



107A, Sos Oltenitei
Sector 4, CP 041303
Bucharest,Romania

Tel: 0040 21 3119904
Fax: 0040 21 3119905
email:office@certsign.ro

Instrucțiunile practice de marcarea temporală

Cuprins

1	Solicitarea de marcare temporala.....	3
1.1	Software client de marcare temporala.....	3
1.2	ClickSIGN.....	4
2	Raspunsul la solicitarea de marcare temporala.....	4
2.1	Intervalul de timp in care se primeste raspunsul la cererea de marcare temporala: modalitate de calcul si eroarea admisibila	5
3	Aplicatia software client pentru serviciile de marcare temporala.....	6
3.1	Descriere functionare si ghid de utilizare	6
3.2	Verificarea online gratuita a marcilor temporale	8
3.3	Verificarea marcilor temporale si dupa expirarea certificatului	10

1 Solicitarea de marcare temporala

1.1 Software client de marcare temporala

Solicitarea unei marci temporale se face prin folosirea unui software-client de marcare temporala, de catre un utilizator care are acces la serviciul de marca temporala al furnizorului.

Inainte de prima accesare a serviciului:

1. solicitantul obtine accesul la serviciul de marca temporala prin contactarea furnizorului de servicii (prin incheierea unui contract de furnizare de servicii)
2. solicitantul obtine si instaleaza echipamentele hardware si software necesare (calculator, sistem de operare etc.), si accesul la internet printr-un furnizor de astfel de servicii
3. solicitantul obtine si instaleaza software-ul client de marca temporala pe calculatorul sau
4. solicitantul configureaza software-ul client cu:
 - datele de acces la autoritatea de marca temporala
 - parametrii impliciti de compunere a marcii temporale:
 - algoritmul de hash folosit
 - includerea nonce-ului
 - politica sub care se doreste emiterea marcii temporale
 - indicator de includere in raspuns a certificatului autoritatii

Solicitarea propriu-zisa:

1. solicitantul alege in cadrul aplicatiei-client documentul pe care doreste aplicarea marcii temporale
2. daca aplicatia-client permite, solicitantul va alege/modifica parametrii impliciti de compunere a cererii de marca temporala
3. solicitantul verifica daca parametrii cererii sunt cei doriti, apoi comanda din aplicatia-client trimiterea cererii la furnizor prin Internet.

1.2 ClickSIGN

Pasii anteriori (alegerea parametrilor si trimiterea solicitarii) pot fi executati si automat, in cadrul procesului simultan de semnare si marcare temporala a unui document folosind aplicatia-client **clickSIGN**.

2 Raspunsul la solicitarea de marcare temporala

Prelucrarea solicitarii la furnizor:

1. furnizorul de servicii temporale primeste solicitarea de marcare temporala de la client
2. furnizorul verifica:
 - dreptul clientului de acces la serviciu
 - corectitudinea structurii de date din care este formata solicitarea de marca temporala
 - acceptabilitatea parametrilor solicitarii (algoritmul hash, politica, extensii)
 - precizia timpului propriu
3. daca solicitarea a indeplinit toate conditiile pentru acceptabilitate, sistemul informatic executa urmatoarele:
 - genereaza marca temporala
 - o stocheaza in registrul propriu
 - consemneaza evenimentul (cu detaliile relevante) in cadrul jurnalelor proprii
 - genereaza raspunsul de marca temporala
 - trimite solicitantului raspunsul generat
4. daca nu, sistemul informatic executa urmatoarele:
 - consemneaza evenimentul (cu detaliile relevante) in cadrul jurnalelor proprii
 - genereaza un raspuns de eroare
 - trimite solicitantului raspunsul generat

Autoritatea genereaza raspunsul de marca temporala conform structurii TimeStampResponse definita in RFC 3161.

Continutul raspunsului:

- statutul PKI (PKIStatus, RFC 3161): arata daca solicitarea a fost acceptata sau nu, si optional motivele pentru care nu a fost acceptata solicitarea
- marca temporala propriu-zisa (TimeStampToken-ul descris la capitolul anterior): daca este cazul (solicitarea a fost acceptata)

Raspunsul de marca temporală este impachetat într-un mesaj HTTP a cărui structură este de asemenea descrisă în RFC 3161.

