunt cele mai utilizate (XML, CMS și PDF), începând cu acest capitol ne vom concentra doar pe aceste formate de semnătură electronică avansată și în special pe formatul PDF.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.2 TIPURI DE SEMNĂTURI ELECTRONICE CÂND AVEM MAI MULȚI SEMNATARI AI ACELUIAȘI DOCUMENT

SEMNĂTURI PARALELE SAU CO-SEMNĂTURA
(„parallel signatures”) - presupun că toți semnatarii semnează același conținut, deci nu contează ordinea în care se semnează și semnăturile nu depind una de cealaltă.

SEMNĂTURI ÎNSERIATE
(„serial signature”) - acestea sunt semnături aplicate diferitelor obiecte de date dintr-un document și a căror ordine de generare este relevantă. Pentru astfel de semnături este necesar să se identifice semnăturile necesare și ordinea lor și la ce obiect (obiecte) de date ar trebui să se aplice fiecare și unde trebuie să apară aceste semnături.

CONTRA-SEMNĂTURI
(“counter signature”) - acestea sunt un tip special de semnături înseriate, utilizate în procesele care stabilesc că o anumită semnătură nu are niciun efect decât dacă este aplicată pe rând după o altă semnătură, de obicei generată de o anumită entitate îndreptățită să confere un astfel de efect primului. Contra-semnăturile se aplică una după celelalte și sunt utilizate acolo unde ordinea în care se aplică semnăturile este importantă.

Formatul PDF permite doar semnăturile înseriate, răspunzând tuturor aspectelor practice întâlnite în semnarea documentelor.

CMS și XML permit atât semnături paralele, cât și semnături înseriate, inclusiv contra-semnături.

Facem precizarea că această clasificare a tipurilor de semnături este una pur tehnică și nu are nici o legătură cu efectul juridic al respectivelor semnături.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.3 CUM SE DIFERENȚIAZĂ SEMNĂTURA ELECTRONICĂ FAȚĂ DE SEMNĂTURA OLOGRAFĂ

Poate lucrul cel mai important care trebuie înțeles de către utilizatori este că, așa cum pentru a ajunge să semneze olograf un om mai întâi trebuie să învețe să scrie și să citească, tot la fel, ca să ajungă să semneze electronic, trebuie să învețe să utilizeze tehnologia (computer/laptop-uri/tablete/ telefoane + datele electronice + aplicațiile software aferente).

Semnătura olografă și semnătura electronică sunt strâns legate de contextul în care sunt create, context care diferă foarte mult între semnătura olografă și semnătura electronică. La fel și verificarea semnăturilor se face corelat cu respectivul context, deci în moduri total diferite.

Scopul utilizării semnăturilor este însă același: demonstrarea actului de voință al semnatarului informațiilor de pe hârtie, respectiv cele în format electronic.

Trebuie să fie semnătură electronică vizibilă ca și semnătura olografă?

Semnătura electronică NU trebuie să fie vizibilă pentru că nu ne putem baza pe simțuri pentru a verifica o semnătură electronică, așa cum nu ne putem bază pe simțuri pentru a descifra un document electronic. Documentul electronic și semnătura electronică sunt accesate prin intermediul unui sistem informatic.

Deci nu ne ajută prea mult dacă vedem o semnătură electronică. Ce ne ajută cu adevărat este că sistemul informatic (în care trebuie să avem încredere) ne „spune” că un document este semnat electronic și ne afișează informațiile cu privire la acea semnătură electronică, dacă este de încredere sau nu.

Experiența de lucru cu diverse organizații arată însă că este mai ușor procesul de adopție al semnăturii electronice dacă este și vizibilă.

De aceea formatul PDF, de exemplu permite adăugarea unei imagini care să indice existența unei semnături electronice (digitale, mai precis) ca în figura 2, semnătura electronică într-un document PDF.

Figura 2 Semnătura electronică într-un document PDF

Trebuie semnată electronic fiecare pagină a unui document electronic pdf?

NU, nu ajută cu nimic dacă semnăm electronic fiecare pagină a unui document pdf.

Dacă pe hârtie, scopul semnării fiecărei pagini este pentru a minimiza riscul ca ea să fie înlocuită cu o altă pagină, în format electronic acest lucru este imposibil dacă am semnat o singură dată electronic cu o semnătura electronică creată cu o tehnologie care îndeplinește cerințele unei semnături avansate, pentru că se îndeplinește condiția prevăzută la lit. d din art. 26 din Regulamentul 910/2014.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ GENEREZE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

3.4.1 POLITICA DE SEMNARE ELECTRONICĂ ÎNTR-O ORGANIZAȚIE

Așa cum am arătat în capitolul 3.1, o abordare pragmatică pentru o organizație este de a utiliza cât mai puține tehnologii și formate pentru a semna electronic documente.
Ar trebui să existe o politică privind semnarea electronică a documentelor în organizația respectivă. Această politică se referă la crearea semnăturii electronice precum și modul de validare a unei semnături electronice, în funcție de categoria de documente și fluxul de lucru existent în organizație, dacă este cazul. În Anexe este prezentat un model de politică de bază pentru semnătura electronică pentru o organizație (inspirată dintr-un exemplu publicat de SANS.org), referitor la documentele generate în interiorul organizației.
Evident, în funcție de complexitatea organizației, această politică va putea fi extinsă.

Un document exhaustiv cu privire la politicile de semnare îl reprezintă standardul ETSI TS 119 172-1
Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ GENEREZE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

3.4.2 FORMATUL PDF ȘI ADOBE ACROBAT READER DC

Cel mai „prietenos” format pentru documentele electronice, fiind foarte mult apropiat modului în care arată un document pe hârtie, este formatul PDF. În ultimii ani, formatul PDF a devenit și mai popular pentru următoarele motive:

▸ Cele mai utilizate editoare de documente (Word, Excel, Pages, OpenOffice etc) au o funcție de salvare a unui document în format PDF;

▸ Aplicația Adobe Acrobat Reader DC este o aplicație gratuită pentru „citirea” fișierelor PDF care în plus are și facilitatea de creare a semnăturilor electronice pe respectivele documente;

▸ Aplicația Adobe Acrobat Reader DC este integrată cu infrastructura de verificare a certificatelor digitale și ale mărcilor temporale calificate conform Regulamentului 910/2014.

Din aceste motive, minimal, într-o organizație se poate utiliza aplicația Adobe Acrobat Reader DC pentru semnarea documentelor electronice în format PDF și pentru verificarea documentelor PDF semnate.

Cu privire la semnătură electronică, Adobe Acrobat Reader DC permite următoarele:

1. Semnarea electronică a aceluiași document de către mai mulți semnatari - cu următoarele mențiuni:

a. Este posibilă aplicarea doar de semnături inseriate, cu următorul specific. Fiecare semnatar poate să adauge cu Adobe Acrobat Reader DC doar mențiuni/comentarii/adnotări, iar semnătura se aplică inclusiv peste acestea și peste tot ce conținea documentul înainte de adnotări, inclusiv semnăturile electronice existente deja; avantajul foarte mare este că se asigură posibilitatea de a se vizualiza exact ce versiune a documentului a semnat fiecare semnatar; este de asemenea importantă ordinea în care se semnează un document PDF;

b. Nu este posibilă semnarea doar a unei porțiuni dintr-un document PDF.

2. Aplicarea unei mărci temporale asociate semnăturii electronice; se poate configura utilizarea unei mărci temporale furnizate de un prestator de servicii de marcare temporală sau se poate aplica ora de pe computer-ul local, dar acest lucru nu este recomandat.

Aceasta deoarece momentul semnării este foarte important atunci când se validează o semnătură electronică, deoarece validarea se face raportat la momentul semnării.

3. Validarea semnăturilor electronice aplicate unui document cu posibilitatea de vizualizare a tuturor versiunilor dcoumentului anterior semnate.

4. Validarea semnăturilor calificate conform Regulamentului 910/2014 este implicită, în sensul că nu sunt necesare configurări suplimentare, dar trebuie să existe conexiune la Internet.

5. Pentru validarea semnăturilor necalificate sunt necesare configurări suplimentare, cum ar fi de exemplu configurarea unei anumite autorități de certificare ca fiind de încredere.
În anexe este prezentat în detaliu cum se semnează un fișier PDF utilizând Adobe Acrobat Reader DC.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ GENEREZE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

3.4.3 SISTEME DE MANAGEMENT AL DOCUMENTELOR ELECTRONICE. SISTEME DE MANAGEMENT AL FLUXURILOR DE AVIZARE/SEMNARE A DOCUMENTELOR ELECTRONICE

În mod ideal, o organizație ar trebui să aibă o politică de gestionare a documentelor electronice în organizație, care să implice inclusiv un sistem de management al documentelor electronice.

Acesta este util pentru gestionarea eficientă a documentelor electronice indiferent dacă sunt semnate sau nu.

Pentru eficientizarea fluxurilor de lucru cu documentele electronice, inclusiv al procesului de semnare când sunt mai mulți semnatari este foarte important să existe un sistem de de gestionare a fluxurile de avizare/semnare a documentelor electronice în organizație.

Cel mai simplu (dar foarte rudimentar) sistem de avizare de fluxuri este pe bază de email. Deci cu Adobe Acrobat Reader DC și sistemul de email se pot gestiona fluxuri de semnare electronică, dar pentru organizații mari, poate deveni ineficient.

Dacă există mai mult decât un sistem de email, adică organizația utilizează un sistem dedicat pentru scopul de management al fluxurilor de avizare, atunci:

- Există posibilitatea ca respectivul sistem să nu aibă integrată o funcție de semnătura electronică și atunci se utilizează respectivele sisteme pentru a ajunge la forma finală a documentului electronic; apoi acesta este extras din sistem, este semnat electronic de părțile semnatare folosind Adobe Acrobat Reader DC și apoi este introdus înapoi în sistem;

- Există posibilitatea ca respectivul sistem să aibă integrată funcția de semnătura electronică și atunci documentul se semnează prin intermediul acestui sistem.

3. MODALITĂȚI DE SEMNARE ELECTRONICĂ A DOCUMENTELOR

3.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ GENEREZE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

3.4.4 SEMNĂTURA LA DISTANȚĂ. INTEGRAREA CU SISTEMELE DE MANAGEMENT AL FLUXURILOR DE AVIZARE/SEMNARE AL DOCUMENTELOR ELECTRONICE

Ca urmare a prevederilor Regulamentului 910/2014 este acum posibil să se implementeze conceptul de semnătura electronică la distanță. În cazul acesteia, cheia privată nu mai stă local pe un token criptografic, dacă vorbim de semnătură calificată, ci cheia privată stă în cloud-ul prestatorului de servicii de încredere, care pune la dispoziție mecanisme sigure de acces exclusiv al semnatarului la cheia sa privată.

Acest concept are avantajul că permite o integrare mult mai facilă între sistemele de management de fluxuri de avizare (care nu știu nativ să semneze electronic) cu serviciile de semnătura la distanță, mult mai facil decât integrarea token-urilor criptografice, care vin cu restricția ca documentul care trebuie semnat să existe local, pe stația pe care este montat token-ul criptografic.

În cazul în care semnătura se creează cu astfel de sisteme integrat cu semnătura la distanță oferită de prestatorul de servicii de încredere, subliniem faptul că documentul semnat NU se creează cu Adobe Acrobat Reader ci cu acel sistem al organizației și organizația trebuie să se asigure că respectivul sistem generează documentul semnat în formatul corespunzător, respectând standardele specificate de Regulamentul 910/2014.

