

SSL (SECURE SOCKETS LAYER)

Mulți dintre dumneavoastră, măcar întâmplător, ați dat peste acest termen, SSL. La ce se referă acesta? Tehnologia SSL vă ajută să vă protejați site-ul și oferă o garanție de încredere în site-ul dumneavoastră în fața vizitatorilor. Certificatul SSL conține date unice, autentice, despre deținătorul certificatului și asigură criptarea datelor confidențiale pe timpul tranzacțiilor online.

Când aveți nevoie de un certificat SSL? Ori, din altă perspectivă, când ați fi interesat de verificarea existenței unui asemenea certificat? Iată câte situații:

- când aveți un magazin virtual și acceptați plata prin card; desigur, dacă sunteți client al unui asemenea magazin vă puteți interesa dacă tranzacția este sigură prin verificarea existenței unui certificat SSL;

- protecția autentificării pe propriul site;

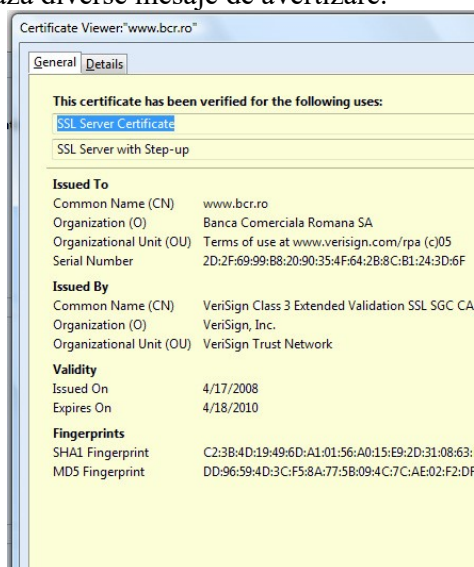
- atunci când procesați date confidențiale, cum sunt datele personale.

Orice certificat SSL constă dintr-o cheie publică și o cheie privată. Cheia publică este folosită pentru criptare, iar cea privată pentru decriptare. Atunci când un browser accesează un server securizat, are o loc o autentificare între server și client (browserul web). O metodă de criptare este stabilită între cele două entități și este o stabilită o cheie unică de sesiune pentru transmiterea securizată a datelor.



Semnul exclamării indicat de săgeata roșie sugerează că există o problemă cu certificatul digital.

Dacă nu ați observat deja, la accesarea unui server, browserul dumneavoastră cere și afișează (dacă are ce) date despre certificatul digital. În cazul în care certificatul a expirat ori lipsesc date, browserul afișează diverse mesaje de avertizare.



Certificat BCR (poate fi vizualizat online de pe pagina BRC.ro).
Certificatul, după cum se vede, este eliberat de VeriSign.

Semnarea documentelor Office. Certificate digitale (Avoco secure2trust, IntelliSafe Vault).

Avoco secure2trust: Gestionează drepturile întreprinderii pentru a proteja conținutul documentelor. secure2trust vă permite să controlați ce persoane accesează conținutul și ce pot

face aceste persoane cu conținutul, precum și procesul de aprobare a conținutului utilizând semnături digitale. secure2trust se integrează în sistemele de autentificare ale întreprinderii, cum ar fi Active Directory și certificatele digitale, pentru a se asigura că informațiile sensibile și proprietatea intelectuală sunt accesate doar de persoanele care au dreptul.

IntelliSafe®: Semnează digital, trimite și stochează în siguranță documentele. IntelliSafe® oferă aplicații cu drept de autor pentru semnături digitale, care asigură autenticitatea și originalitatea fișierelor. IntelliSafe Vault® acceptă sistemul Office 2007 și se adresează nevoilor oamenilor de afaceri care realizează avantajele tranzacțiilor și aprobărilor electronice. IntelliSafe oferă posibilitatea de a crea, de a semna și de a stoca în siguranță documente legale, de autoritate, într-un mediu complet virtual, direct de la Microsoft Office.

Semnați digital un document din aproximativ aceleași motive pentru care ați semna un document pe hârtie. O semnătură digitală se utilizează pentru a autentifica informațiile digitale — cum ar fi documente, mesaje de poștă electronică și macrocomenzi — utilizând criptografia informatică. Semnăturile digitale contribuie la stabilirea următoarelor fapte:

Autenticitate - Semnătura digitală contribuie în a asigura că semnatarul este cel care pretinde că este.

