

Cat de... avansata e semnatura ta avansata?

Costin Burdun

Sa ne amintim din episoadele precedente...

- „**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;
- „**semnătură electronică avansată**” înseamnă o **semnătură electronică** ce îndeplinește cerințele prevăzute la articolul 26;
 - 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.
- „ **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

Sa ne amintim din episoadele precedente...

- **Semnatura digitala** este un **mecanism tehnic pentru crearea unei semnaturi electronice**
- Elementele de baza ale unei semnaturi digitale
 - Formatul tehnic de semnatura
 - Cheia privata a subiectului
 - Certificatul digital care contine cheia publica corespunzatoare cheii private asociata cu elemente de identificare ale subiectului
 - Autoritatea de certificare emitenta
 - Politica de certificare a autoritatii de certificare
- Datorita proprietatilor sale de a asigura autentificare, integritate si non-repudiere, **semnatura digitala este mecanismul tehnic specificat de Regulamentul EIDAS pentru crearea semnaturii electronice avansate si calificate**

Sa ne amintim din episoadele precedente...

Mediul fizic	Mediul electronic	Reflecta actul de vointa al semnatarului?
Semnatura olografa	Semnatura electronica calificata	DA, <u>conform Regulamentului EIDAS semnatura calificata are acelasi effect juridic ca si semnatura olografa</u>
N/A	<u>O</u> semnatura electronica avansata ne-calificata	DA, <u>cu conditia dovedirii indeplinirii conditiilor Art. 26 din Regulamentul EIDAS</u>
N/A	<u>O</u> semnatura electronica care nu este avansata (simpla)	NU – O semnatura electronica ne-avansata nu reflecta actul de vointa al semnatarului, deci utilizarea ei poate avea consecinte pe care le putem asuma, dar, in cunostinta de cauza; - o instanta este obligata sa o ia in considerare conform Regulamentului EIDAS

Sa ne amintim din episoadele precedente...

- Ne putem baza pe o semnatura electronica ce a fost creata utilizand un certificat digital DACA SI NUMAI DACA avem incredere in acel certificat digital
- Avem incredere intr-un certificat digital DACA SI NUMAI DACA avem incredere in Autoritatea de certificare care l-a emis
- Avem incredere intr-o Autoritate de certificare DACA SI NUMAI DACA avem incredere in Politica de certificare
- La nivel european exista European Trusted List (EUTL) care contine lista autoritatilor de certificare calificate, care aplica o politica standardizata la nivel UE, numita Politica de certificare pentru emiterea de certificate calificate
- Pentru o semnatura electronica bazata pe certificat ne-calificat, sunt necesare costuri mari pentru a valida daca un certificat ne-calificat este sau nu de incredere pentru ca teoretic exista o multitudine de autoritati de certificare care nu emit certificate calificate

Cum stiu ca o semnatura electronica NU este avansata?

- **Indiciu– Nu este realizata utilizand semnatura digitala ca mecanism tehnic**
 - Regulamentul EIDAS stabileste ca formatul semnaturii electronice avansate trebuie sa fie bazat pe semnatura digitala
 - Acest lucru inseamna ca fiecare semnatar trebuie sa aiba un certificat digital si cheie private asociata cu care semneaza electronic
 - Certificatele digitale trebuie sa aiba in subiect NUMELE semnatarilor

Cum stiu ca o semnatura electronica NU este avansata?

- Indiciu – Nu este realizata utilizand semnatura digitala ca mecanism tehnic, cum se vede in exemplul de mai jos, unde cei doi “semnatari” nu au certificate digitale



Cum se “vad” semnăturile digitale - exemplu

 Semnat, cu toate semnăturile valide. Panou cu semn

Semnături

 Validare globală

✓  Rev. 1: Semnată de Constantin Burdun <constantin.burdun@certsign.ro>

Semnătura este validă:

Sursă de autentificare obținută de la European Union Trusted Lists (EUTL).

Aceasta este o Semnătură electronică calificată conform Regulamentului UE 910/2014.

Documentul nu a fost modificat după aplicarea acestei semnături

Identitatea semnatarului este validă

Semnătura include un marcaj temporal încorporat.