DE REȚINUT

▸ Înainte de a utiliza un sistem de semnătura la distanță pentru semnătură calificată, trebuie să vă asigurați ca acesta implementează/utilizează un Dispozitiv Calificat pentru crearea de semnături electronice (QSCD) publicat de Uniunea Europeană la adresa **https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds**;

▸ Implementarea, respectiv utilizarea acelui QSCD de către serviciul de semnare la distanță trebuie să se realizeze în conformitate cu politica de utilizare a acelui QSCD specificată pe site-ul mai sus-menționat.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.1 CERINȚELE REGULAMENTULUI 910/2014 CU PRIVIRE LA VERIFICAREA SEMNĂTURII CALIFICATE

Orice semnătura electronică trebuie verificată de către destinatar, inclusiv semnătura calificată trebuie să fie verificată/validată că într-adevăr este o semnătura calificată.

Regulamentul 910/2014 prevede la art. 32 cerințele pentru validarea semnăturilor electronice calificate:

"**(1)** Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:

(a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu **anexa I**;

(b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;

(c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar;

(d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului;

(e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;

(f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;

(g) integritatea datelor semnate nu a fost compromisă;

(h) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării.

(2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate."

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.2 CERINȚELE REGULAMENTULUI 910/2014 CU PRIVIRE LA VERIFICAREA SEMNĂTURII AVANSATE

Decizia de punere în aplicare a Regulamentului 1506/2015 specifică la art. 2, alin. (2) următoarele cerințe pentru verificarea unei semnături avansate:

(2) Posibilitățile de validare a semnăturilor:

(a) permit altor state membre să valideze online, gratuit și într-un mod care poate fi înțeles de vorbitorii altei limbi materne decât cea în cauză semnăturile electronice primite;

(b) sunt indicate în documentul semnat, în semnătura electronică sau în fișierul-container al documentului electronic; și (c) confirmă valabilitatea unei semnături electronice avansate, în următoarele condiții:

1. certificatul care stă la baza semnăturii electronice avansate era valabil la momentul semnării și, în cazul în care semnătura electronică avansată are la bază un certificat calificat, acesta din urmă era, la momentul semnării, un certificat calificat pentru semnături electronice conform cu **anexa I** din Regulamentul (UE) nr. 910/2014 și fusese emis de un prestator de servicii de încredere calificat;

2. datele de validare a semnăturilor corespund datelor furnizate de beneficiar;

3. setul unic de date care reprezintă semnatarul este furnizat corect beneficiarului;

4. utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;"

5. în cazul în care semnătura electronică avansată este creată printr-un dispozitiv de creare a semnăturilor electronice calificat, utilizarea unui astfel de dispozitiv este indicată clar beneficiarului;

6. integritatea datelor semnate nu a fost compromisă;

7. cerințele prevăzute la articolul 26 din Regulamentul (UE) nr. 910/2014 erau îndeplinite la momentul semnării;

8. sistemul utilizat pentru validarea semnăturii electronice avansate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate."

De precizat că punctele a și b sunt îndeplinite automat, dacă se utilizează formatele PDF, XML sau CMS, specificate de Regulament. Dacă se alege utilizarea altor formate, atunci trebuie asigurată și îndeplinirea acestor cerințe.

Mai mult decât atât, în preambulul Deciziei 1506/2015 se precizează: "(9), În vederea asigurării unor cerințe de validare comparabile și a sporirii încrederii în posibilitățile de validare oferite de statele membre pentru semnăturile sau sigiliile electronice în formate diferite de cele utilizate în mod curent, cerințele stabilite în prezenta decizie pentru instrumentele de validare se bazează pe cerințele de validare a semnăturilor și a sigiliilor electronice calificate, astfel cum sunt menționate la articolele 32 și 40 din Regulamentul (UE) nr. 910/2014."

Aceasta precizare arată foarte clar că spiritul Regulamentului 910/2014 este acela de a încuraja cât mai mult utilizarea semnăturii calificate, reglementată în detaliu de Regulament, atât din punct de vedere tehnic, cât și procedural.

Totodată însă, Regulamentul 910/2014 permite utilizare și de alte tehnologii, DAR numai cu condiția ca acestea să îndeplinească cerințele de validare a semnăturilor și sigiliilor calificate.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Verificarea unei semnături electronice este un pas obligatoriu pe care trebuie sa îl facă o parte interesata. Prin parte interesata înțelegem persoana fizică sau juridică ce invocă/se bazează pe respectiva semnătură electronică.

În **Tabelul 3** este prezentată o analiză comparativă între condițiile de verificare ale semnăturii calificate și ale semnăturilor avansate. Se observă faptul că pentru semnătura calificată și pentru semnătura avansată, cerințele de verificare/validare sunt practic aceleași, de fapt, condițiile de verificare ale semnăturii calificate sunt un caz concret de verificare al unei semnături avansate, ceea ce este explicabil, având în vedere că semnătură calificată specifică tehnologia utilizată pentru crearea ei.

În **Tabelul 4** am indicat pentru fiecare cerință ce informații are la dispoziție un software de validare a semnăturii pentru verificarea unei semnături calificate.

În **Tabelul 5** am indicat pentru fiecare cerință ce informații are la dispoziție un software de validare a semnăturii pentru verificarea unei semnături avansate. Se observă că, în cazul în care semnătura (potențial) avansată este creată utilizând tehnologia bazată pe certificat digital, este necesar ca partea interesată să se asigure că respectivul certificat ne-calificat a fost emis astfel încât, în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată.

Practic, partea interesată trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat, doar că, spre deosebire de situația certificatului calificat, partea interesată este pe cont propriu.

Prin condiții similare înțelegem inclusiv condițiile cu privire la identificarea persoanei în vederea emiterii certificatului specificate de art. 24, alin. 1 din Regulamentul 910/2014:

„**(1)** Atunci când emite un certificat calificat pentru un serviciu de încredere, un prestator de servicii de încredere calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat.

Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în conformitate cu dreptul intern:

(a) de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau

(b) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice și care îndeplinesc cerințele stabilite la articolul 8 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”; sau

(c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu dispozițiile de la litera (a) sau (b); sau

(d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică. Nivelul de asigurare echivalent este confirmat de un organism de evaluare a conformității.”

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Când va trebui să invoce semnătura avansată, partea interesată va trebuie să aibă capabilitatea de a dovedi singură îndeplinirea condițiilor din **Tabelul 5**, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat (acesta fiind obligat prin Regulamentul 910/2014 să acorde acest suport), iar în cazul culpei acestuia, semnatarul este despăgubit.

De asemenea, în cazul utilizării unui certificat necalificat, este necesar ca software-ul de validare al semnăturii să fie configurat pentru a considera de încredere respectivul certificat. Această configurare depinde de software-ul de validare.

În cazul în care se utilizează un software de validare de tip COTS (de exemplu Adobe Acrobat Reader DC), acestea în general sunt pre-configurate să valideze automat un certificat în raport cu lista de încredere EUTL de la nivelul Uniunii Europene, ceea ce aduce avantaje pentru utilizatori, în cazul în care trebuie să valideze o semnătură bazată pe certificat calificat.

Validarea unui certificat necalificat la software-urile de tip COTS presupun că utilizatorul stabilește el Autoritatea de Certificare de încredere - dar aici trebuie foarte multă atenție, pentru că există riscul ca, printr-o astfel de configurare, un utilizator mai puțin instruit să configureze ca fiind de încredere o altă Autoritate de certificare decât cea corectă.

De exemplu poate alege de încredere „Autoritatea de Certificare a Ministerului de Interne”, când de fapt autoritatea corectă este „Autoritatea de Certificare a Ministerului Administrației și Internelor”. Consecința este dezastruoasă pentru că un destinatar poate valida astfel un document practic fals.

În cazul în care tehnologia utilizată pentru crearea semnăturii avansate nu este bazată pe certificat digital, atunci trebuie să există un software de validare a semnăturii specific acelei tehnologii și cerințele de validare trebuie îndeplinite identificând în cadrul acelei tehnologii elementele de referință specificate în condițiile de validare.

În Anexe, am prezentat în detaliu fiecare pas de validare a unei semnături calificate, respectiv avansate, utilizând Adobe Acrobat Reader DC.

Concluzia este că procesul de validare este cel mai facil (deci mai ieftin) și mai sigur pentru o parte interesată, în sensul că este bine definit, în cazul semnăturii electronice calificate, tocmai pentru 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, inclusiv prevede obligativitatea prestatorului calificat de a acorda suport semnatarului și despăgubiri în cazul în care a fost o culpă a acestuia.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 3. Comparație între condițiile de validare semnătură calificată vs semnătură avansată

VERIFICAREA SEMNĂTURII CALIFICATE art. 32 Regulamentul 910/2014	VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015
	(2) Posibilitățile de validare a semnăturilor: **(a)** permit altor state membre să valideze online, gratuit și într-un mod care poate fi înțeles de vorbitorii altei limbi materne decât cea în cauză semnăturile electronice primite; **(b)** sunt indicate în documentul semnat, în semnătura electronică sau în fișierul-container al documentului electronic;
(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:	**c)** confirmă valabilitatea unei semnături electronice avansate, în următoarele condiții:
(a) certificatul care stă la bază semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu **anexa I**; **(b)** certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;	**1.** certificatul care stă la baza semnăturii electronice avansate era valabil la momentul semnării și, în cazul în care semnătura electronică avansată are la bază un certificat calificat, acesta din urmă era, la momentul semnării, un certificat calificat pentru semnături electronice conform cu **anexa I** din Regulamentul (UE) nr. 910/2014 și fusese emis de un prestator de servicii de încredere calificat;
(c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar;	**2.** datele de validare a semnăturilor corespund datelor furnizate de beneficiar;
(d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului;	**3.** setul unic de date care reprezintă semnatarul este furnizat corect beneficiarului;
(e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;	**4.** utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;
(f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;	**5.** în cazul în care semnătura electronică avansată este creată printr-un dispozitiv de creare a semnăturilor electronice calificat, utilizarea unui astfel de dispozitiv este indicată clar beneficiarului;
(g) integritatea datelor semnate nu a fost compromisă;	**6.** integritatea datelor semnate nu a fost compromisă;
(h) cerințele prevăzute la articolul 26 **au fost îndeplinite la momentul semnării.**	**7.** cerințele prevăzute la articolul 26 din Regulamentul (UE) nr. 910/2014 **erau îndeplinite la momentul semnării**;
(2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.	**8.** sistemul utilizat pentru validarea semnăturii electronice avansate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 4. Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături calificate

VERIFICAREA SEMNĂTURII CALIFICATE art. 32 Regulamentul 910/2014	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:	
(a) certificatul care stă la bază semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu anexa I;	Software-ul de verificare a semnăturii identifică faptul că certificatul utilizat este emis de un prestator calificat de servicii de încredere aflat pe lista de încredere EUTL publicată la nivelul Uniunii Europene. Conform standardelor ETSI, certificatul calificat obligatoriu trebuie să conțină o extensie care indică faptul că este un certificat emis în conformitate cu Anexa 1.
(b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;	În plus, certificatul conține informații cu privire la locația de unde software-ul de verificare a semnăturii își poate lua informațiile cu privire la valabilitatea certificatului la momentul semnării. Momentul semnării este foate important, de aceea este bine ca el să fie certificat printr-o marcă temporală emisă de un prestator calificat de servicii de încredere.
(c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar;	Formatele de semnătură PDF, CMS, XML includ certificatul corepunzator cheii de semnare și software-ul de verificare a semnăturii trebuie să utilizeze respectivul certificat pentru verificarea cu success a semnăturii.
(d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului;	Formatului certificatului digital păstrează setul unic de date care reprezintă semnatarul, în secțiunea Subject. Corectitudinea acestor date este verificată de Prestatorul de servicii de încredere calificat, înainte de a emite certificatul. Software-ul de validare trebuie să afișeze corect această Secțiune cu toate componentele sale.
(e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;	Formatul certificatului digital indică în mod clar existența unui pseudonim și software-ul de validare a semnăturii trebuie să poată indica prezența acestuia în certificat.
(f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;	Conform standardelor ETSI, în cazul în care cheia privată corespunzătoare certificatului calificat rezidă pe un dispozitiv de creare a semnăturilor electronice calificat, certificatul calificat obligatoriu trebuie să conțină o extensie care indică acest fapt.
(g) integritatea datelor semnate nu a fost compromisă;	Integritatea datelor se verifică implicit prin verificarea semnăturii digitale. Dacă aceasta nu se validează, înseamnă că integritatea datelor a fost compromisă.
(h) cerințele prevăzute la articolul 26 a**u fost îndeplinite la momentul semnării.**	A se vedea **Tabelul 1**