Integritate - Semnătura digitală contribuie în a asigura că un conținut nu a fost modificat sau alterat de la momentul în care a fost semnat digital.

Nerepudiare - Semnătura digitală contribuie în a demonstra tuturor părților care este originea conținutului semnat. „Repudiare” se referă la acțiunea unui semnatar care neagă orice asociere cu conținutul semnat.

Pentru aceste asigurări, creatorul de conținut trebuie să semneze digital conținutul utilizând o semnătură ce îndeplinește următoarele criterii:

- Semnătura digitală este validă.
- Certificatul asociat semnăturii digitale este curent (neexpirat).
- Persoana sau organizația care semnează, cunoscută cu numele de editor, este de încredere.
- Certificatul asociat cu semnătura digitală a fost emis către editorul semnatar de o autoritate de certificare recunoscută.

Există două moduri de a utiliza semnăturile digitale pentru a semna documente Office:

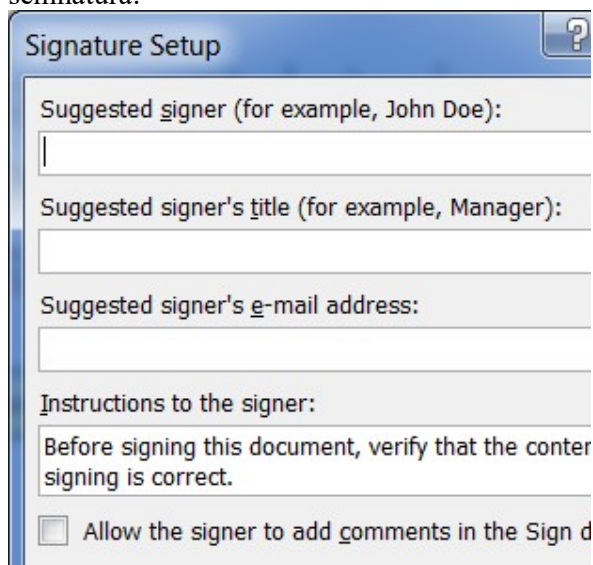
1. Adăugați linii de semnătură vizibile la un document pentru a captura una sau mai multe semnături digitale.
2. Adăugați o semnătură digitală invizibilă la un document.

În următoarele secțiuni sunt descrise diferențele între aceste două metode și detalii despre modul cum se semnează digital un document într-unul dintre aceste două moduri.

Crearea unei linii de semnătură în Word sau Excel

1. În document sau în foaia de lucru, plasați indicatorul unde doriți să creați o linie de semnătură.
2. Pe fila **Inserare**, în grupul **Text**, faceți clic pe lista **Linie de semnătură**, apoi faceți clic pe **Linia de semnătură Microsoft Office**.

3. În caseta de dialog **Configurare semnătură**, tastați informațiile care vor apărea sub linia de semnătură:



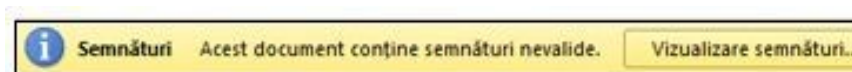
- **Sugestie pentru semnatar** Numele întreg al semnatarului.
- **Sugestie pentru funcția semnatarului** Funcția semnatarului, dacă este cazul.
- **Sugestie pentru adresa de e-mail a semnatarului** Adresa de e-mail a destinatarului, dacă este necesar.
- **Instrucțiuni pentru semnatar** Adăugați instrucțiuni pentru semnatar.

4. Selectați una sau ambele dintre următoarele casete de selectare:

- **Se permite semnatarului să adauge comentarii în caseta de dialog Semnătură** Permite utilizatorului să tasteze un scop pentru semnare.
- **Se afișează data semnării în linia semnăturii** Data semnăturii va apărea odată cu semnătura.

Pentru a adăuga linii de semnătură suplimentare, repetați acești pași.

Dacă documentul rămâne nesemnat, apare Bara de mesaje **Semnături**. Faceți clic pe **Vizualizare semnături** pentru a finaliza procesul de semnare.



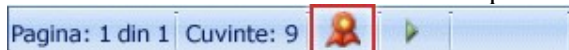
X
Tasca Nicolae
Sefu

Adăugarea unei semnături digitale invizibile la un document.