Semnătura este activată pentru LTV

Detalii semnătură

[Detalii certificat...](#)

Ultima verificare: 2021.10.09 15:38:34 +03'00'

Câmp: Signature2 la pagina 1

[Faceți clic pentru a vizualiza această versiune](#)

1 modificări diverse

✓  Rev. 2: Semnată de Constantin Burdun <costin.burdun@gmail.com>

Semnătura este validă:

Sursă de autentificare obținută de la European Union Trusted Lists (EUTL).

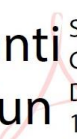
ACESTA ESTE UN DOCUMENT DE TEST SEMNAT DE MINE IN DOUA CALITATI:

- De persoana fizica
- De persoana fizica, in calitate de angajat la o companie

CONSTANTIN BURDUN – persoana fizica

Constantin Burdun  Semnat digital de Constantin Burdun
Data: 2021.10.09 15:38:11 +03'00'

CONSTANTIN BURDUN – angajat la o companie

Constantin Burdun  Semnat digital de Constantin Burdun
Data: 2021.10.09 15:36:05 +03'00'

Cum se “vad” semnăturile digitale - exemplu

Document de test.pdf - Adobe Acrobat Reader DC (32-bit)

Fișier Editare Vizualizare Semnare Fereastră Asistență

Pagina principală Instrumente QUALIFIED LONG T...

Certificate

Semnat, cu toate semnăturile valide.

Semnături

Validare globală

Rev. 1: Semnată de Constantin Burdun <constantin.burdun@cert...

Semnătura este validă:

Sursă de autentificare obținută de la European Union Trusted Lists (E...

Aceasta este o Semnătură electronică calificată conform Regulament...

Documentul nu a fost modificat după aplicarea acestei semnături

Identitatea semnatarului este validă

Semnătura include un marcaj temporal încorporat.

Semnătura este activată pentru LTV

Detalii semnătură

Detalii certificat...

Ultima verificare: 2021.10.09 15:38:34 +03'00'

Câmp: Signature2 la pagina 1

Faceți clic pentru a vizualiza această versiune

Program de vizualizare certificate

Această casetă de dialog vă permite să vizualizați detaliile unui certificat și lanțul său integral de emiter. Detaliile corespund intrării selectate.

☐ Afișare globală căi de certificare găsite

certSIGN Qualified CA
Constantin Burdun <constant...

Sumar Detalii Revocare Autentificare Reguli Prevederi legale

Date certificat:

Nume	Valoare
Versiune	3
Algoritm semnătură	SHA256 RSA
Subiect	givenName=Constantin, sn=Burdun, c=RO...
Emitent	2.5.4.97=VATRO-18288250, cn=certSIGN Q...
Număr de serie	22 05 83 72 9F 5C B3 3D B0 62 8C 06
Validitatea începe	2021/05/17 10:22:21 +03'00'
Validitatea se încheie	2022/05/17 10:22:21 +03'00'
Instrucțiuni QC	<vezi detalii>
Utilizare cheie extinsă	Autentificare client, Protecție e-mail, Semn...

givenName=Constantin
sn=Burdun
c=RO
serialNumber=BC1
cn=Constantin Burdun

CONSTANTIN BURDUN – angajat la o
companie

Constantin Burdun Semnat digital de
Constantin Burdun
Data: 2021.10.09
15:36:05 +03'00'

Cum se “vad” semnăturile digitale - exemplu

Document de test.pdf - Adobe Acrobat Reader DC (32-bit)

Fișier Editare Vizualizare Semnare Fereastră Asistență

Pagina principală Instrumente QUALIFIED LONG T...

Certificate

Semnăt, cu toate semnăturile valide.

Semnături

Validare globală

Detalii semnătură

Detalii certificat...

Ultima verificare: 2021.10.09 15:38:34 +03'00'

Câmp: Signature2 la pagina 1

[Faceți clic pentru a vizualiza această versiune](#)

1 modificări diverse

Rev. 2: Semnată de Constantin Burdun <costin.burdun@gmail.com>

Semnătura este validă:

Sursă de autentificare obținută de la European Union Trusted Lists

Aceasta este o Semnătură electronică calificată conform Regulamentului UE 910/2014 Anexa I

Documentul nu a fost modificat după aplicarea acestei semnături

Semnat de utilizatorul curent

Semnătura include un marcat temporal încorporat.

Program de vizualizare certificate

Această casetă de dialog vă permite să vizualizați detaliile unui certificat și lanțul său integral de emiter. Detaliile corespund intrării selectate.