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 1 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
(2) Posibilitățile de validare a semnăturilor: **(a)** permit altor state membre să valideze online, gratuit și într-un mod care poate fi înțeles de vorbitorii altei limbi materne decât cea în cauză semnăturile electronice primite; **(b)** sunt indicate în documentul semnat, în semnătura electronică sau în fișierul-container al documentului electronic;	În cazul în care tehnologia utilizată pentru crearea semnăturii avansate nu este bazată pe formatele PDF, CMS sau XML prevăzute de Regulament, este obligatoriu ca tehnologia utilizată să asigure îndeplinirea acestor condiții și să pună la dispoziție gratuit posibilitatea de validare.
(c) confirmă valabilitatea unei semnături electronice avansate, în următoarele condiții:	

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 2 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
1. certificatul care stă la baza semnăturii electronice avansate era valabil la momentul semnării și, în cazul în care semnătura electronică avansată are la bază un certificat calificat, acesta din urmă era, la momentul semnării, un certificat calificat pentru semnături electronice conform cu anexa I din Regulamentul (UE) nr. 910/2014 și fusese emis de un prestator de servicii de încredere calificat;	Software-ul de verificare a semnăturii identifică faptul că certificatul utilizat este emis de un prestator calificat de servicii de încredere aflat pe lista de încredere EUTL publicată la nivelul Uniunii Europene. Conform standardelor ETSI, certificatul calificat obligatoriu trebuie să conțină o extensie care indică faptul că este un certificat emis în conformitate cu Anexa 1. În plus, certificatul conține informații cu privire la locația de unde software-ul de verificare a semnăturii își poate lua informațiile cu privire la valabilitatea certificatului la momentul semnării. Momentul semnării este foate important, de aceea este bine ca el să fie certificat printr-o marca temporală emisă de un prestator calificat de servicii de încredere. **DE REȚINUT** În cazul în care certificatul nu este calificat, software-ul de validare al semnăturii trebuie configurat suplimentar pentru a considera de încredere Autoritatea care a emis respectivul certificat. Această acțiune este una foarte sensibilă și trebuie ca beneficiarul să fie foarte bine atenționat cum să se asigure că se referă într-adevăr la o Autoritate de certificare de încredere. De asemenea, partea interesată trebuie să se asigure că respectivul certificat ne-calificat a fost emis astfel încât în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată. Practic, partea interesată trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat (inclusiv cele pentru identificare, menționate la art.24 alin 1 din Regulamentul 910/2014), doar că, spre deosebire de situația certificatului calificat, partea interesată este pe cont propriu. Și dacă ulterior va trebui să invoce semnătura avansată, va trebuie să aibă capabilitatea de a dovedi singură îndeplinirea condițiilor din acest tabel, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat, iar în cazul culpei acestuia, semnatarul este despăgubit.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 3 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
2. datele de validare a semnăturilor corespund datelor furnizate de beneficiar;	Formatele de semnătura PDF, CMS, XML include certificatul corepunzator cheii de semnare și software-ul de verificare a semnăturii trebuie să utilizeze respectivul certificat pentru validarea semnăturii. Datele de validare a semnăturilor sunt reprezentate de cheia publică, inclusă în certificatul digital. **ATENȚIE** În cazul în care certificatul nu este calificat, software-ul de validare al semnăturii trebuie configurat suplimentar pentru a considera de încredere Autoritatea care a emis respectivul certificat. Această acțiune este una foarte sensibilă și trebuie ca beneficiarul să fie foarte bine atenționat cum să se asigure că se referă într-adevăr la o Autoritate de certificare de încredere. De asemenea, partea interesată trebuie să se asigure că respectivul certificat ne-calificat a fost emis astfel încât în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată. Practic, partea interesată trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat (inclusiv cele pentru identificare, menționate la art.24 alin1 din Regulamentul 910/2014), doar că, spre deosebire de situația certificatului calificat, partea interesată este pe cont propriu. Și dacă ulterior va trebui să invoce semnătura avansată, va trebuie să aibă capabilitatea de a dovedi singură îndeplinirea condițiilor din acest tabel, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat, iar în cazul culpei acestuia, semnatarul este despăgubit. **DE REȚINUT** În cazul în care nu se utilizează tehnologia pe bază de semnătură digitală, tehnologia utilizată trebuie să definească clar care sunt datele de validare a semnăturilor.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 4 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
3. setul unic de date care reprezintă semnatarul este furnizat corect beneficiarului;	Formatulul certificatului digital păstrează setul unic de date care reprezintă semnatarul, în secțiunea Subject. Software-ul de validare trebuie să afișeze corect această secțiune cu toate componentele sale. **ATENȚIE** În cazul în care certificatul nu este calificat, software-ul de validare al semnăturii trebuie configurat suplimentar pentru a considera de încredere Autoritatea care a emis respectivul certificat. Această acțiune este una foarte sensibilă și trebuie ca beneficiarul să fie foarte bine atenționat cum să se asigure că se referă într-adevăr la o Autoritate de certificare de încredere. De asemenea, semnatarul trebuie să se asigure că respectivul certificat ne-calificat a fost emis astfel încât în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată. Practic, semnatarul trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat, doar că, spre deosebire de situația certificatului calificat, semnatarul este pe cont propriu. Și dacă ulterior va trebui să invoce semnătura avansată, va trebui să aibă capabilitatea de a dovedi singur îndeplinirea condițiilor din acest tabel, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat, iar în cazul culpei acestuia, semnatarul este despăgubit. **DE REȚINUT** În cazul în care nu se utilizează tehnologia pe bază de semnătură digitală, tehnologia utilizată trebuie să definească clar modul de reprezentare a setului unic de date care reprezintă semnatarul.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 5 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
4. utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;	Formatul certificatului digital indică în mod clar existența unui pseudonim și software-ul de validare a semnăturii trebuie să poată indică prezența acestuia în certificat. **ATENȚIE** În cazul în care certificatul nu este calificat, software-ul de validare al semnăturii trebuie configurat suplimentar pentru a considera de încredere Autoritatea care a emis respectivul certificat. Această acțiune este una foarte sensibilă și trebuie ca beneficiarul să fie foarte bine atenționat cum să se asigure că se referă într-adevăr la o Autoritate de certificare de încredere. De asemenea, semnatarul trebuie să se asigure că respectivul certificat ne-calificat a fost emis astfel încât în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată. Practic, semnatarul trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat, doar că, spre deosebire de situația certificatului calificat, semnatarul este pe cont propriu. Și dacă ulterior va trebui să invoce semnătura avansată, va trebui să aibă capabilitatea de a dovedi singur îndeplinirea condițiilor din acest tabel, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat, iar în cazul culpei acestuia, semnatarul este despăgubit. **DE REȚINUT** În cazul în care nu se utilizează tehnologia pe bază de semnătură digitală, tehnologia utilizată trebuie să definească modul de utilizare al pseudonimelor.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.3 VERIFICAREA SEMNĂTURII AVANSATE VS VERIFICAREA SEMNĂTURII CALIFICATE

Tabel 5 (partea 6 din 6). Modalitatea de îndeplinire a cerințelor pentru verificarea unei semnături avansate

VERIFICAREA SEMNĂTURII AVANSATE art. 2 alin. (2) din Decizia de punere în aplicare 1506/2015	MODALITATEA DE ÎNDEPLINIRE A CERINȚELOR
5. în cazul în care semnătura electronică avansată este creată printr-un dispozitiv de creare a semnăturilor electronice calificat, utilizarea unui astfel de dispozitiv este indicată clar beneficiarului;	Conform standardelor ETSI, structura certificatului permite o extensie care indică aspectul potrivit căruia cheia privată corespunzătoare certificatului rezidă pe un dispozitiv de creare a semnăturilor electronice calificat. **ATENȚIE** În cazul în care certificatul nu este calificat, software-ul de validare al semnăturii trebuie configurat suplimentar pentru a considera de încredere Autoritatea care a emis respectivul certificat. Această acțiune este una foarte sensibilă și trebuie ca beneficiarul să fie foarte bine atenționat cum să se asigure că se referă într-adevăr la o Autoritate de certificare de încredere. De asemenea, semnatarul trebuie să se asigure că respectivul certificat ne-calificat a fost emis astfel încât în baza acestuia să poată dovedi ulterior că, la momentul semnării, semnătura avansată creată cu acel certificat chiar era avansată. Practic, semnatarul trebuie să se asigure că acel certificat ne-calificat a fost emis în condiții similare cu cele ale unui certificat calificat, doar că, spre deosebire de situația certificatului calificat, semnatarul este pe cont propriu. Și dacă ulterior va trebui să invoce semnătura avansată, va trebui să aibă capabilitatea de a dovedi singur îndeplinirea condițiilor din acest tabel, pe când, în cazul certificatului calificat, dovedirea o realizează cu suportul prestatorului calificat, iar în cazul culpei acestuia, semnatarul este despăgubit.
6. integritatea datelor semnate nu a fost compromisă;	Integritatea datelor se verifică implicit prin validarea semnăturii digitale. Dacă aceasta nu se valideaza, în condițiile în care punctul c) este îndeplinit, înseamnă că integritatea datelor a fost compromisă. **DE REȚINUT** În cazul în care nu se utilizează tehnologia pe bază de semnătură digitală, tehnologia utilizată trebuie să definească clar modalitatea în care se verifică integritatea datelor semnate.
7. cerințele prevăzute la articolul 26 din Regulamentul (UE) nr. 910/2014 erau îndeplinite la momentul semnării;	A se vedea **Tabelul 2**.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ SOLICITE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

Prima recomandare fundamentală este de a nu lua decizii ca cele ce urmează:

„Organizația noastră oferă un serviciu online care necesită semnătură electronică" sau „Organizația noastră oferă un serviciu online care necesită semnătură electronică avansată", pentru că, așa cum am arătat în capitolul 1, „semnătura electronică", respectiv „semnătura electronică avansată" sunt concepte care pot fi create printr-o multitudine de tehnologii.

Există o legătură biunivocă între tehnologia cu care este creată și cea cu care se verifică o semnatură electronică, ceea ce înseamnă că organizația care ar lua deciziile de mai sus, ar trebui să aibă implementate mecanisme de verificare pentru orice astfel de tehnologie, ceea ce, evident nu este posibil.

Deciziile trebuie să se refere la aspecte ca: „Organizația noastră oferă un serviciu online care necesită semnătură electronică/semnătură electronică avansată creată cu tehnologiile X/Y/Z etc.", sau „Organizația noastră oferă un serviciu online care necesită semnătură electronică calificată", pentru că semnătura calificată specifică, prin definiția ei, tehnologia cu care este creată.

