



certSIGN®

Companie
a grupului **UTi**

Serviciul de marcare temporală



Agenda

- ❖ **Ce este marca temporală**
- ❖ **De ce este necesară marca temporală**
- ❖ **certSAFE Time Stamping Authority**

Ce este marca temporală

23 martie 2009



Marca temporală

- ❖ **Legea 451 din 2004**
 - ❖ **“Colecție de date în formă electronică, atașată în mod unic unui document electronic; ea certifică faptul că anumite date în formă electronică au fost prezentate la un moment de timp determinat furnizorului de servicii de marcare temporală”**
- ❖ **Marca temporală**
 - ❖ **Numar serial**
 - ❖ **Rezumatul documentului (hash)**
 - ❖ **Momentul de timp (data și ora)**
 - ❖ **Semnătura electronică a furnizorului mărcii temporale**



Serviciul de marcare temporală

• Serviciu de încredere

- Garantează și certifică momentul de timp asociat unui document electronic**
- Garantează înălțuirea unică a mărcilor temporale (nu se emit mărci temporale “din urmă”)**

• Serviciul de marcare temporală

- Infrastructură hardware și software pentru generarea și gestionarea mărcilor temporale emise**
- Personal**
- Politică și cod de practici și proceduri publice**
- Garanție financiară**



De ce este necesară marca temporală

23 martie 2009



Non –repudiabilitatea semnăturii electronice pe termen lung

❖ Scenariu:

❖ 19.03.2009

- ❖ Dan semnează electronic un document prin care se obligă să facă o plată către George în data de 01.04.2009
- ❖ George verifică semnătura electronică a lui Dan de pe document și verificarea este OK

❖ 23.03.2009

- ❖ Dan merge la Autoritatea de Certificare și revocă certificatul motivând că a pierdut token-ul criptografic
- ❖ Autoritatea de certificare revocă certificatul și publică lista de certificate revocate în care apare data revocării 23.03.2009 pentru certificat



Non –repudiabilitatea semnăturii electronice pe termen lung

❖ **01.04.2009**

- ❖ **George nu face plata**
- ❖ **Dan îi prezintă documentul semnat electronic de George**
- ❖ **George neagă faptul că a semnat el documentul, deoarece el a pierdut token-ul și certificatul său a fost revocat**
- ❖ **Dan îi arată lista de certificate revocate din care rezultă că revocarea a avut loc după semnarea documentului de către George, dată la care certificatul era valid**
- ❖ **George susține contrariul**
- ❖ **Concluzie: inexistența unui moment de timp, garantat de un furnizor de marcare temporală, asociat cu semnătura electronică face greoaie, chiar imposibilă validarea unei semnături electronice ulterior**

