
certSIGN®

certSIGN în cifre

50 proiecte de PKI implementate în 20 țări, din care 40 proiecte la nivel de autorități naționale

15 audituri ANUALE pentru verificarea diferitelor servicii oferite în domeniul PKI

7 participări la teste internaționale de interoperabilitate în domeniul semnăturii electronice

20 doctori, doctoranzi și masteranzi în domeniul securității IT, PKI sau criptografie

3 generații de specialiști în domeniul PKI formate în certSIGN, care lucrează în cele mai renumite companii internaționale

19 produse proprii dezvoltate în domeniul semnăturii electronice și criptării

3 produse proprii inscrise in catalogul ORNISS pentru utilizarea in protectia informatiilor clasificate din care 2 sunt si in catalogul NATO

1 QSCD (Dispozitiv calificat de creare a semnaturii electronice) propriu recunoscut la nivel UE

1 patent în domeniul criptării homomorfice înregistrat în US și în curs de înregistrare în UE

1 cerere de patent depusă în domeniul blockchain

20 Ani de experienta in domeniu criptografiei cu chei publice si a semnaturii electronice

certSIGN®

Aspecte practice cu privire la crearea și verificarea semnăturilor electronice conform Regulamentului 910/2014

certSIGN®

Definiţii

Regulamentul eIDAS definește mai multe tipuri de semnătură electronică (art. 3 alin. 9 - 11):

Semnătura 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.

Semnătura electronică avansată pentru care există cerințe cf. art 26:

- face trimitere exclusiv la semnatar;
- permite identificarea semnatarului;
- 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
- este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.

certSIGN®

Definiţii

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.

Şi mai departe:

- **dispozitiv de creare a semnăturilor electronice calificat** înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II;
- **dispozitiv de creare a semnăturilor electronice** înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;
- **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;
- **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;
- **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;
- **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;
- **serviciu de încredere calificat** înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute **de prezentul regulament**;
- **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;

certSIGN®

Diferențe între semnăturile electronice

Semnătura electronică poate însemna orice fel de semnătură pe un suport informatic, aceasta poate fi și o semnătură scanată inclusă într-un document electronic sau semnătura de la finalul unui e-mail. Astfel de semnături pot fi ușor de reprodus și nu asigură niciun fel de protecție pentru datele electronice cărora le-au fost atașate. Nu există niciun fel de cerințe cu privire la formatul acestei semnături. Din acest motiv este dificil de stabilit a priori nivelul de încredere și de dovedit ulterior că a fost realizată de o anumită persoană.

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

Semnatura electronică avansată, este tot un concept abstract, care este strâns legat de gradul de încredere pe care cineva se presupune că ar trebui să îl aibă într-o semnatura electronica.

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 din definiție, exprimă “cu un nivel ridicat de încredere” actul de voință al semnatarului.

certSIGN®

Diferențe între semnăturile electronice

- O afirmație de genul *“documentele semnate cu semnătură avansată exprimă actul de voință al semnatarului”* este un TRUISM, pentru că din definiția semnăturii avansate, este evident că o semnătură electronică, care îndeplinește cele 4 condiții reprezintă actul de voință al semnatarului.

- O afirmație care are sens este următoarea: *“documentele semnate cu semnătură avansată realizată cu tehnologia X exprimă actul de voință al semnatarului”,* pentru că se asigura posibilitatea de a verifica (mai ușor sau mai greu, în funcție de tehnologie) că se indeplinesc cele 4 condiții din definiția semnăturii avansate.

certSIGN®

Diferențe între semnăturile electronice

- **Semnătura electronică calificată**, spre deosebire de conceptul de *“semnătură electronică avansata”*, este o semnătură electronică pentru 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 am arătat mai sus, și în Anexe la care se adaugă o serie considerabilă de cerințe precizate în Regulament și mai departe în decizii de 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 **semnătura avansată DOVEDITĂ/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.

certSIGN®

Formate de semnătură avansată

- Conform art. 27 alin. 5 din Regulament, a fost emisa 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.

- Decizia (UE) 1506/2015 descrie **cerințele tehnice** pentru recunoașterea semnăturilor avansate:

  - Prin utilizarea **unor formate de semnături definite de standardele ETSI: PDF, CMS sau XML** la nivelul de conformitate B, T sau LT (cf. art. 1)

sau

  - Prin utilizarea **altor formate decât cele definite la art. 1**, cu conditia sa indeplineasca o lista de cerinte pe care le respecta formatele precizate mai sus.

certSIGN®

Formate de semnătură avansată

- Conform Regulamentului, cel puțin în relația cu instituțiile publice, este foarte important de subliniat că prin Regulament se acceptă formatele de semnături definite de standardele ETSI precizate anterior.