Alegerea tipului/tipurilor de tehnologii pentru crearea semnăturii electronice pe care o organizație decide să le solicite pentru documentele electronice care provin din afara organizației ar trebui să se facă ținând cont de următoarele criterii:

- ușurința în utilizare de către semnatar, incluzând aici și cât de simplu este pentru semnatar să-și procure și instaleze respectiva tehnologie;

- costul suportat de semnatar pentru a-și procura respectiva tehnologie;

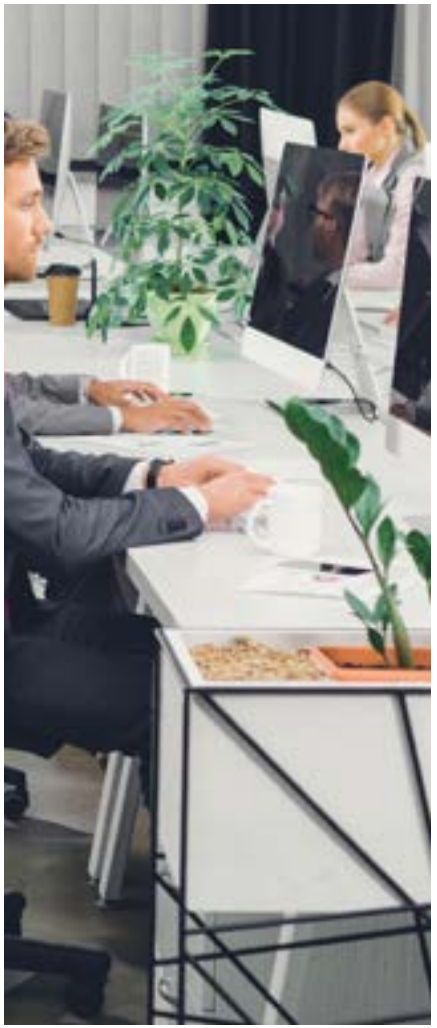
- costul suportat de organizația destinatar pentru a integra tehnologia

- pentru verificarea semnăturii electronice:

  - costurile suportate de organizație pentru a integra tehnologia de verificare a faptului că într-adevăr o semnătură avansată îndeplinea, la momentul semnării, cerințele așa cum le-am detaliat în capitolul 4.3, **Tabelul 5**, în cazul semnăturii avansate;

  - costurile suportate de organizație pentru a integra tehnologia de verificare a faptului că într-adevăr o semnătura calificată îndeplinea, la momentul semnării, cerințele pentru semnătura calificată, așa cum le-am detaliat în capitolul 4.3, **Tabelul 4**

- cât de mare este riscul pe care și-l poate asuma organizația destinatar ca documentul semnat electronic să nu producă efectele juridice așteptate, cu alte cuvinte riscul ca organizația să nu poată dovedi că acel document este actul de voință al semnatarului - de aici rezultă că o organizație poate decide să utilizeze diverse tehnologii pentru diverse tipuri de documente.

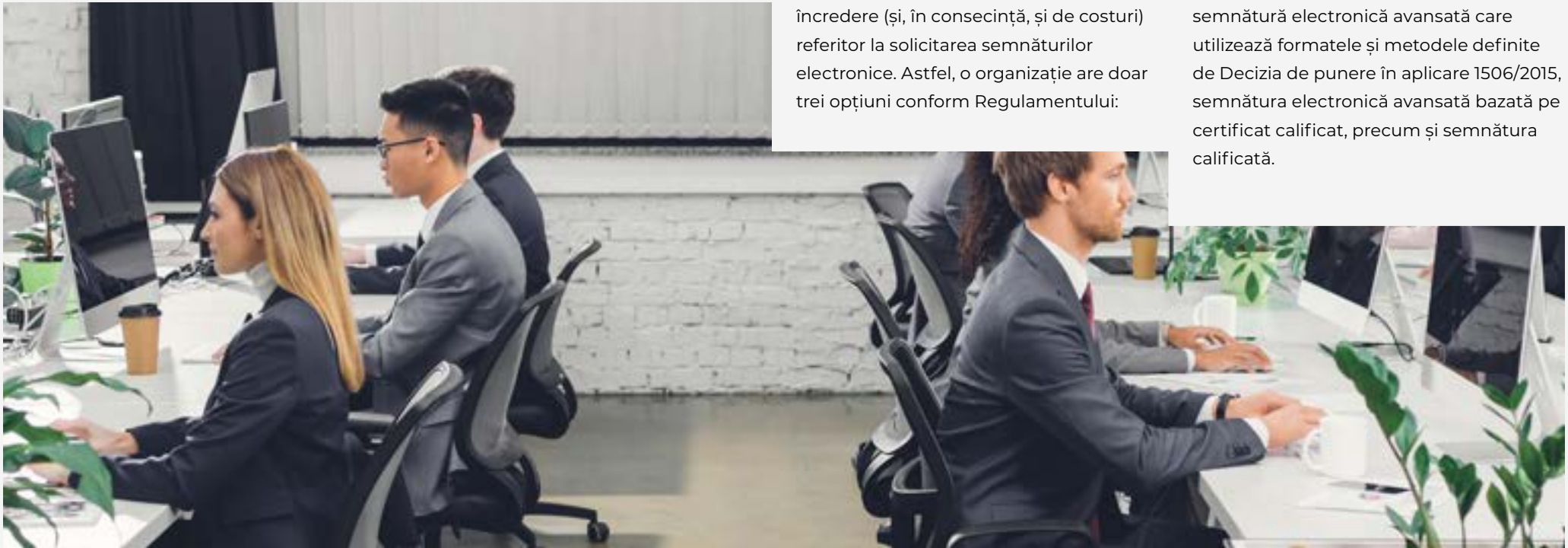


4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ SOLICITE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

În **Tabelul 6** am încercat să dăm estimări pentru aceste criterii pentru câteva tehnologii de creare de semnătură electronică, folosind scara (EXTREM DE MIC / FOARTE MIC / MIC / MEDIU / MARE / FOARTE MARE / EXTREM DE MARE). Indicatorii sunt prezentați strict pentru comparare. O evaluare precisă nu poate fi realizată fără analiza detaliată a fiecărei tehnologii (mecanismele tehnice și procedurale).

Pentru autoritățile și instituțiile publice, am realizat **Tabelul 7**, în care costul acestora devine mult mai mare pentru situația în care respectiva organizație decidesă solicite tehnologii pentru creare de semnătură avansată, pentru că este obligată să implementeze cerințele art. 27 din Regulamentul 910/2014, așa cum am arătat în capitolul 3.1.



DE REȚINUT

Solicitarea unei anumite tehnologii de creare a semnăturii electronice avansate implică asumarea de costuri pentru a verifica că respectiva semnătură îndeplinește cerințele descrise în capitolele anterioare.

Pentru organizațiile/instituțiile publice, Regulamentul 910/2014, prin articolul 27, stabilește o ierarhie a nivelului de încredere (și, în consecință, și de costuri) referitor la solicitarea semnăturilor electronice. Astfel, o organizație are doar trei opțiuni conform Regulamentului:

- Prima opțiune este să solicite doar semnătură calificată;

- A doua opțiune este să solicite doar semnătura electronică avansată bazată pe certificat calificat și semnătură calificată;

- A treia opțiune este să solicite orice semnătură electronică avansată care utilizează formatele și metodele definite de Decizia de punere în aplicare 1506/2015, caz în care trebuie să accepte orice altă semnătură electronică avansată care utilizează formatele și metodele definite de Decizia de punere în aplicare 1506/2015, semnătura electronică avansată bazată pe certificat calificat, precum și semnătura calificată.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ SOLICITE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

Tabel 6. Analiza comparativă a criteriilor de alegere de către o organizație a tipurilor de tehnologii de creare de semnătură electronică pe care să le solicite unui terț din afară

CRITERII → **TEHNOLOGII solicitate de organizație pentru creare de semnătură electronică ↓**	**Ușurința în utilizare de către semnatar**	**Costul pentru semnatar**	**Costul pentru organizația destinatar**	**Riscul ca organizația destinatar/transmițătorul să nu poată dovedi că acel document este actul de voință al semnatarului**
Semnătură electronică realizată prin specificarea numelui la sfârșitul documentului	EXTREM DE MARE	EXTREM DE MIC	FOARTE MIC	A se vedea **capitolul 5**
Semnătură electronică realizată prin utilizarea unui scan al semnăturii olografe	FOARTE MARE	FOARTE MIC	MIC-MEDIU	A se vedea **capitolul 5**
Semnătură electronică avansată bazată pe certificat digital necalificat emis de organizația destinatar	MEDIE-MARE	MIC	MARE-FOARTE MARE	A se vedea **capitolul 5**
Semnătură electronică avansată bazată pe certificat digital necalificat emis de un terț	MEDIE-MARE	MEDIU	MARE	A se vedea **capitolul 5**
Semnătură electronică avansată conform art. 5 alin.(3) OUG 38	MEDIE-MARE	MEDIU-MIC	MARE-FOARTE MARE	A se vedea **capitolul 5**
Semnătură electronică avansată bazată pe certificat digital calificat	MEDIE-MARE	MEDIU	MEDIU-MIC	A se vedea **capitolul 5**
Semnătură electronică calificată bazată pe token criptografic	MEDIE	MEDIU-MARE	MEDIU-MIC	A se vedea **capitolul 5**
Semnătură electronică calificată la distanță	MEDIE-MARE	MEDIU-MIC	MEDIU-MIC	A se vedea **capitolul 5**

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.4 RECOMANDĂRI PENTRU O ORGANIZAȚIE CARE DECIDE SĂ SOLICITE DOCUMENTE ÎN FORMĂ ELECTRONICĂ, SEMNATE ELECTRONIC

Tabel 7. Analiza comparativă a criteriilor de alegere de către o autoritate/instituție publică a tipurilor de tehnologii de creare de semnătură electronică pe care să le solicite în cadrul serviciilor online prestate de respectivele autorități/instituții

CRITERII → TEHNOLOGII solicitate de organizație pentru creare de semnătură electronică ↓	Ușurința în utilizare de către semnatar	Costul pentru semnatar	Costul pentru organizația destinatar	Riscul ca organizația destinatar/ transmițătorul să nu poată dovedi că acel document este actul de voință al semnatarului
Semnătură electronica avansată bazată pe certificat digital necalificat emis de organizația destinatar	MEDIE-MARE	MIC	EXTREM DE MARE*	A se vedea **capitolul 5**
Semnătură electronica avansată bazata pe certificat digital necalificat emis de un terț	MEDIE-MARE	MEDIU	EXTREM DE MARE*	A se vedea **capitolul 5**
Semnătură electronică avansată conform art. 5 alin.3 OUG 38	MEDIE-MARE	MEDIU-MIC	EXTREM DE MARE*	A se vedea **capitolul 5**
Semnătură electronica avansată bazată pe certificat digital calificat	MEDIE- MARE	MEDIU	MEDIU-MIC	A se vedea **capitolul 5**
Semnătură electronica calificată bazata pe token criptografic	MEDIE	MEDIU-MARE	MEDIU-MIC	A se vedea **capitolul 5**
Semnătură electronică calificată la distanță	MARE-MEDIU	MEDIU-MIC	MEDIU-MIC	A se vedea **capitolul 5**

* Este dată de suma costurilor cu sistemele de verificare a semnăturii pentru orice semnătură avansată care respectă formatele și metodele definite în Decizia de punere în aplicare 1506/2015, precum și costurile cu sisteme de verificare a semnăturii pentru semnătura avansată bazată pe certificat calificat și pentru semnătura calificată.