☐ Afișare globală căi de certificare găsite

certSIGN Qualified CA
Constantin Burdun <costin.bu

Sumar Detalii Revocare Autentificare Reguli Prevederi legale

Constantin Burdun <costin.burdun@gmail.com>

Emis de: certSIGN Qualified CA
CERTSIGN SA

Valid de la: 2021/06/09 19:23:06 +03'00'

Valid până la: 2022/06/09 19:23:06 +03'00'

Utilizare recomandată: Semnătură digitală, Nerepudiere, Autentificare client, Protecție e-mail, Semnarea documentului

Acest certificat este calificat în conformitate cu Regulamentul UE 910/2014 Anexa I

Cheia privată legată de acest certificat se află într-un dispozitiv de creare a semnăturilor calificate (QSCD)

Export...

Document de test.... x

Panou cu s

ALITATI:

CONSTANTIN BURDUN – angajat la o companie

Constantin Burdun Semnat digital de Constantin Burdun
Data: 2021.10.09 15:36:05 +03'00'

Cum stiu ca o semnatura electronica NU este avansata?

- **Indiciu– In vederea emiterii certificatului digital, in Politica de certificare a Autoritatii de certificare, nu exista specificat un proces de verificare a identitatii care sa garanteze indeplinirea cerintelor a si b din Art. 26 din Regulamentul EIDAS**
 - Pentru ca o semnatura electronica sa faca trimitere exclusiv la semnatar si sa permita identificarea semnatarului, trebuie ca procesul de verificare a identitatii sa fie unul corect, raportat la standarde, sau, cel putin, la bunele practici

Cum stiu ca o semnatura electronica NU este avansata?

- **Indiciu– In vederea emiterii certificatului digital, in Politica de certificare a Autoritatii de certificare, nu exista specificat un proces de verificare a identitatii care sa garanteze indeplinirea cerintelor a si b din Art. 26 din Regulamentul EIDAS**
 - Exemple de modalitati de verificare a identitatii care NU asigura crearea unei semnaturi electronice avansate
 - Transmiterea pe mail sau printr-o aplicatie a unui scan al cartii de identitate!!!
 - O discutie pe skype/WatsApp cu o persoana care face identificarea in care prezinti cartea de identitate!!!
 - Utilizarea unei aplicatii care face comparatie intre imaginea din poza din CI si o poza a persoanei, fara alte mecanisme suplimentare de verificare (ex. un document electronic de identitate) – **conform ETSI TS 119 461** – aparut in iulie 2021

Cum stiu ca o semnatura electronica NU este avansata?