Dacă nu este necesar să inserați linii de semnătură vizibile în document, dar tot mai doriți să oferiți asigurări pentru autenticitatea, integritatea și originea unui document, aveți posibilitatea

să adăugați o semnătură digitală invizibilă la document. Semnăturile digitale invizibile se pot adăuga la documente Word, registre de lucru Excel și la prezentări PowerPoint.

Spre deosebire de o linie de semnătură Office, o semnătură digitală invizibilă nu este vizibilă chiar în conținutul documentului, dar destinatarul documentului pot determina dacă documentul a fost semnat digital, vizualizând semnătura digitală a documentului sau privind la butonul Semnături din bara de stare din partea de jos a ecranului.



După ce un document a fost semnat digital, devine doar în citire pentru a împiedica modificările.

Faceți clic pe butonul Microsoft Office , indicați spre *Pregătire*, apoi pe *Adăugare semnătură digitală*.

Dacă doriți să enunțați scopul pentru semnarea documentului, tastați aceste informații în caseta de sub Scopul semnării acestui document în caseta de dialog Semnare.

Faceți clic pe Semnare.

Pasii de depunere a unei cereri si de primire a unei semnături digitale personale gratuite de la TC TrustCenter (<https://www.trustcenter.de>)

Certificatele SSL sunt oferite contra cost de catre aceasta organizatie

1. Accesam http://www.trustcenter.de/en/products/tc_internet_id.htm

- » International X.509 standard
- » Entry in the directory serviceAufnahme in den Verzeichnisdienst
- » Revocation service
- » Online Infocenter (no telephone support)

You will be notified by e-mail before your certificate expires, so you apply for a new certificate

Please note: to enroll online for a certificate it is required to generate a key pair on your PC local JavaScript has to be enabled. In case of using MS Internet Explorer make sure browser options allow ActiveX controls.

Price Information

We offer TC Internet ID free of charge, including e-mail address check and delivery. TC Internet personal, private use only - commercial users please refer to **TC Business ID**.

[Request Certificate](#)

If any questions arise before or while requesting TC Internet ID you will find respective information [online knowledge base](#). Telephone support is not provided for this free of charge product

Se tasteaza Request Certificate

Se completeaza cererea:

https://www.trustcenter.de/RetailStore/cid/CustomerDataInput.action

Download Fringe... Download IObit Free... Biblioteca Universită... Utilizarea și program... Fringe Season 4 Sub... www.physics.pub.ro... 2. Curent alternativ |... Cp

Certificate request TC Internet ID

Step 1: Customer data Step 2: Finalization Confirmation

Customer data

Applicant

1 Salutation*
☒ Mr.
☐ Ms.

2 Title
 std
 Prof. Dr. PhD.

3 Name and Surname (given name and family name)*
 Noroc Vitlu

4 Street and number*
 12ds
 24 Main Street

5 ZIP code and location*
 12312 bilboua

6 State or province
 MD
 Texas

7 Country*
 Moldova

8 Email address*
 vicu07@list.ru
 webmaster@stonehillbaker.com

Request overview

Product: TC Internet ID
 Validity: 1 year -- €0.00
 Price: €0.00

Apoi next. Se testeaza cererea de revocare si se accepta termenii:

https://www.trustcenter.de/RetailStore/cid/CustomerDataInput.action

Download Fringe... Download IObit Free... Biblioteca Universită... Utilizarea și program... Fringe Season 4 Sub... www.physics.pub.ro... 2. Curent alternativ |... Cp

Certificate request TC Internet ID

Step 1: Customer data Step 2: Finalization Confirmation

Customer data

Applicant

1 Salutation*
☒ Mr.
☐ Ms.

2 Title
 std
 Prof. Dr. PhD.

3 Name and Surname (given name and family name)*
 Noroc Vitlu

4 Street and number*
 12ds
 24 Main Street

5 ZIP code and location*
 12312 bilboua

6 State or province
 MD
 Texas

7 Country*
 Moldova

8 Email address*
 vicu07@list.ru
 webmaster@stonehillbaker.com

Request overview

Product: TC Internet ID
 Validity: 1 year -- €0.00
 Price: €0.00

Succes!!

https://www.trustcenter.de/RetailStore/cid/ConfirmationInput.action

Download Fringe... Download IObit Free... Biblioteca Universită... Utilizarea și program... Fringe Season 4 Sub... www.physics.pub.ro... 2. Curent alternativ |... Cp

TRUSTCENTER
 Now part of Symantec

Certificate request TC Internet ID

Step 1: Customer data Step 2: Finalization Confirmation

Confirmation

✓ You request has been successfully submitted to TC TrustCenter.
 ✓ Your request number is: 408257505
 You'll need that number for potential support requests.