4. MODALITĂȚI DE VERIFICARE A SEMNĂTURILOR ELECTRONICE

4.5 SEMNĂTURA ELECTRONICĂ AVANSATĂ ÎN CONTEXTUL OUG 38/2020

OUG 38/2020 definește, la art. 5 alin. (3): Înscrisurile semnate cu semnătură electronică avansată, care sunt transmise prin utilizarea unor mecanisme de autentificare de nivel substanțial sau ridicat, sunt asimilate, în ceea ce privește condițiile și efectele lor, cu înscrisurile sub semnătură privată.

Formularea de la art. 5 alin (3) nu stabilește modalitatea de verificare a semnăturii avansate. De asemenea, introduce un termen nou, „mecanisme de autentificare de nivel substanțial sau ridicat", care nu este definit de Regulamentul 910/2014 și nici de textul actului normati

Gradul de complexitate al verificării semnăturii avansate crește în contextul art.5 alin. (3). Trebuie verificat și mecanismul de transmitere a înscrisurilor semnate cu semnătură avansată și, mai mult, trebuie ca mecanismul tehnic folosit pentru semnătura avansată să asigure păstrarea informațiilor cu privire la respectivul mecanism de transmitere, ceea ce nu este prevăzut de standardele menționate de Regulamentul 910/2014, acest lucru ducând cu siguranță la o lipsă de interoperabilitate între sisteme.

În plus, organizația/instituția publică, în cazul în care decide să recunoască (sa proceseze tehnic) semnătură avansată specificată la art.5 alin (3), este obligata de art.27 din Regulamentul 910/2014, să aloce costuri pentru recunoaște (procesa tehnic)

- orice altă semnătură electronică avansată care utilizează formatele și metodele definite de Decizia de punere în aplicare 1506/2015, și

- semnătură electronică avansată bazată pe certificat calificat, precum și

- semnătură calificată,

așa cum am arătat în secțiunile anterioare.

OUG
38 / 2020

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.1 EFECTELE JURIDICE ALE SEMNĂTURILOR ELECTRONICE CONFORM REGULAMENTULUI 910/2014

Art. 25 din Regulamentul 910/2014 prevede următoarele: "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.

(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 membre."

DE REȚINUT

▸ 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, asa cum am arătat în capitolul 1.1.3.;

▸ Conform Regulamentului 910/2014, nici unei semnaturi 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.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.2 CONSIDERAȚII ASUPRA DIFERENȚEI ÎNTRE EFECTUL JURIDIC AL UNEI SEMNĂTURI ELECTRONICE AVANSATE ȘI SOLICITAREA ȘI RECUNOAȘTEREA SEMNĂTURILOR AVANSATE ÎN CONTEXTUL REGULAMENTULUI 910/2014

În continure, reluăm art. 27 alin (1), (2) si (3) din Regulamentul 910/2014:
“Articolul 27.

Semnăturile electronice în cadrul serviciilor publice

(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 întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

(2) În cazul în care un stat membru **solicită o semnătură electronică avansată bazată pe un certificat calificat 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** bazate pe un certificat calificat și semnăturile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

(3) 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.**”

Analizând cuvintele subliniate din acest articol, concluzia pe care o tragem este că noțiunile „solicită” și „recunoaște” au legătură exclusiv cu capabilitățile tehnice ale serviciului online, prestat de către un organism public, de a procesa tehnologiile pentru semnătură electronică.

Un organism public (autoritate/instituție publică), atunci când pune la dispoziție un serviciu online, conform art. 27 trebuie să stabilească, în specificațiile tehnice ale respectivului serviciu online, tehnologia/ tehnologiile pe care serviciul public online respectiv le solicită pentru semnătura electronică, pentru că nu este posibil din punct de vedere tehnic să solicite orice tehnologie, având un buget limitat, așa cum am arătat în capitolul precedent.

Dar, totodată, în cadrul specificațiilor tehnice ale respectivului serviciu online, organismul public este obligat să prevadă mecanismele tehnice necesare recunoașterii acelor tehnologii de semnătură electronică pe care este obligat să le recunoască, conform art. 27.

Astfel, un organism public are doar trei opțiuni conform art.27, cand stabilește cerințele tehnice pentru un serviciu online:

Prima opțiune este să solicite și să recunoască (proceseze tehnic) doar semnătura calificată;

A doua opțiune este să solicite și să recunoască (proceseze tehnic) doar semnătura electronică avansată bazată pe certificat calificat și semnătura calificată;

A treia opțiune este să solicite o anumită tehnologie pentru semnătura electronică avansată care utilizează formatele și metodele definite de Decizia de punere în aplicare 1506/2015, caz în care trebuie să recunoască (proceseze tehnic) orice altă semnătură electronică avansată care utilizeaza formatele și metodele definite de Decizia de punere în aplicare 1506/2015, semnătura electronică avansată bazată pe certificat calificat, precum și semnătura calificată.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.2 CONSIDERAȚII ASUPRA DIFERENȚEI ÎNTRE EFECTUL JURIDIC AL UNEI SEMNĂTURI ELECTRONICE AVANSATE ȘI SOLICITAREA ȘI RECUNOAȘTEREA SEMNĂTURILOR AVANSATE ÎN CONTEXTUL REGULAMENTULUI 910/2014

Așadar, art. 27 nu aduce nimic în plus cu privire la efectul juridic al semnăturilor electronice, față de articolul 25, contextul articolului 27 fiind unul pur tehnic și în legătură directă cu serviciul public online pe care un organism public îl pune la dispoziție.

Din punct de vedere al efectului juridic, în contextul Regulamentului 910/2014, semnătura calificată aplicată documentelor primite prin intermediul respectivului serviciu pubic online, are același efect juridic cu semnătura olografă, iar celelalte semnături electronice nu pot fi respinse ca probe în procedurile judiciare.

DE REȚINUT

Dacă există însă un context legal specific sau de reglementare, în afara Regulamentului, cu privire la serviciul public online furnizat de un organism public care prevede un anumit efect juridic pentru o semnătură electronică avansată, atunci acel efect juridic este același atât pentru orice altă semnătură electronică avansată care utilizează formatele și metodele definite de Decizia de punere în aplicare 1506/2015, pentru semnătura electronică avansată bazată pe certificat calificat, precum și pentru semnătura calificată.

Articolul 27 din Regulamentul 910/2014 nu se referă la efectul juridic al semnăturilor electronice.

Este foarte important de subliniat că Regulamentul 910/2014 nu prevede obligativitatea ca un organism public să furnizeze un serviciu public online care să accepte semnătura electronică.

În cazul în care, însă, un organism public alege să furnizeze un serviciu public online care să accepte semnătură electronică, atunci organismul este OBLIGAT ca respectivul serviciu public online să recunoască, adică să proceseze din punct de vedere tehnic, minim semnătura electronică calificată, indiferent de ce efect juridic stabilește respectivul organism public sau legiuitorul sau o autoritate de reglementare, pentru alte tipuri de semnătură electronică decât cea calificată.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.3 POSIBILE SCENARII CU PRIVIRE LA UTILIZAREA SEMNĂTURII ELECTRONICE ȘI LA EFECTUL JURIDIC AL ACESTEIA

5.3.1 SCENARIUL ÎN CARE O ORGANIZAȚIE NU ARE CAPABILITATEA TEHNICĂ DE A RECUNOAȘTE (NU POATE PROCESA TEHNIC) O SEMNĂTURĂ ELECTRONICĂ AVANSATĂ CARE ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014

Plecăm de la premiza că o organizație stabilește că poate procesa tehnic semnătura electronică realizată doar cu anumite tehnologii pentru semnătură electronică (dar respectând prevederile art. 27 din Regulamentul 910/2014, dacă este vorba de un organism public).

Întrebarea este ce se întâmplă dacă NU are capabilitatea de a recunoaște (nu poate procesa tehnic) o semnătură electronică avansată care are un anumit efect juridic stabilit în afara Regulamentului 910/2014 și îi este invocat un document semnat astfel?

Variantele posibile sunt:

▸ organizația să nu accepte documentul electronic respectiv și transmițătorul nu are altă cale decât să invoce în instanță respectivul document, unde trebuie să facă (pe cheltuiala transmițătorului, a se revedea capitolul 4.3) dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În cazul în care dovedesc toate aceste aspecte, organizația este obligată să accepte respectivul document, conform efectului juridic stabilit pentru acea semnătură, cu implicațiile prevăzute de legislație asupra documentului electronic semnat cu acea semnătură;

▸ organizația să solicite transmițătorului (pe cheltuiala lui, a se revedea capitolul 4.3), dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În acest caz, riscul pentru organizație este foarte mare, pentru că, ulterior transmițătorul poate nega că a semnat respectivul document și trecem în scenariul următor, unde vom vedea că organizația trebuie să dovedească (pe cheltuiala sa, a organizației) verificarea respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.3 POSIBILE SCENARII CU PRIVIRE LA UTILIZAREA SEMNĂTURII ELECTRONICE ȘI LA EFECTUL JURIDIC AL ACESTEIA

5.3.2 SCENARIUL ÎN CARE O ORGANIZAȚIE PRIMEȘTE UN DOCUMENT SEMNAT ELECTRONIC CU O TEHNOLOGIE PE CARE O RECUNOAȘTE ȘI CARE ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014, DAR ULTERIOR, TRANSMIȚĂTORUL NEAGĂ CĂ A SEMNAT RESPECTIVUL DOCUMENT

În acest caz, organizația trebuie să invoce în instanță respectiva semnătură electronică și să facă (pe cheltuiala sa, a organizației, a se revedea capitolul 4.3) dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În cazul în care dovedește toate aceste aspecte, transmițătorul este obligat să accepte efectul juridic al respectivei semnături cu implicațiile prevăzute de legislație asupra documentului electronic semnat cu acea semnătură.

5.3.3 SCENARIUL ÎN CARE O ORGANIZAȚIE PRIMEȘTE UN DOCUMENT SEMNAT ELECTRONIC CU O TEHNOLOGIE PE CARE O RECUNOAȘTE ȘI CARE ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014, DAR ULTERIOR, ORGANIZAȚIA NEAGĂ CĂ A SEMNAT RESPECTIVUL DOCUMENT

În acest caz, transmițătorul trebuie să invoce în instanță respectiva semnătură electronică și să facă (pe cheltuiala sa, a transmițătorului, a se revedea capitolul 4.3) dovada verificării respectivei semnaturi avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014.
În cazul în care dovedește toate aceste aspecte, organizația este obligată să accepte efectul juridic al respectivei semnături cu implicațiile prevăzute de legislație asupra documentului electronic semnat cu acea semnătură.

5.3.4 SCENARIUL ÎN CARE O ORGANIZAȚIE NU ARE CAPABILITATEA TEHNICĂ DE A RECUNOAȘTE (NU POATE PROCESA TEHNIC) O SEMNĂTURĂ ELECTRONICĂ AVANSATĂ CARE NU ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014.

Plecăm de la premiza că o organizație stabilește că poate procesa tehnic semnătura electronică realizată doar cu anumite tehnologii pentru semnătură electronică (dar respectând prevederile art. 27 din Regulamentul 910/2014, în cazul organismelor publice). Întrebarea este ce se întâmplă dacă NU are capabilitatea de a recunoaște (nu poate să proceseze tehnic) o semnătură electronică avansată care nu are un anumit efect juridic stabilit în afara Regulamentului 910/2014 și îi este invocat un document semnat astfel?

