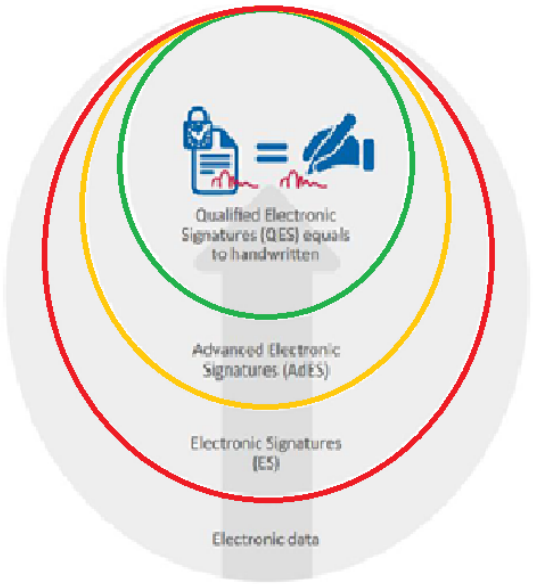
# Semnatura digitala. Certificatul digital

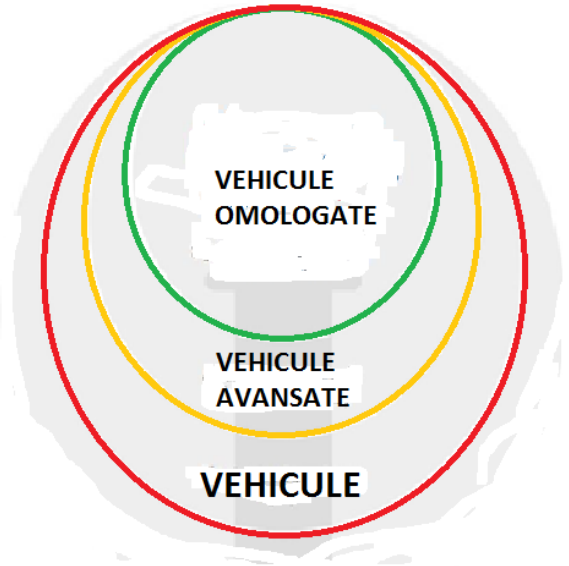
Costin Burdun

# Sa ne amintim din episodul precedent – analogia cu vehiculele

**CATEGORIILE DE SEMNATURI ELECTRONICE DEFINITE DE REGULAMENT**




**CATEGORII DE VEHICULE**



# Sa ne amintim din episodul precedent…

- Termenii de „**semnătură electronică**” si „**semnătură electronică avansată**” au fost introdusi inca din 1999 prin Directiva 1999/93 referitoare la semnatura electronica, inlocuita in 2014 de Regulamentul EIDAS

- Termenul de „**semnătură electronică**” defineste de fapt o **categorie (multime)** de tipuri concrete de astfel de semnaturi electronice, fiecare tip identificandu-se prin mecanismul tehnic si procedural prin care el este creat; aceste tipuri sunt extrem de variate, asa cum sunt, de exemplu, tipurile de vehicule

- Termenul de „ **semnătură electronică avansată**” defineste de fapt o **categorie (multime)** de tipuri concrete de astfel de semnaturi electronice, inclusa in multimea semnaturilor electronice, diferentiindu-se prin indeplinirea unor cerinte suplimentare; aceste tipuri sunt de asemenea extrem de variate si nici aceasta multime nu este cunoscuta de dinainte, asa cum nu se stiu nici care sunt vehiculele avansate din analogia noastra, pana cand nu sunt demonstrate cerintele de avansat

- Termenul de „ **semnătură electronică calificată**” defineste **un tip** de **semnătură electronică avansată,** prin indicarea mecanismului tehnic si procedural utilizat pentru crearea ei, mecanism dovedit ca indeplineste cerintele pentru semnatura avansata, asa cum un vehicul omologat din analogia noastra este certificat ca indeplineste cerintele pentru un vehicul avansat