Request overview

Request number 408257505

Product: TC Internet ID
 Validity: 1 year -- €0.00
 Price: €0.00

Your Promotion Code: (no value)

Certificate data:

Name (first name, given name): Noroc
 Last name: Vitlu
 Location: bilboua
 State or province: MD
 Country: Moldova

Personal Information:

.....

Next step

As soon as your request has been approved you will be informed and the requested certificate delivered via the order status web page. The required URL and password to access the web page will be provided by separate emails.

Further links

[Back to TC TrustCenter home page](#)

Do you have any questions concerning your certificate request? Please contact us -- our support will assist you during European business hours.

Mesajul de confirmare:

📧 **Your TC Internet ID request no. 408257585 has been approved**

От кого: certificate@tctrustcenter.com 
Кому: vicu07@list.ru
Сегодня, 23:05  1 файл

Dear std Vitu,

You have requested a TC Internet ID with the following data:

Name:..... Noroc Vitu
Country:..... Moldova

We confirm your request with the order ID 408257585.

Issuance of the Certificate

To issue your certificate you have to generate a respective key pair on the order status webpage.

The required password to access the order status webpage will be provided to you in a separate email.

Order status webpage:

<https://www.trustcenter.de/RetailStore/cid/Login.action?loginName=ZNacOtdGD0>

After key generation the certificate will be issued and installed in your browser instantly.

Please Note: After you have successfully installed your certificate, we highly

If you have no access to your key, you can initiate the revocation by phone:

Phone: +49 40 / 80 80 26-113

After stating your revocation password, your certificate will be blocked.

Support

For technical support, please contact:

<http://www.verisign.com/support/contact/index.html>

Kind regards,

Your TC TrustCenter Team

--

TC TrustCenter GmbH - Now part of Symantec

Sonninstrasse 24-28

20097 Hamburg

Phone: +49 40 80 80 26-0, Fax: +49 40 80 80 26-127

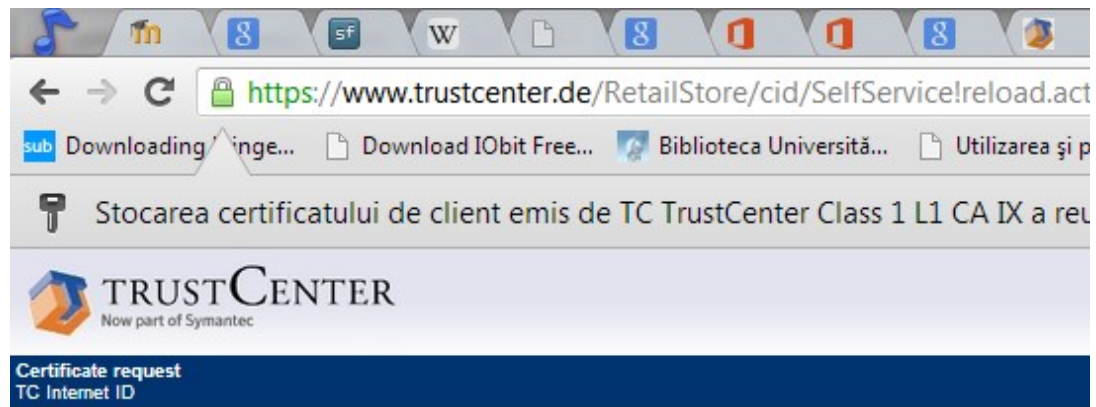
E-mail: registration@trustcenter.de, Internet: www.trustcenter.de

Managing Directors: Austin McCabe, Norman Osumi

AG Hamburg, HRB 96168

This e-mail has been digitally signed. If your e-mail software does not support the necessary validation feature, please disregard.