În acest caz, organizația trebuie să nu accepte documentul electronic respectiv și transmițătorul nu are alta cale decât să invoce în instanță respectivul document, unde trebuie să facă (pe cheltuiala transmițătorului, a se revedea capitolul 4.3) dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În funcție de modul în care dovedește toate aceste aspecte, instanța va decide efectul juridic al respectivei semnături, cu implicațiile prevăzute de legislație asupra documentului electronic semnat cu acea semnătură.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.3 POSIBILE SCENARII CU PRIVIRE LA UTILIZAREA SEMNĂTURII ELECTRONICE ȘI LA EFECTUL JURIDIC AL ACESTEIA

5.3.5 SCENARIUL ÎN CARE O ORGANIZAȚIE PRIMEȘTE UN DOCUMENT SEMNAT ELECTRONIC CU O TEHNOLOGIE PE CARE O RECUNOAȘTE, DAR CARE NU ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014, IAR, ULTERIOR, TRANSMIȚĂTORUL NEAGĂ CĂ A SEMNAT RESPECTIVUL DOCUMENT.

În acest caz, organizația trebuie să invoce în instanță respectiva semnătură electronică și să facă (pe cheltuiala sa, a organizației, a se revedea capitolul 4.3) dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În funcție de modul în care dovedesc toate aceste aspecte, instanța va decide efectul juridic al respectivei semnături, cu implicațiile prevăzute de legislație asupra documentului electronic semnat cu acea semnătură.

5.3.6 SCENARIUL ÎN CARE O ORGANIZAȚIE PRIMEȘTE UN DOCUMENT SEMNAT ELECTRONIC CU O TEHNOLOGIE PE CARE O RECUNOAȘTE, DAR CARE NU ARE UN ANUMIT EFECT JURIDIC STABILIT ÎN AFARA REGULAMENTULUI 910/2014, IAR, ULTERIOR, ORGANIZAȚIA NEAGĂ CĂ A SEMNAT RESPECTIVUL DOCUMENT.

În acest caz, transmițătorul trebuie să invoce în instanță respectiva semnătură electronică și să facă (pe cheltuiala sa, a transmițătorului, a se revedea capitolul 4.3) dovada verificării respectivei semnături avansate conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014. În funcție de modul în care dovedește toate aceste aspecte, instanța va decide efectul juridic al respectivei semnături, cu implicațiile prevazute de legislație asupra documentului electronic semnat cu acea semnătură.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.4 INVOCAREA ÎN INSTANȚĂ A UNEI SEMNĂTURI ELECTRONICE

Invocarea în instanță a unei semnături electronice presupune, obligatoriu, parcurgerea următoarelor etape:

▸ **Etapa 1** - Demonstrarea de către partea care invocă semnătură a îndeplinirii condițiilor de validare a respectivei semnături electronice, în funcție de tehnologia utilizata pentru crearea ei

▸ **Etapa 2** - Are loc numai după parcurgerea etapei 1 și constă în stabilirea efectului juridic al respectivei semnături

În cadrul Etapei 1, partea care invocă semnătură electronică trebuie să facă dovada îndeplinirii condițiilor de validare astfel:

▸ Pentru o semnătură calificată, conform tabelului 4 și tabelului 1 - așa cum am arătat în capitolele anterioare este un proces foarte simplu, toate informațiile pentru verificare fiind accesibile prin infrastructura dezvoltată la nivelul Uniunii Europene.

▸ Pentru o semnătură avansată, conform tabelului 5 și tabelului 2 - așa cum rezultă din aceste tabele, este un proces mult mai costisitor, pentru că informațiile pentru verificare nu sunt la fel de la îndemână ca acelea pentru semnătura calificată; practic, este necesară expertiza tehnică pentru dovedirea îndeplinirii condițiilor de validare a unei tehnologii de creare de semnătură avansată, alta decât semnătura calificată; subliniem încă o dată că o tehnologie (soluție tehnică și procedurală) utilizată pentru crearea unei semnături avansate trebuie să îndeplinească cerințe de același nivel ca si o semnătură calificată.

După parcurgerea Etapei 1, se trece la Etapa 2, în care se stabilește afectul juridic al respectivei semnături, astfel:

▸ Dacă, în urma etapei 1 s-a confirmat faptul că este o semnătură calificată, atunci efectul juridic al semnăturii este echivalent cu cel al semnăturii ologrefe, conform Art. 25 din Regulamentul 910/2014.

▸ Dacă în urma etapei 1 s-a confirmat faptul că respectiva semnătură electronica este o semnătură avansată și există un cadru legislativ, în afara Regulamentului 910/2014, care stabilește un efect juridic pentru acel tip de semnătură electronică, atunci acel efecte juridic este garantat, dacă instanța a constat că se respectă condițiile prevăzute de actul oficial (lege, hotărâre, ordin etc) care stabilește efectul juridic respectiv.

▸ Dacă în urma etapei 1 s-a confirmat faptul ca respectiva semnătură electronică este o semnătură avansată și nu există un cadru legislativ, în afara Regulamentului 910/2014, care să stabilească un efect juridic pentru acel tip de semnătură electronică, atunci instanța este cea care stabilește efectul juridic al respectivei semnături electronice.

▸ Dacă în urma etapei 1 s-a confirmat faptul ca respectiva semnătură electronică îndeplinește doar parțial cerințele pentru o semnătură avansată și nu există un cadru legislativ, în afara Regulamentului 910/2014, care sa stabilească un efect juridic pentru acel tip de semnătură electronică, atunci instanța este cea care stabilește efectul juridic al respectivei semnături electronice

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.4 INVOCAREA ÎN INSTANȚĂ A UNEI SEMNĂTURI ELECTRONICE

În Tabelul 8 este prezentată o analiză comparativă, pentru fiecare dintre cele doua etape obligatorii cu privire la:

▸ necesitatea demonstrării îndeplinirii condițiilor de validare pentru o semnătură electronică avansată (inclusiv calificată);

▸ costul acestei verificări;

▸ garantarea efectului juridic al respectivei semnături electronice

între diversele tipuri de tehnologii de creare de semnătură electronică care s-ar invoca în instanță.

DE REȚINUT

Orice organizație publică sau privată ESTE LIBERĂ SĂ DECIDĂ, INDEPENDENT DE EFECTUL JURIDIC STABILIT PENTRU DIVERSELE TIPURI DE SEMNĂTURI ELECTRONICE, dacă recunoaște (poate procesa tehnic) semnăturile electronice și ce tipuri de tehnologii pentru semnătură electronică recunoaște (poate procesa tehnic), cu precizarea suplimentară pentru organismele publice că trebuie să respecte art. 27.

Nicio organizație, publică sau privată, nu poate fi obligată să recunoască (să proceseze tehnic) nicio tehnologie de creare de semnătură electronică avansată care are un anumit efect juridic (nici măcar semnătura electronică calificată), pentru că acest lucru depinde de capabilitățile sale tehnice și financiare.

În schimb poate fi obligată să accepte efectele juridice ale unei semnături electronice avansate, în cazul în care transmițătorul face dovada în instanță a verificării respectivei semnături electronice conform capitolului precedent, inclusiv îndeplinirea, la momentul semnării, a cerințelor art. 26 din Regulamentul 910/2014.

În interacțiunea cu un serviciu public online oferit de un organism public care solicită semnătură electronică avansată, orice transmițător (persoană fizică sau juridică) are dreptul prin Regulamentul 910/2014, de a alege să trimită documente semnate cu orice semnătură avansată care respectă standardele și formatele definite de Regulament, sau cu semnătură avansată bazată pe certificat calificat, sau cu semnătură calificată.

Alegerea trebuie să o facă în funcție de costuri, dar mai ales de cât de ușor poate demonstra ulteriror în instanță condițiile pentru o semnătură avansată/calificată, în cazul în care are nevoie să invoce respectiva semnătură.

Nu se poate stabili efectului juridic al semnăturii electronice, decât după ce a fost parcursă etapa obligatorie de demonstrare a îndeplinirii condițiilor de validare pentru o semnătură electronică avansată (inclusiv calificată).

Deci prima etapă OBLIGATORIE când se invocă în instanță o semnătură electronică este acea de demonstrare a îndeplinirii condițiilor de validare pentru o semnătură electronică avansată (inclusiv calificată). Costul acestei verificări este cel mai mic în cazul semnăturii calificate, putându-se atrage răspunderea prestatorului calificat daca validarea nu se realizează din culpa acestuia.

5. VALOAREA LEGALĂ A DOCUMENTELOR SEMNATE ELECTRONIC

5.4 INVOCAREA ÎN INSTANȚĂ A UNEI SEMNĂTURI ELECTRONICE

Tabel 8. Comparație privind invocarea în instanță a diverselor tipuri de semnături electronice

ÎN CAZUL ÎN CARE ESTE INVOCATĂ O SEMNĂTURĂ ELECTRONICĂ ÎN INSTANȚĂ	Semnătură electronică calificată	Tehnologie pentru semnătură avansată cu efect juridic stabilit În plus față de prevederile Regulamentului 910/2014	Tehnologie pentru semnătură avansată fără efect juridic, altul decât cel stabilit de prevederile Regulamentului 910/2014	Tehnologie pentru semnătură electronică fără efect juridic, altul decât cel stabilit de prevederile Regulamentului 910/2014
Etapa 1. Partea care invocă această semnătură în instanță trebuie să demonstreze îndeplinirea condițiilor de validare pentru o semnătură avansată (inclusiv calificată)	**DA** **ESTE PRIMA ETAPĂ OBLIGATORIE**	**DA** **ESTE PRIMA ETAPĂ OBLIGATORIE**	**DA** **ESTE PRIMA ETAPĂ OBLIGATORIE**	**N/A** **Este prima etapă obligatorie**, dar se verifică în ce măsură respectiva semnătură electronică îndeplinește condițiile unei semnături avansate.
ÎN CADRUL ETAPEI 1 COSTUL DEMONSTRĂRII ÎNDEPLINIRII CONDIȚIILOR DE VALIDARE ESTE	**MIC,** asa cum e poate vedea din **tabelul 4**. Se poate atrage răspunderea prestatorului calificat, în cazul culpei acestuia.	**MAI MARE,** în cele mai multe situații implicând expertize tehnice care să parcurgă pașii detaliați în **tabelul 5**. Analizați cu atenție și **tabelele 6** și **7**	**MAI MARE,** în cele mai multe situații implicând expertize tehnice care să parcurgă pașii detaliați în **tabelul 5**. Analizați cu atenție și **tabelele 6** și **7**	**MAI MARE,** în cele mai multe situații implicând expertize tehnice care să parcurgă pașii detaliați în **tabelul 5**. Analizați cu atenție și **tabelele 6** și **7**
Etapa 2. În cazul în care se parcurge etapa 1 cu succes, efectul juridic al respectivei semnături este garantat?	**DA,** conform Regulamentului 910/2014, art. 25.	**DA,** dacă se respectă condițiile prevăzute de actul oficial (lege, hotărâre, ordin etc) care stabilește efectul juridic respectiv.	**NU.** STABILEȘTE INSTANȚA DE JUDECATĂ EFECTUL JURIDIC. Nu poate fi respinsă ca proba judiciară conform Regulamentului 910/2014, art. 25.	**NU.** STABILEȘTE INSTANȚA DE JUDECATĂ EFECTUL JURIDIC. Nu poate fi respinsă ca proba judiciară conform Regulamentului 910/2014, art. 25.

6. ANEXE

6.1 ANEXA I LA REGULAMENTUL 910/2014

CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SEMNĂTURI ELECTRONICE

Certificatele calificate pentru semnături electronice conțin:

(a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice;

(b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin statul membru în care este stabilit prestatorul respectiv; și

- în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;

- în cazul unei persoane fizice: numele persoanei;

(c) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

(d) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice;

(e) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului;

(f) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de încredere calificat;

(g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent;

(h) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit;

(i) localizarea serviciilor care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat;

(j) în cazul în care datele de creare a semnăturilor electronice legate de datele de validare a semnăturilor electronice sunt situate într-un dispozitiv de creare a semnăturilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.