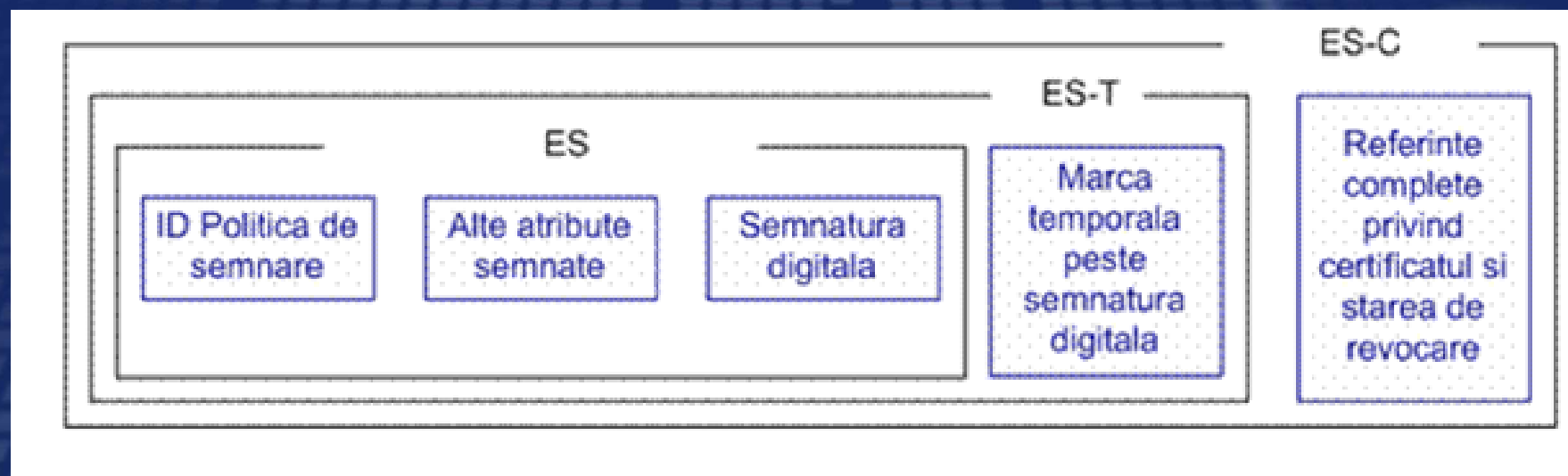


Non –repudiabilitatea semnăturii electronice pe termen lung

❖ Concluzii:

- ❖ Inexistența unui moment de timp, garantat de un furnizor de marcarea temporală, asociat cu semnătura electronică face greoaie, chiar imposibilă validarea unei semnături electronice ulterior**
- ❖ Calitatea unei semnături electronice de a fi non-repudiabilă se poate pierde**
- ❖ Semnătura electronică trebuie să fie asociată cu momentul de timp al semnării**

Formate de semnătură conform reglementărilor tehnice UE



Formate de semnătură conform reglementărilor tehnice UE

- ❖ **PKCS7**
- ❖ **Noi standarde tehnice pentru implementarea formatelor de semnătură electronică ce se au în vedere în viitor**
 - ❖ **XAdES – XML Advanced Electronic Signatures**
 - ❖ **CAAdES – CMS Advanced Electronic Signatures**
- ❖ **CERTSIGN – singura companie românească participantă la testele de interoperabilitate organizate de ETSI (European Telecommunications Standards Institute)**



Aplicațiile mărcii temporale

- **Notar electronic (Legea 589 din 2004)**
- **Arhivare electronică (Legea 135 din 2007)**
- **Facturare electronică (Legea 260 din 2007)**
- **Registratură electronică**
- **Poșta electronică cu confirmare de primire**

certSAFE Time Stamping Authority

23 martie 2009



certSAFE Time Stamping Authority

- ❖ **Singurul serviciu de marcare temporală în conformitate cu Legea mărcii temporale**
- ❖ **Publicat în Registrul furnizorilor de marcă temporală gestionat de ANC**
- ❖ **Serviciu disponibil 24/7 implementat printr-un sistem informatic dedicat certificat ISO 27001 din punct de vedere al managementului securității informatice**
- ❖ **Cheile criptografice gestionate cu dispozitive hardware criptografice (HSM) certificate FIPS 140-2 Level 3**
- ❖ **Are la bază produsul software certSAFE TS din suita certSAFE acreditate de către ORNISS pentru a proteja informații clasificate Secret de Stat, SECRET**
- ❖ **Centru de recuperare în caz de dezastru**



Concluzii

23 martie 2009



Concluzii

- ❖ **certSIGN oferă:**
 - ❖ **Serviciul de marcarea temporală certSAFE Time Stamping Authority**
 - ❖ **Pentru utilizarea serviciului**
 - ❖ **Kit de semnătură electronică ce permite asocierea semnăturii electronice cu un moment de timp pentru orice tip de fișier**
 - ❖ **Dezvoltarea de componente software la cheie pentru marcarea temporală a documentelor electronice în organizație și integrarea acestor componente**
 - ❖ **Performanțe ridicate în marcarea temporală de documente “bulk”**

Întrebări?

23 martie 2009



Contact

Constantin Burdun

Director Adjunct

certSIGN

Telefon fix: 004-021-311.9901

Fax: 004-021-311.9905

Mobil: 004-0723.275.582

e-mail: costin.burdun@certsign.ro