- Consecința acestei decizii este că, în conformitate cu standardele specificate, semnătura avansată acceptată în relația cu instituțiile publice se bazează ca mecanism tehnic pe **semnătura digitală realizată cu certificat digital (calificat sau necalificat).**

- **Certificatele digitale reprezintă un serviciu de încredere definit de Regulament, și deci ele trebuie emise de prestatori de servicii de încredere, care trebuie să îndeplinească cerințele Regulamentului cu privire la orice prestatorii de servicii ce încredere.**

- Conform Deciziei (UE) 1506/2015, în fapt, un emitent de certificat digital pentru semnătură avansată ar trebui să îndeplinească aceleași condiții ca unul de certificat calificat pentru semnătură calificată doar că, în cazul certificatului digital necalificat pentru semnătură avansată, îndeplinirea condițiilor este pe propria răspundere a semnatarului.

certSIGN®

Formate de semnătură avansată acceptate de autoritati – art.5 alin. 2 din OUG38/2020

- Coroborand prevederile art. 27 si decizia de punere in aplicare concluzia este ca, din perspectiva Regulamentului, o organizatie publica are urmatoarele optiuni:

- Sa aleaga sa utilizeze/accepte semnatura electronica bazata pe certificat necalificat (intr-unul din formatele PDF, CMS si/sau XML), cu conditia sa dovedeasca faptul ca este avansata, DAR conform art. 27 este **OBLIGATA sa accepte si**:

  - semnatura electronica avansata bazata pe orice tip de certificat necalificat (in formatul corespunzator ales PDF, CMS si/sau XML), care de asemenea trebuie sa se dovedeasca ca este avansata

  - semnatura electronica avansata bazata pe certificat calificat (in formatul corespunzator ales PDF, CMS si/sau XML), care de asemenea trebuie sa se dovedeasca ca este avansata

  - semnatura calificata (in formatul corespunzator ales PDF, CMS si/sau XML) – care am aratat anterior ca este CERT ca este avansata

certSIGN®

Formate de semnătură avansată acceptate de autoritati – art.5 alin. 2 din OUG38/2020 - CONTINUARE

- Sa aleaga sa utilizeze/accepte semnatura electronica bazata pe certificat calificat (intr-unul din formatele PDF, CMS si/sau XML), cu conditia sa dovedeasca faptul ca este avansata, DAR conform art. 27 este OBLIGATA sa accepte si:
  - semnatura calificata (in formatul corespunzator ales PDF, CMS si/sau XML) – care am aratat in capitolul precedent ca este CERTA ca este avansata
- Sa aleaga sa utilizeze/accepte **doar** semnatura electronica calificata (intr-unul din formatele PDF, CMS si/sau XML).

certSIGN®

Verificarea semnăturii electronice

- Orice semnătură electronică TREBUIE să poată fi verificată/validată, scopul fiind acela de a avea certitudinea că documentul semnat electronic reprezintă actul de voință al semnatarului.

- Pentru o semnătura avansată sau calificată trebuie verificate conditiile așa cum sunt precizate în Regulament:

  - Pentru semnătura calificată – art. 32 din Regulament;

  - Pentru semnătura avansată – art. 2, alin. (2) din Decizia de aplicare 2015/1506.

certSIGN®

Verificarea semnăturii electronice

VERIFICAREA SEMNĂTURII CALIFICATE (art. 32 Regulament)	VERIFICAREA SEMNĂTURII AVANSATE (art. 2 alin. (2) din Decizia de aplicare 2015/1506)
(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:	(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; (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;	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;
(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;	2. datele de validare a semnăturilor corespund datelor furnizate de beneficiar;