6. ANEXE

6.2 ANEXA II LA REGULAMENTUL 910/2014

CERINȚE PENTRU DISPOZITIVELE DE CREARE A SEMNĂTURILOR ELECTRONICE CALIFICATE

1. Dispozitivele de creare a semnăturilor electronice calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că:

(a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil;

(b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată;

(c) există suficiente asigurări că datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice nu pot să fie descoperite prin deducție și că semnătura electronică este protejată în mod fiabil împotriva falsificării utilizând tehnologia disponibilă în prezent;

(d) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice pot să fie protejate în mod fiabil de către semnatarul legitim împotriva utilizării de către alte persoane.

2. Dispozitivele de creare a semnăturilor electronice calificate nu modifică datele care urmează să fie semnate sau nu împiedică prezentarea lor semnatarului înainte de a semna.

3. Generarea sau gestionarea datelor de creare a semnăturilor electronice în numele semnatarului se pot realiza numai de către un prestator de servicii de încredere calificat.

4. Fără a aduce atingere punctului 1 litera (d), prestatorii de servicii de încredere calificați care gestionează datele de creare a semnăturilor electronice în numele semnatarului pot duplica datele de creare a semnăturilor electronice numai în scopul de a le avea de rezervă, cu condiția ca următoarele cerințe să fie îndeplinite:

(a) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale;

(b) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului.

6. ANEXE

6.3 ANEXA LA DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1506 A COMISIEI

Lista specificațiilor tehnice pentru semnăturile electronice avansate în formatele XML, CMS sau PDF și pentru fișierele-container cu semnătură asociată
Semnăturile electronice avansate menționate la articolul 1 din decizie trebuie să respecte una dintre următoarele specificații tehnice ale ETSI, cu excepția secțiunii 9:

Profilul de bază XAdES	**ETSI TS 103171 v.2.1.1.**
Profilul de bază CAdES	**ETSI TS 103173 v.2.2.1.**
Profilul de bază PAdES	**ETSI TS 103172 v.2.2.2.**
Fișierele-container cu semnătură asociată menționate la articolul 1 din decizie trebuie să respecte următoarele specificații tehnice ale ETSI:	
Profilul de bază al fișierului container cu semnătura asociată	**ETSI TS 103174 v.2.1.1.**

6. ANEXE

6.4 ANEXA MODEL - POLITICA DE SEMNARE ELECTRONICĂ ÎN <NUME ORGANIZAȚIE>

1. SCOP
Scopul acestei politici este de a stabili cerințe cu privire la utlizarea semnăturilor electronice în cadrul <Nume organizație>. Deoarece comunicarea a devenit în principal electronică, scopul este de a reduce confuzia cu privire la încrederea într-o semnătură electronică.

2. CUI SE APLICĂ
Această politică se aplică tuturor angajaților <Nume organizație> și afiliaților. Această politică nu se aplică documentelor generate în afara organizației și primite de către organizație.

3. POLITICA
Semnătura electronică se poate utiliza în loc de semnătură olografă pe orice document care intră în organizație, cu excepția celor menționate la adresa: <URL-ul Listei cu documente care nu se pot semna electronic>.

<Conducerea Organizației> va menține o listă la nivelul întregii organizații cu tipurile de documente care nu sunt acoperite de această politică.

Semnăturile electronice trebuie să se utilizeze numai de către persoanele fizice.

4. RESPONSABILITĂȚI
Acceptarea semnăturii electronice necesită acțiuni specifice atât pentru angajatul care semnează documentul (în continuare denumit semnatar), cât și pentru angajatul care primește / citește documentul (în continuare denumit destinatar).

4.1. Resposabilitățile semnatarului

4.1.1. Semnatarii trebuie să dețină un certificat digital, pe care îl primesc prin grija <Departament responsabil>. Aceast certificat digital este emis de <Nume companie/Departament Organizație> denumită în continuare Autoritatea de certificare (AC).

4.1.2. Semnatarii trebuie să semneze documentele folosind software-ul aprobat de <Nume organizație>.

4.1.3. Semnatarii trebuie să-și protejeze cheia privată și să o păstreze în secret, în conformitate cu Termenii și condițiile de utilizare a certificatului.

4.1.4. Dacă un semnatar consideră că cheia sa privată a fost furată sau compromisă în alt mod, semnatarul trebuie să contacteze imediat <Departament organizație> pentru a revoca certificatul.

4.2. Resposabilitățile destinatarului

4.2.1. Destinatarii trebuie să citească documentele folosind software-ul aprobat de <Nume organizație>

4.2.2. Destinatarii trebuie să verifice dacă certificatul a fost emis de AC și nu a fost revocat, prin vizualizarea detaliilor despre certificat folosind software-ul pe care îl utilizează pentru a citi documentul, conform instrucțiunilor de utilizare detaliate furnizate de <Departament organizație>

4.2.3. Dacă semnătura electronică a semnatarului nu pare validă, destinatarul nu trebuie să aibă încredere în sursa documentului.

4.2.4. Dacă un destinatar consideră că o semnătură electronică a fost utilizată în scopuri ilegitime, destinatarul trebuie să raporteze la <Departament organizație>.

5. RESPECTAREA POLITICII

5.1. Măsurarea conformității
<Departament organizație> va verifica respectarea acestei politici prin diferite metode, inclusiv, fără a se limita la, rapoarte privind instrumentele de afaceri, audituri interne și externe și feedback-ul către proprietarul politicii.

5.2. Excepții
Orice excepție de la politică trebuie să fie aprobată în prealabil de către echipa <Departamentul organizației>.

5.3. Nerespectarea
Dacă se constată că un angajat a încălcat această politică, acesta poate fi supus unei acțiuni disciplinare, până la încetarea contractului de muncă.

6. STANDARDE, POLITICI ȘI PROCESE CONEXE
TBD

7. REFERINȚE
Regulamentul 910/2014
TBD

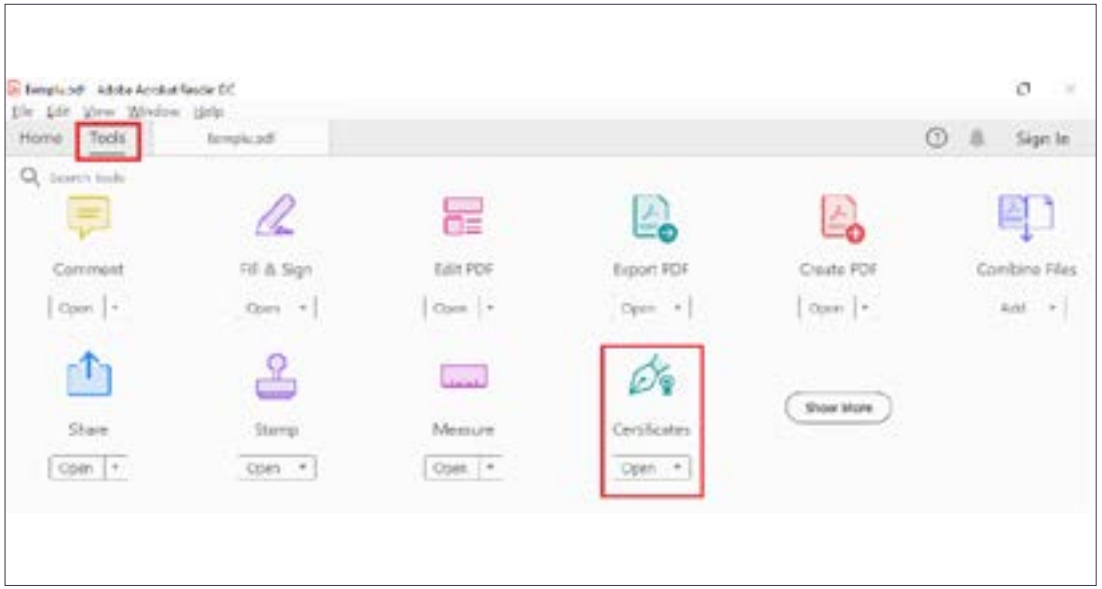
8. DEFINIȚII
TBD

9. ISTORIC REVIZII

6. ANEXE

6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

1. Cu Adobe Acrobat Reader DC, deschideți documentul care trebuie semnat și efectuați click pe **Tools**. Din fereastra care apare, selectați opțiunea **Certificates**.