Mesajul astfel format constituie răspunsul la solicitarea de marcă temporală, răspuns care este trimis solicitantului prin aceeași modalitate de transport prin care a fost primit (conexiune internet).

2.1 Intervalul de timp în care se primește răspunsul la cererea de marcă temporală: modalitate de calcul și eroarea admisibilă

Componentele principale ale timpului de răspuns

- t_{wait} - intervalul de timp de așteptare în coadă
 t_{ts} - intervalul de timp necesar pentru crearea marcii temporale

Estimarea valorilor componentelor

t_{wait} = min: 0, max: 10 s , tipic: 50 ms (pentru o coadă de așteptare de 10 de cereri la 5 ms/cerere)

t_{ts} : 3 - 10 ms , în funcție de încărcarea sistemului informatic - tipic 5 ms

Estimarea timpului total de răspuns

Valoare minimă : 3 ms

Valoare tipică: 55 ms

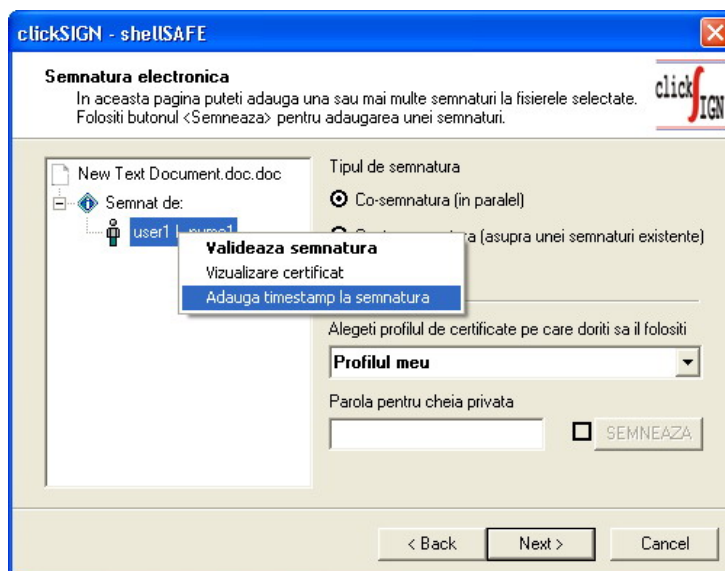
Valoare maximă: 10 secunde (determinat practic de coadă de așteptare)

3 Aplicatia software client pentru serviciile de marcare temporala

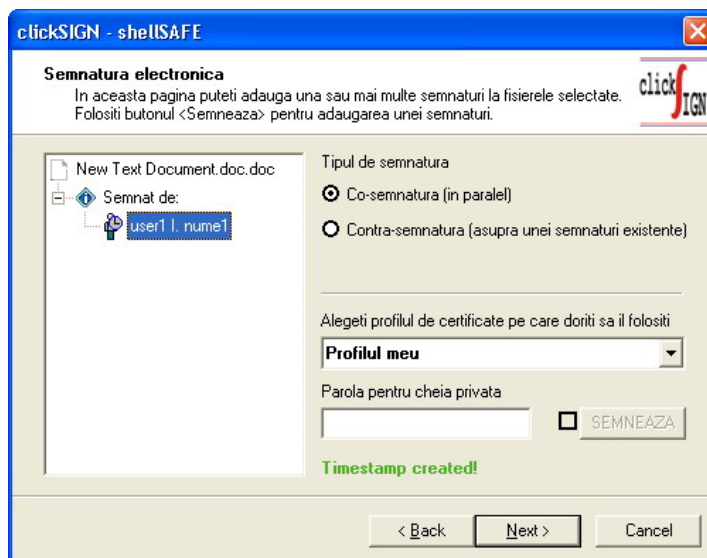
3.1 Descriere functionare si ghid de utilizare

Folosind aplicatia clickSIGN, marcarea temporala a unui document poate fi aplicata impreuna cu semnatura digitala a acestuia. O marca temporala este asociata cu o semnatura si certifica faptul ca respectiva semnatura exista la un moment de timp dat. Marca temporala poate fi adaugata in momentul semnarii fisierului sau mai tarziu.