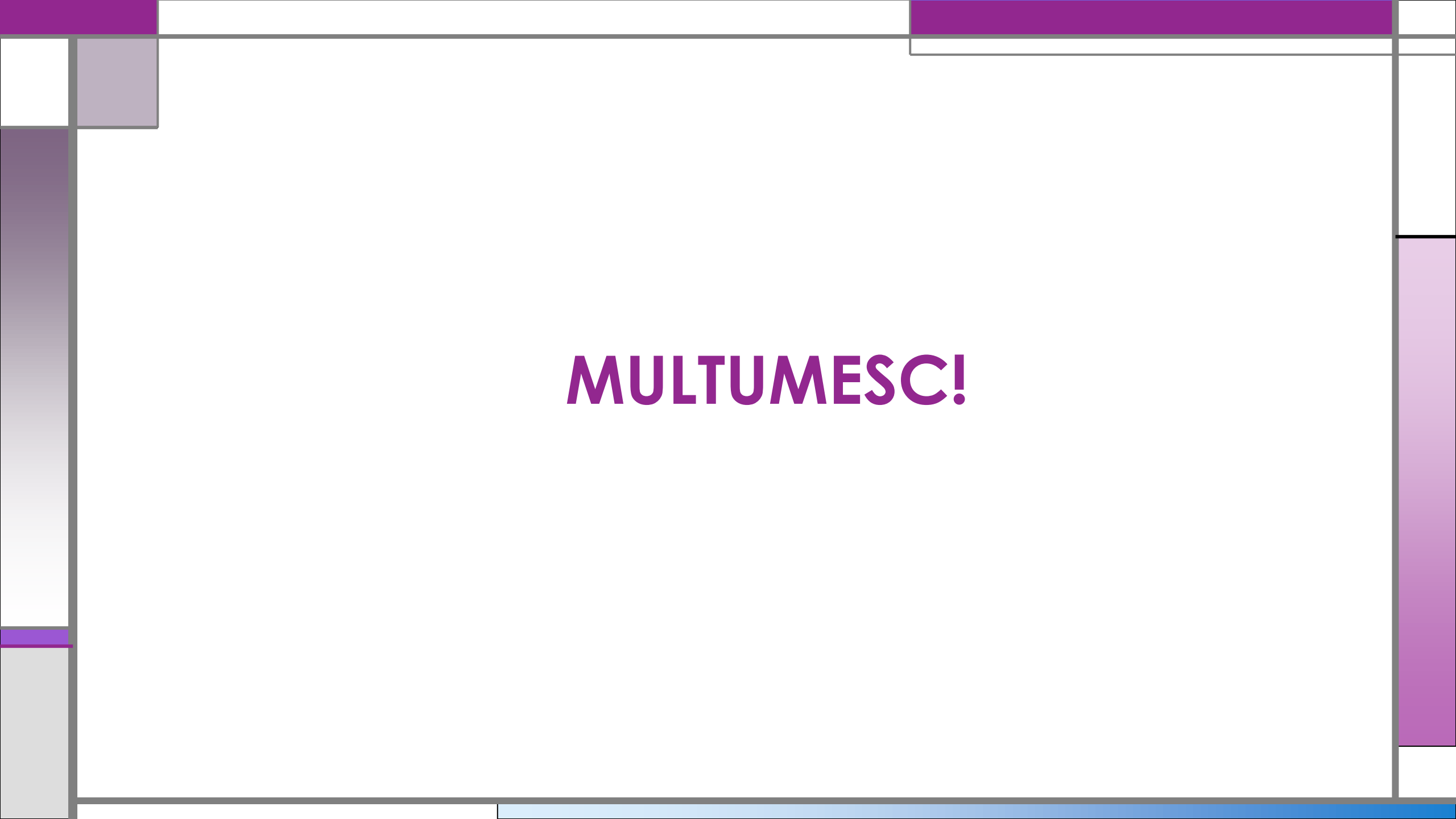
- **Indiciu – In Politica de certificare a Autoritatii de certificare, nu exista specificat un proces de protejare a cheii private a semnatarului, care sa garanteze ca semnatarul o poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său**
 - Exemple de modalitati de protectie a cheii private care NU asigura crearea unei semnaturi electronice avansate
 - Pastrarea cheii private intr-un fisier protejat cu parola
 - Transmiterea cheii private catre semnatar impreuna cu credentialele de access la aceasta

Concluzii

- Semnatura avansata este o categorie de tipuri de semnături electronice tinta, obiectiv, care, asa cum am aratat in discutiile precedente, reflecta actul de vointa al semnatarului, daca, intr-adevar sunt indeplinite cele 4 conditii de la art. 26 din Regulamentul EIDAS
- Indeplinirea acestor conditii nu este simpla si nici ieftina si este o impresie falsa ca o semnatura electronica avansata ne-calificata e mai ieftin de realizat decat o semnatura calificata, din cauza ca Regulamentul nu detaliaza decat cerinte pentru semnatura calificata (intotdeauna ceva foarte detaliat pare mult mai complicat decat ceva care nu este detaliat)
- Din cauza ca pot exista o multitudine de tipuri de semnături electronice, nu se pot emite “retete generale” pentru evaluarea unei semnături electronice avansate

Concluzii

- Putem însă să identificăm niste indicii care arată că o semnătură electronică NU este avansată:
 - Dacă mecanismul tehnic utilizat de semnatar nu se bazează pe semnătură digitală a acestuia, atunci acea semnătură electronică NU este avansată conform Regulamentului EIDAS
 - În acest sens, o semnătură electronică bazată pe autentificarea la email și/sau pe o semnătură desenată cu mouse-ul sau cu degetul pe ecran NU este o semnătură electronică avansată
 - Dacă procesul de verificare a identității în vederea emiterii certificatului digital al semnatarului nu demonstrează modul în care se garantează faptul că semnătura face trimitere exclusiv la semnatar și că permite identificarea semnatarului, atunci semnătură electronică NU este avansată
 - Dacă cheia privată a semnatarului nu este protejată corespunzător, astfel încât să se garanteze faptul că semnatarul o poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său, atunci semnătură electronică NU este avansată



MULTUMESC!