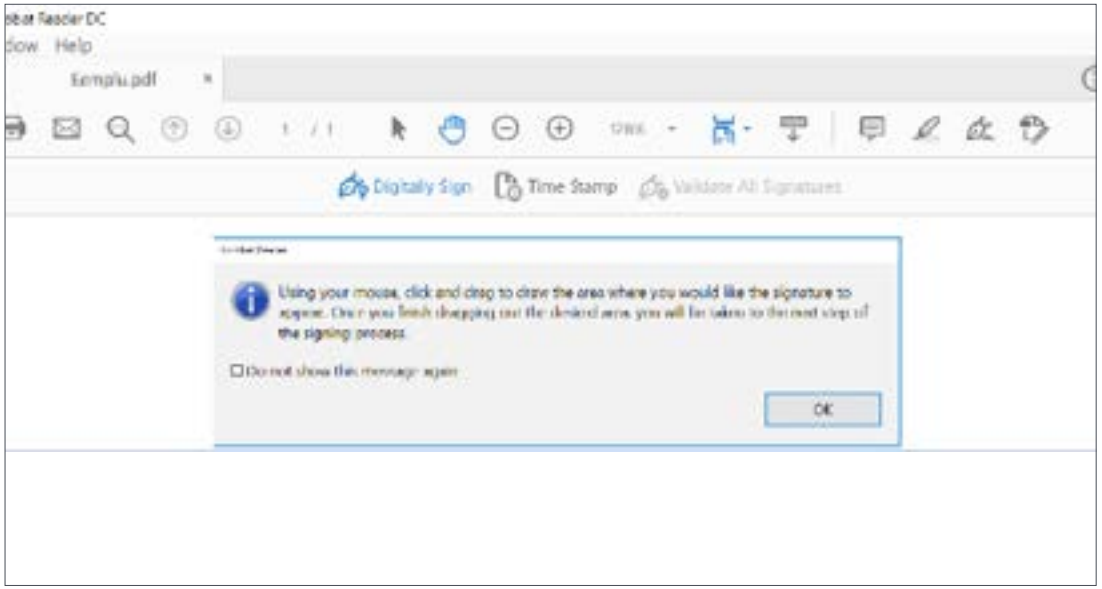


Pasul 1

6. ANEXE

6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

2. Efectuați click pe Digital Sign și apăsați butonul OK din următorul mesaj.

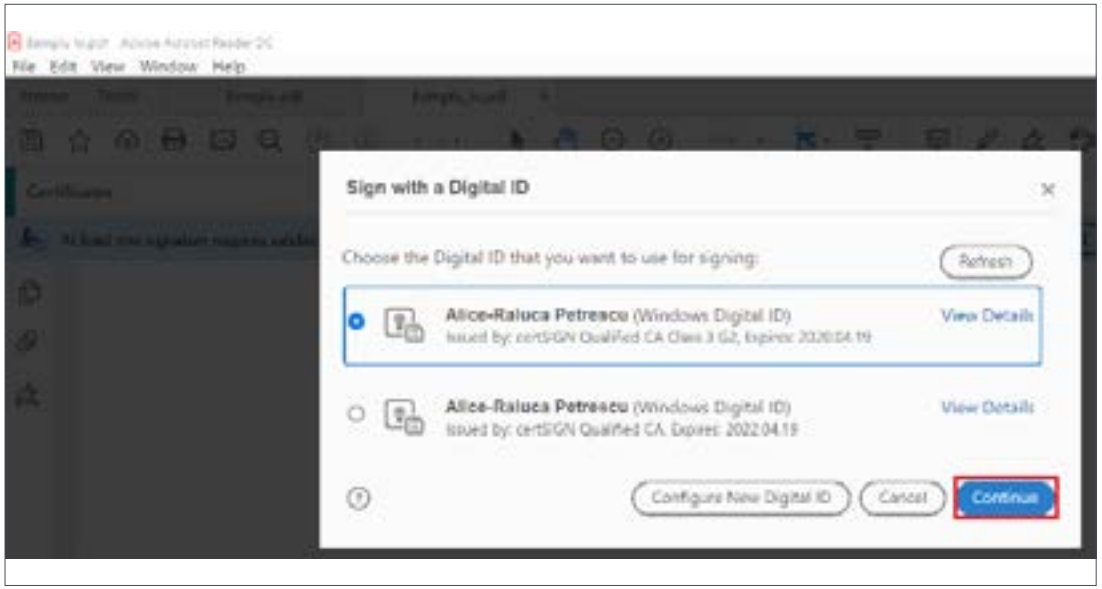


Pasul anterior
Pasul 2

6. ANEXE

6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

3. Trasați un dreptunghi în locul unde doriți să aplicația semnătura. În fereastra care apare, selectați certificatul digital dorit și efectuați click pe butonul **Continue**. Dacă aveți mai multe certificate, trebuie să selectați certificatul dorit pentru semnare.



Pasul anterior
Pasul 3

6. ANEXE

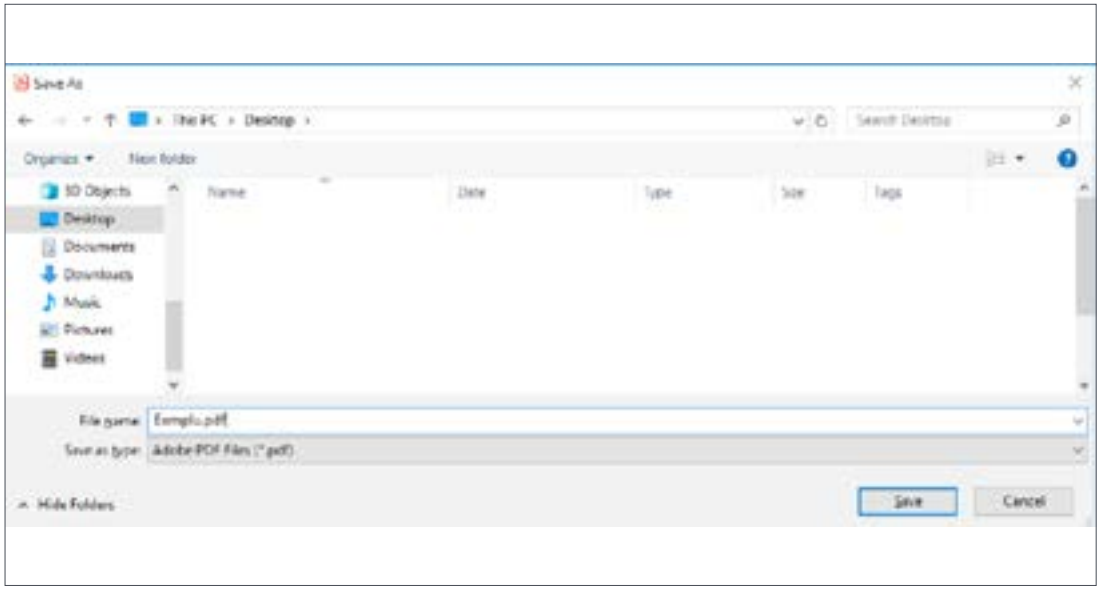
6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

4. În fereastra următoare, dați click pe butonul Sign pentru a continua semnarea documentului.

6. ANEXE

6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

5. În fereastra următoare, vi se va solicita să salvați documentul și să introduceți PIN-ul de la token-ul pe care se află certificatul.



Pasul anterior
Pasul 5

6. ANEXE

6.5 SEMNAREA DOCUMENTELOR PDF CU ADOBE ACROBAT READER DC

6. După introducere PIN, pe document va apărea semnătura în locul în care ați desenat dreptunghiul de semnare.

Pasul anterior

6. ANEXE

6.6 VERIFICAREA SEMNĂTURII CALIFICATE PDF CU ADOBE ACROBAT READER

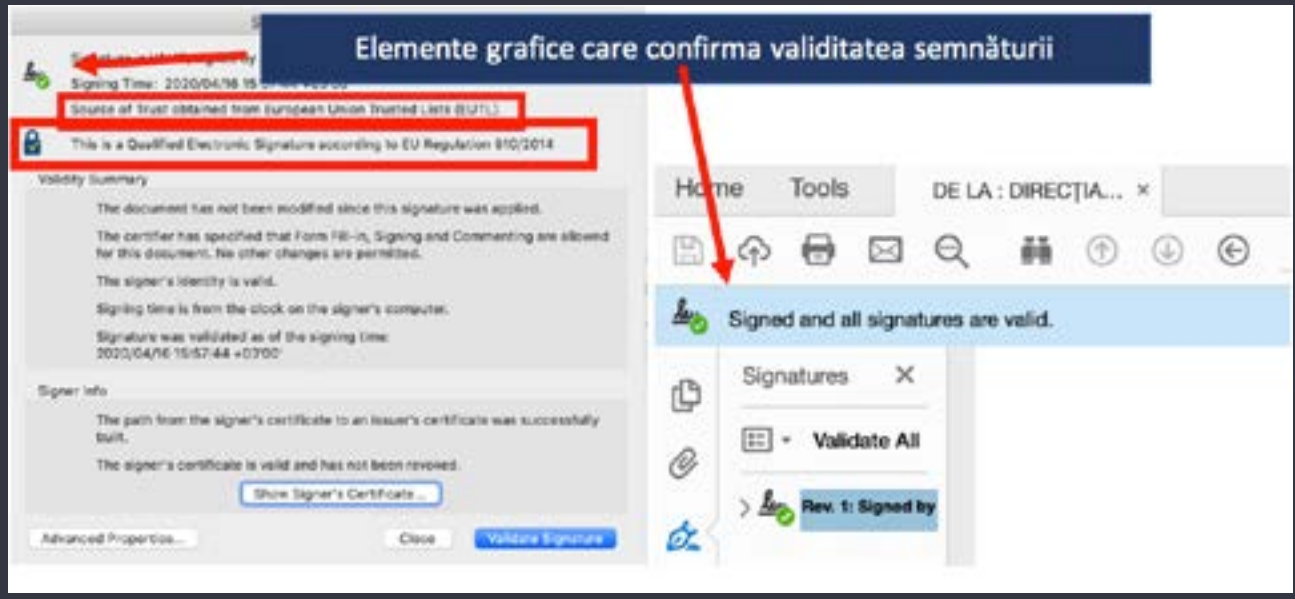
O semnătură calificată apare în Adobe Acrobat Reader ca fiind validă (bifă verde) și conține informații despre verificarea ei față de lista de încredere europeană.

Sunt afișate elemente grafice ușor de verificat, care să transmită utilizatorilor nivelul de încredere:

▸ Bifa verde și textul „Signed and all signatures are valid” (semnat și toate semnaturile sunt valide)

▸ Este indicată sursa informațiilor folosite pentru validarea semnăturii: „Source of Trust obtained from the European Union Trusted Lists (EUTL)” (încrederea în semnătură este dată de listele sigure ale Uniunii Europene)

▸ Marca de încredere a Uniunii Europene (lacătul albastru cu steagul UE) și identificarea semnăturii electronice ca fiind calificată

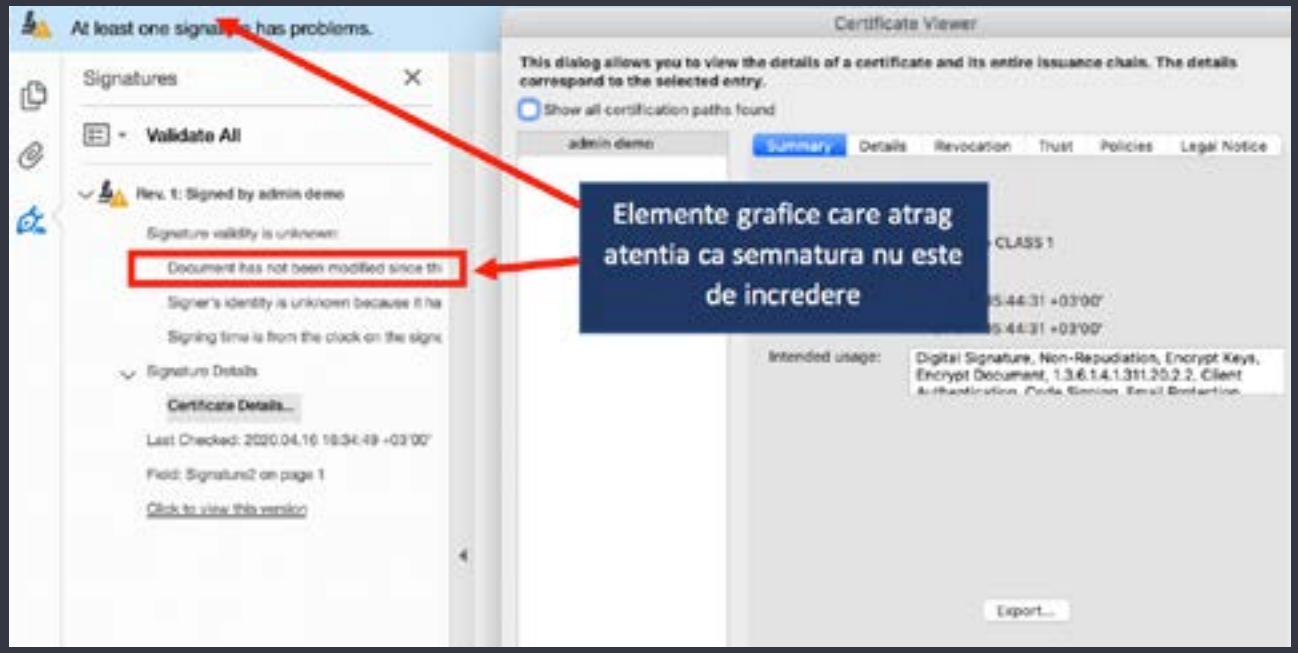


6. ANEXE

6.7 VERIFICAREA SEMNĂTURII (POTENȚIAL) AVANSATE PDF CU ADOBE ACROBAT READER

O semnătură electronică posibil avansată nu este validată automat în Adobe Acrobat Reader.

Aplicația nu poate afișa informații despre aceasta și atrage atenția utilizatorului:

▸ Triunghiul galben cu semnul exclamării și textul „At least one signature has problems” (Cel putin o semnătură are probleme.);

▸ Textul care indică că identitatea persoanei care a semnat nu poate fi validată: „The signer’s identity is unknown because it has not been included in your list of trusted certificates and none or its parent certificates are trusted certificates” (Identitatea semnatarului nu este cunoscută deoarece nu a fost inclus în lista certificatelor de încredere și niciunul dintre certificatele părinte [obs. care au emis certificatul] nu sunt certificate de încredere.).