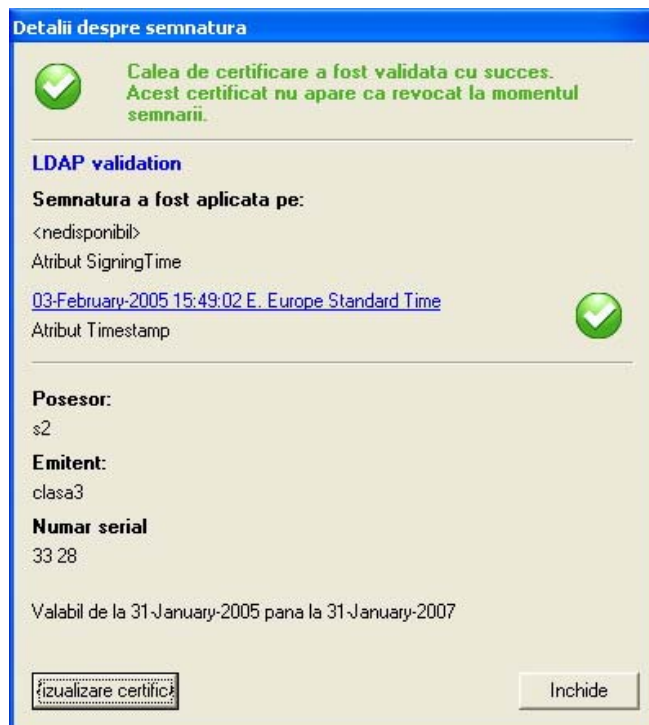
Pentru a adauga o marcare temporala la documentul semnat utilizatorul da click cu butonul drept pe o semnatura din arborele de semnaturi si selecteaza "Adauga timestamp la semnatura".



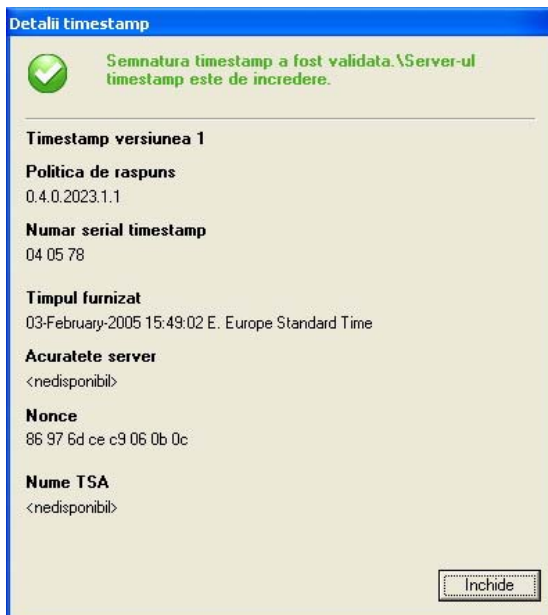
In momentul adaugarii unei marcare temporale va apare un mesaj sub campul "Parola pentru cheia privata" care afiseaza starea operatiei.



O marcare temporală poate fi vizualizată în fereastra care afișează informațiile despre semnătură.



Pentru a vizualiza detaliile marcii temporale utilizatorul trebuie să dea click pe link-ul de culoare albastră.



Daca o marcare temporara a fost alterata un x rosu va aparea langa numele de utilizator din arborele de certificate.

3.2 Verificarea online gratuita a marcilor temporale

1. Verificare prin interfata Web

Componenta Web a sistemului face posibila existenta unui serviciu public permanent de verificare online a marcilor temporale. Acest serviciu poate fi accesat la adresa <http://tss.certsign.ro/ts/> .

Utilizatorul va incarca marca temporala folosind butonul “Alege” aferent “Marca temporala” si apoi va incarca fisierul pentru care a fost generat aceasta marca folosind butonul “Alege” aferent “Fisier”.