Accesam link-ul indicat in mail:



Request Status

Overview

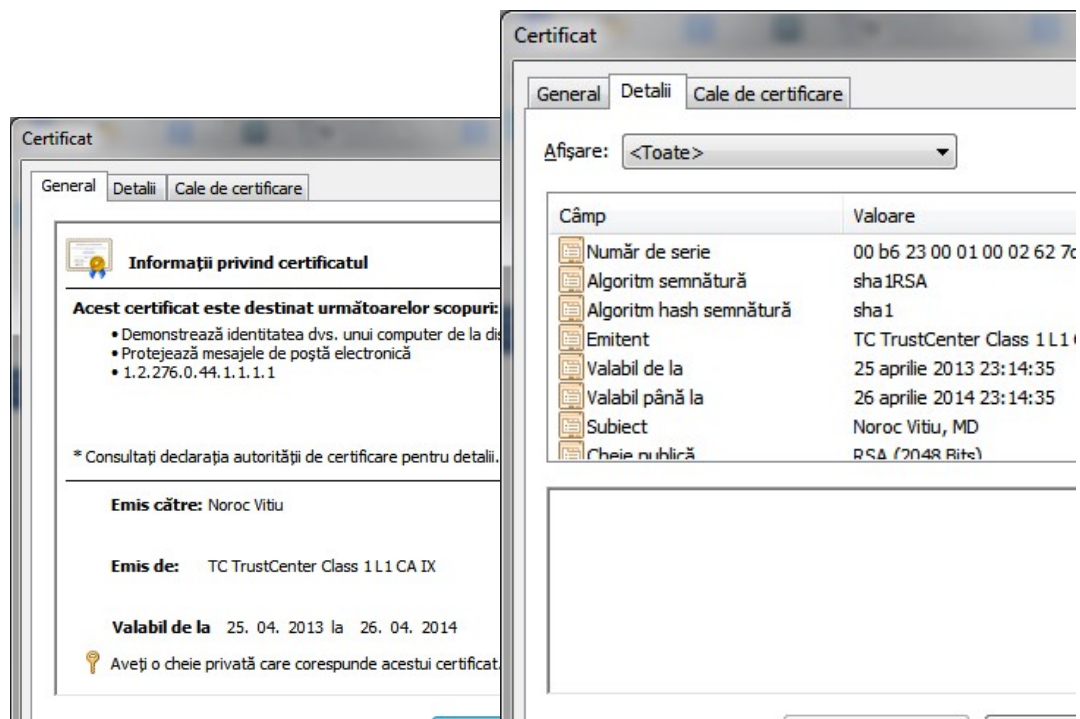
Request number:	408257585
Reference id:	f6894c7bc45849dbc54f3e8df5e2ce97ce7ea03f
Product:	TC Internet ID
Validity:	1 year -- €0.00
Processing status of your certificate request:	Approved

Your Certificate

Instalam certificatul:



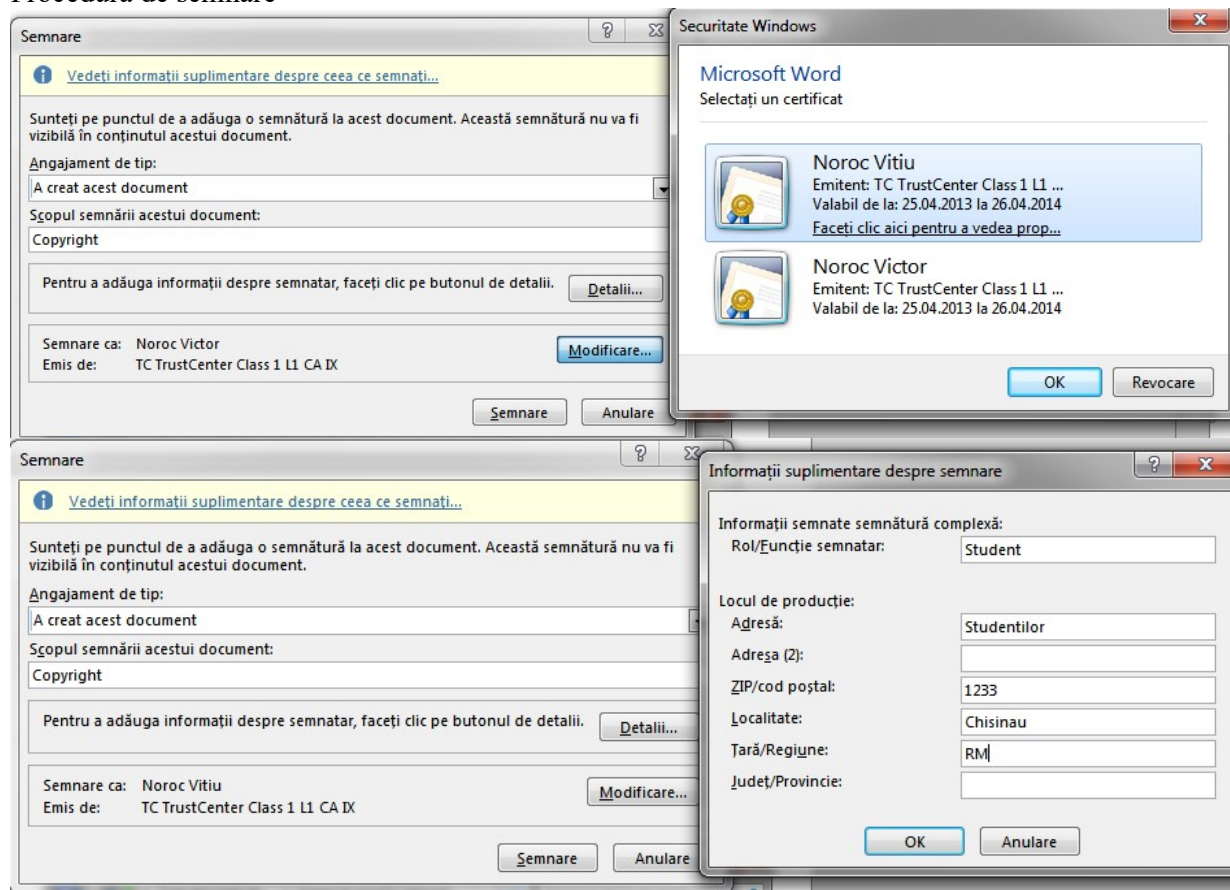
Il deschidem, aici avem acces la mai multe informatii despre certificat (detinator , termen de valabilitate, algoritm de criptare etc.):