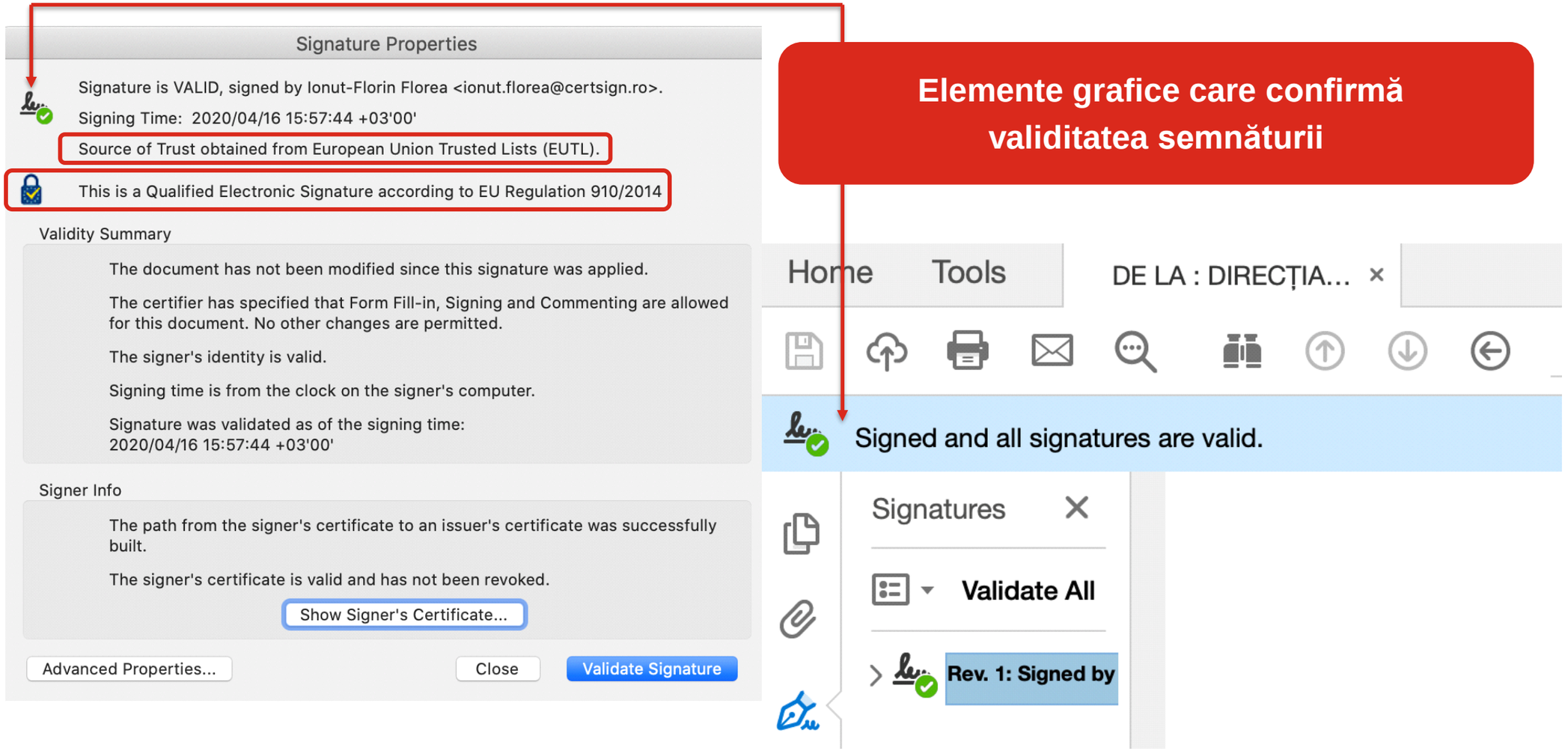
Verificarea semnăturii electronice - continuare

VERIFICAREA SEMNĂTURII CALIFICATE (art. 32 Regulament)	VERIFICAREA SEMNĂTURII AVANSATE (art. 2 alin. (2) din Decizia de aplicare 2015/1506)
(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.