Figura 1 – Verificare marca temporală

Dupa incarcarea marcii, aplicatia va afisa urmatoarele date de identificare ale sale:

- Serial
- Timp
- Algoritm
- Hash
- Rezultat verificare (poate VALID daca marca temporală este valida sau INVALID; pentru cazul INVALID se va afisa si motivul pentru care marca temporală a fost considerata invalida)

si ale fisierului:

- Hash
- Rezultat verificare hash (daca hash-ul fisierului coincide cu cel al marcii temporale rezultatul va fi afisat pe un fundal verde, altfel raspunsul va fi afisat pe un fundal rosu)



Secure your on-line transactions

Registru marci temporale **Verificare marca temporală**

Verificare marca temporală

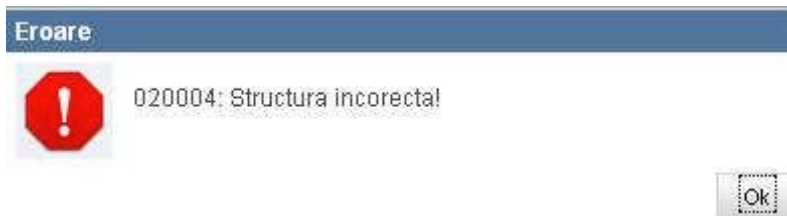
Detalii marca temporală

Marca temporală	catalog.TST	Alege	Fisier	catalog.pdf	Alege
Serial	35F245B34613887ABA3DE47D48ACE5B4DBE02040			Hash	6B 29 16 56 00 44 4A C3 00 56 29 BB 5F B1 3C 7E 76 03 1E DE
Timp	20081112100034.675344Z			Rezultat hash	Hash-ul fisierului coincide cu hash-ul marcii temporale
Algoritm	SHA1				
Hash	6B 29 16 56 00 44 4A C3 00 56 29 BB 5F B1 3C 7E 76 03 1E DE				
Rezultat verificare	VALID				

Reseteaza

Figura 2 – Detalii verificare marca temporală (rezultat valid)

Daca fisierul incarcat nu este o marca temporală, sau este o marca temporală cu o structura corupta, va fi afisat un mesaj de eroare.

**Figura 3 - Eroare structura invalida**



Secure your on-line transactions. Registru marci temporale Verificare marca temporală

Verificare marca temporală

Detalii marca temporală

Marca temporală: Fisier:

Serial: 14F4065233E4530C12CFA007770932C4FC0A0C8C

Timestamp: 2009 10 23 12 15 39.185738Z

Algorithm: SHA1

Hash: D6 91 3A EE CE DB 24 3A D0 E5 C1 4B 07 F8 33 1B E6 81 87 F2

Rezultat verificare: **INVALID** - Froare verificare semnatura!

Figura 4 - Detalii verificare marca temporală (rezultate invalide)

Butonul “Reseteaza” va sterge din pagina rezultatele ultimei verificari.

2. Verificare prin aplicatia software clickSIGN Verify sau clickSIGN

Marcile temporale aplicate documentelor semnate cu aplicatia clickSIGN pot fi verificate si cu ajutorul aplicatiei software clickSIGN Verify, care poate fi descarcata gratuita de la adresa <http://certsign.ro/certsign/resurse/download> .

In timpul verificarii, aplicatia efectueaza urmasorii pasi:

- Pas 1. Se verifica semnatura.
- Pas 2. Se verifica validitatea semnaturii marcii temporale
- Pas 3. Se verifica starea certificatului de semnare a marcii temporale
- Pas 4. Se verifica daca messageImprint-ul aflat in marca temporală este acelasi cu cel calculat din semnatura (acelasi algoritm ca si la crearea request-ului)

3.3 Verificarea marilor temporale si dupa expirarea certificatului

Pentru verificarea marilor temporale si dupa expirarea certificatului cu care s-au semnat aceste marci, certSIGN ofera clientilor sai arhivarea acestor certificate si ale autoritatilor de certificare emitente, impreuna cu CRL-urile aferente.