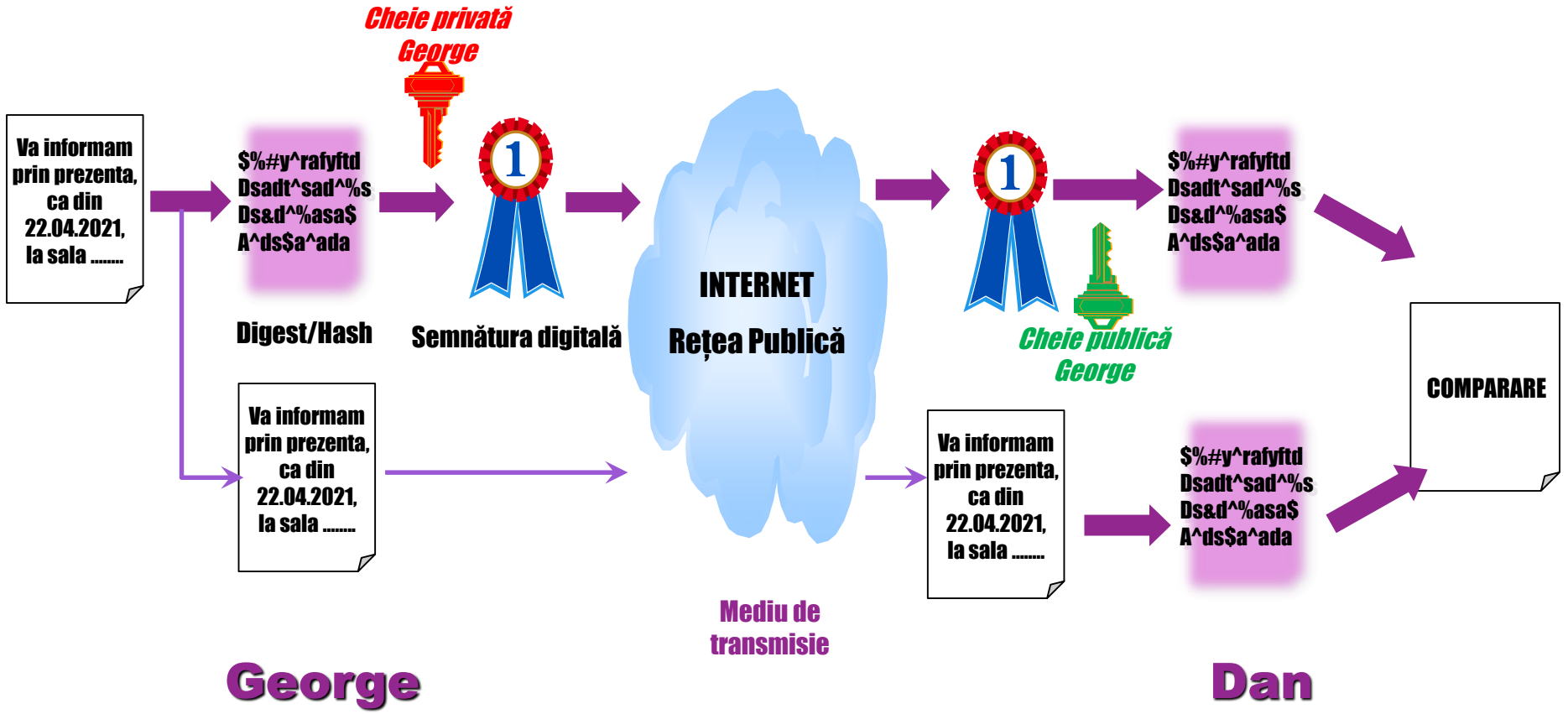
# Exemplu de tip de semnatura electronica – semnatura electronica bazata pe semnatura digitala

- **Semnatura digitala** este un **mecanism tehnic pentru crearea unei semnaturi electronice**
- Semnatura digitala 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 (rezumat)** 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

# Semnatura digitala – cum functioneaza

- Cateva notiuni de de baza

  https://en.wikipedia.org/wiki/Public-key_cryptography



# Cheie publică -> Certificat digital -> Autoritate de certificare

- Cheia publica trebuie sa fie certificata printr-un mecanism ca apartine unei anumite persoane, care detine cheia privata corespunzatoare, sub controlul sau
- Certificarea se face de către o Autoritate de certificare (CA - Certification Authority) prin emiterea asa numitului **certificat digital**
- Astfel, in comunicația dintre două entități, CA-ul reprezinta un terț de încredere (TTP – Trusted Third Party)

# Cheie publică -> Certificat digital -> Autoritate de certificare

- Certificatul digital este un sir de octeti ce contine informatiile personale ale titularului impreuna cu cheia sa publica
- Certificatul este emis si semnat digital de catre o Autoritate de certificare care garanteaza corespondenta dintre cheia publica si datele personale ale titularului mentionate in certificat

# Certificatul digital

- Informații cuprinse în certificatul digital:
  - Subiect
  - Emitent
  - Perioada de valabilitate
  - Cheia publică a subiectului
  - Număr serial
  - Politica de emitere a certificatului digital
  - Semnatura digitala a emitentului peste toate aceste date

# Participanți într-o infrastructura PKI

- Autoritatea de certificare
  - Gestioneaza certificatele digitale si garanteaza legatura cu identitatea fizica a subiectilor
- Titularii de certificate (Subiecti)
  - proprietarii perechilor de chei (privată, publică), utilizatori ai certificatelor digitale
- Părțile terte care se raporteaza la aceste certificate (relying parties)
  - au încredere în certificatele digitale ale altor utilizatori

# Componentele Autoritatii de Certificare

- Componenta de gestiunea certificatelor- CA (certification authority)
  - emite certificate (le semneaza)
  - menține informații despre starea certificatelor şi emite liste de certificate revocate (CRL)
  - publică certificatele neexpirate şi CRL
- Autoritatea de înregistrare – RA (registration authority)
  - verifică datele de identificare ale titularilor certificatelor
  - informațiile furnizate CA-ului despre un utilizator vor fi cele scrise în certificat
- Componenta de publicare (repository)
  - publică certificatele utilizatorilor şi CRL-urile
  - păstrează informațiile despre certificate pe termen lung

# Politica de certificare

- Legal
  - Răspundere

- Organizațional
  - Înregistrare in vederea emiterii certificatului digital
  - Distribuire chei private si certificate digititale
  - Revocare
  - Help Desk
  - Training

- Operațional
  - Locații securizate
  - Recuperare în cazul dezastrelor (Disaster Recovery)
  - Audituri

# In ce scopuri putem utiliza certificatele digitale

- Autentificare -> semnatura digitala
- Nerepudierea si integritatea datelor -> semnatura digitala
- Confidentialitatea datelor -> criptare

# Concluzii

- 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**

# MULTUMESC!