Verificarea cerințelor art. 26 pentru diverse tipuri de semnaturi

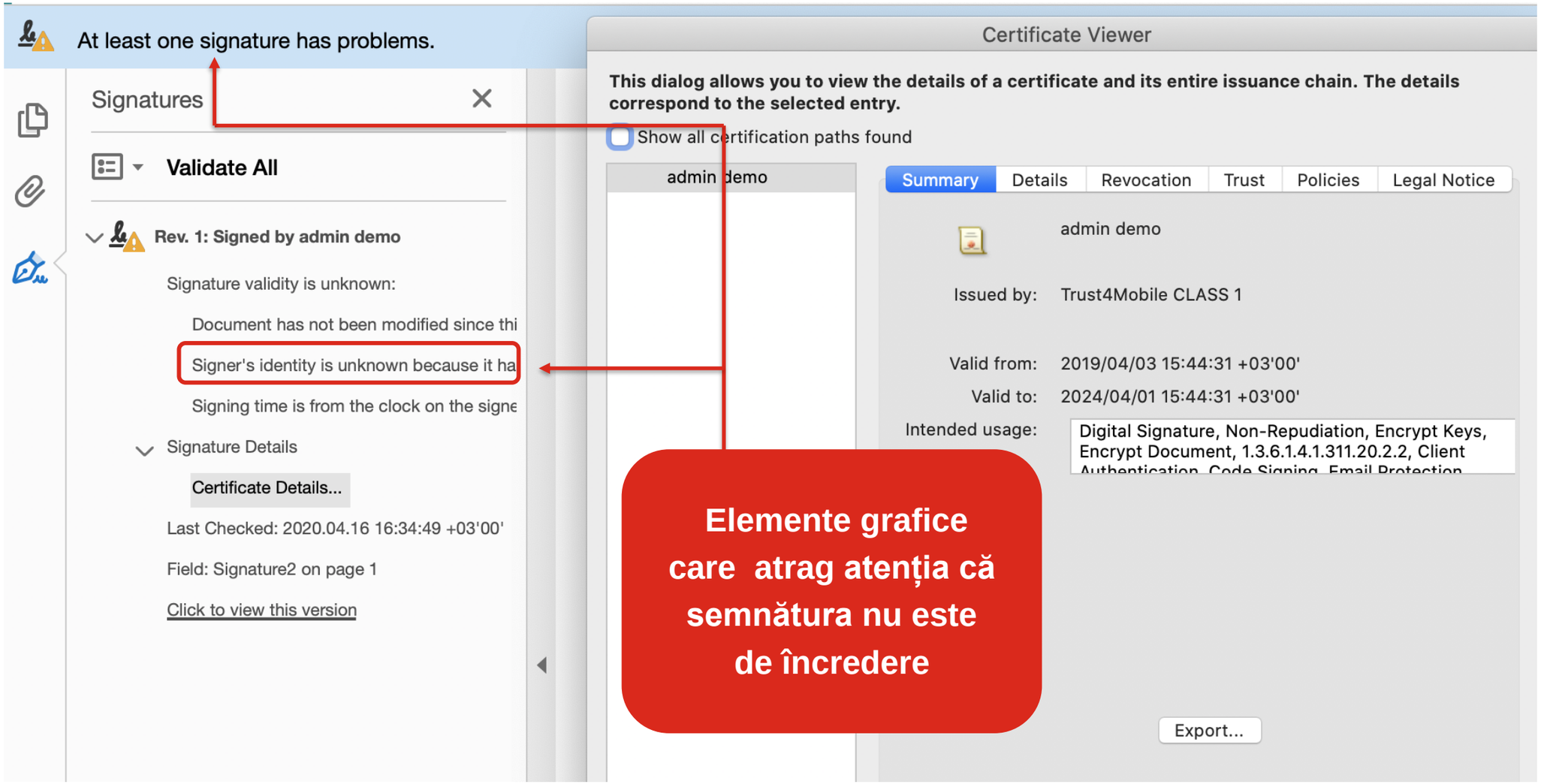
Cerinte art. 26 din Regulamentul 910		(a) face trimitere exclusiv la semnatar;	(b) permite identificarea semnatarului;	(c) este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său;	(d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.
Tipuri de semnaturi					
Semnatura electronica calificata		DA, pentru ca se bazeaza pe si contine certificatul calificat, care face trimitere exclusiv la semnatar, conform Anexei 1 la Regulament, punctul c	DA, pentru ca se bazeaza pe si contine certificatul calificat, care se emite in conditiile prevazute la art. 24 (1)	DA, pentru ca se bazeaza de pe QSCD care indeplineste aceasta cerinta conform Anexei II la Regulament, punctul 1	DA, pentru ca se utilizeaza certificate digitale, adica tehnologie cu chei publice care asigura integritatea datelor semnate, **dar cu conditia utilizarii formatelor standardizate prevazute de Regulament si Decizia 1506**
SEMNATURA ELECTRONICA (POTENTIAL) AVANSATA	**Semnatura electronica bazata pe certificat calificat (fara dispozitiv calificat)**	DA, pentru ca se bazeaza pe si contine certificatul calificat, care face trimitere exclusiv la semnatar, conform Anexei 1 la Regulament, punctul c	DA, pentru ca se bazeaza pe si contine certificatul calificat, care se emite in conditiile prevazute la art. 24 (1)	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea utilizata pentru gestionarea accesului la datele de creare a semnaturii	DA, pentru ca se utilizeaza certificate digitale, adica tehnologie cu chei publice care asigura integritatea datelor semnate, **dar cu conditia utilizarii formatelor standardizate prevazute de Regulament si Decizia 1506**
	Semnatura electronica bazata pe certificat necalificat si fara dispozitiv calificat	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea in care s-a emis respectivul certificat necalificat	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea in care s-a emis respectivul certificat necalificat si a procedurilor de identificare utilizate la momentul emiterii certificatului necalificat.	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea utilizata pentru gestionarea accesului la datele de creare a semnaturii	DA, pentru ca se utilizeaza certificate digitale, adica tehnologie cu chei publice care asigura integritatea datelor semnate, **dar cu conditia utilizarii formatelor standardizate prevazute de Regulament si Decizia 1507**
	Semnatura electronica bazata pe certificat necalificat si fara dispozitiv calificat, asociata unui document transmis prin utilizarea unor mecanisme de autentificare de nivel substanţial sau ridicat(OUG 38, art. 5 alin 3)	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea in care s-a emis respectivul certificat necalificat.	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de modalitatea in care s-a emis respectivul certificat necalificat si a procedurilor de identificare utilizate la momentul emiterii certificatului necalificat.	Daca se poate indica in formatul semnaturii modul de transmitere a documentului semnat (dar standardele existente nu par sa permita acest lucru, decat eventual printr-o fortare, cu implicatii negative pe partea de interoperabilitate), atunci utilizarea mecanismului de autentificare, in sensul de mijloc electronic de identificare de nivel substantial sau ridicat(*) ar putea asigura indeplinirea acestei conditii, cu conditia sa existe dovada ca acel mijloc de identificare este de nivel substantial sau ridicat.	DA, pentru ca se utilizeaza certificate digitale, adica tehnologie cu chei publice care asigura integritatea datelor semnate, **dar cu conditia utilizarii formatelor standardizate prevazute de Regulament si Decizia 1507**
	Semnatura electronica bazata pe alte mecanisme decat semnatura digitala	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de mecanismul utilizat.	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de mecanismul utilizat.	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de mecanismul utilizat.	Trebuie ca semnatarul sa poata demonstra aceasta cerinta, in functie de mecanismul utilizat.
		***) Nu exista definit nici in OUG 38, nici in Regulamentul 910 conceputul de mijloc de autentificare de nivel substantial sau ridicat**			
		Exista definit in Regulamentul 910 mijlocul electronic de identificare de nivel substantial sau ridicat			

Verificarea practică a semnăturii calificate – cu Adobe Reader DC



certSIGN®

Verificarea practică a semnăturii (posibil) avansate – cu Adobe Reader DC



certSIGN®

Verificarea unei semnaturi electronice realizata prin scanarea semnaturii (?)

O amenii să își dea copiii la învățătură de carte. Să nu creadă tot ce scrie pe Internet fără să verifice.

Concluzii

- In mod evident, din motive de costuri, de usurinta in utilizare si pentru interoperabilitate in implementarea proceselor de digitalizare in organizatie si intre organizatii, organizatiile ar trebui sa decida sa se limiteze la a utiliza cat mai putine tehnologii pentru crearea si respectiv acceptarea semnaturilor electronice
- Decizia stabilirii la care dintre tehnologii sa se limiteze o autoritate publica se poate lua doar respectand cerintele Art. 27 din Regulamentul 910/2014, asa cum prevede si OUG 38/2020 la art.5 alin. 2
- De asemenea, decizia alegerii unor anumite tehnologii trebuie sa tina cont si de costurile pe care le presupune implementarea unui sistem de verificare unei semnaturi avansate, inclusiv a celei calificate deoarece **DEMONSTRAREA ca o semnatura avansate indeplinea la momentul semnarii cerintele de la art.26 este OBLIGATORIE**

certSIGN®

Concluzii

- Conform Regulamentului, autoritatile publice trebuie sa aleaga semnaturi electronice bazate pe certificat digital (calificat sau necalificat)
- La nivelul UE, in baza Regulamentului este creata deja infrastructura necesara pentru verificare certificatelor calificate si este disponibila GRATUIT
- Preambul Regulament 910 – punctul 28

“(28) Pentru a spori în special încrederea întreprinderilor mici și mijlocii (IMM) și a consumatorilor în piața internă și pentru a promova utilizarea serviciilor și produselor de încredere, noțiunile de servicii de încredere calificate și prestator de servicii de încredere calificat ar trebui să fie introduse pentru a indica cerințele și obligațiile care asigură securitatea la nivel înalt a oricăror servicii și produse de încredere calificate utilizate sau furnizate.”

certSIGN®

Vă mulțumesc!

Constantin Burdun

Deputy CEO certSIGN

costin.burdun@certsign.ro

certSIGN®