Semnarea unui document Office Word:

Se selectează *Adauga semnatura digitala certificate* din bara cu instrumente.

Procedura de semnare



Information Rights Management pentru Office 2007, 2010

IRM (Information Rights Management) permite persoanelor individuale și administratorilor să specifice permisiunile de acces la documente, registre de lucru și prezentări. Astfel, se împiedică imprimarea, redirecționarea sau copierea informațiilor sensibile de către persoane neautorizate. După ce au fost restricționate permisiunile pentru un fișier utilizând IRM, accesul și restricțiile de utilizare sunt impuse indiferent de locația informațiilor, deoarece permisiunile pentru accesul la un fișier sunt stocate chiar în document, registru de lucru sau fișierul de prezentare în sine.

IRM permite utilizatorilor să impună preferințele personale cu privire la transmiterea informațiilor personale sau confidențiale. De asemenea, IRM permite organizațiilor să impună politici cu privire la controlul și răspândirea informațiilor confidențiale sau cu drept de proprietate.

IRM ajută la realizarea următoarelor:

- Un destinatar care este autorizat pentru a primi conținut restricționat este împiedicat să redirecționeze, să copieze, să modifice, să imprime, să trimită prin fax sau să lipească conținutul pentru utilizare neautorizată
- Se împiedică utilizarea caracteristicii Print Screen în Microsoft Windows pentru copierea de conținut restricționat
- Se restricționează conținutul oriunde este trimis
- Este acceptat termenul de expirare al fișierelor, astfel încât conținutul documentelor, registrelor de lucru sau prezentărilor să nu mai poată fi vizualizat după o perioadă specificată de timp
- Se impun politicile de firmă care controlează utilizarea și răspândirea conținutul în cadrul firmei

IRM nu poate împiedica următoarele:

- Ștergerea, furtul sau capturarea și trimiterea conținutul printr-un program rău intenționat, cum ar fi un cal troian, înregistratorii de secvențe de tastare și anumite tipuri de spyware
- Pierderea sau deteriorarea conținutului din cauza acțiunilor virușilor de computer
- Restricționarea conținutul de la copierea de mână sau retastarea sa de pe afișajul ecranului destinatarului
- Efectuarea unei fotografii digitale de către destinatar a conținutului afișat pe ecran
- Copierea conținutului restricționat prin utilizarea programelor terțe de efectuare a capturilor de ecran

Crearea de conținut cu permisiune restricționată

IRM permite ca un autor individual să creeze un document, un registru de lucru sau o prezentare cu permisiune restricționată pentru anumite persoane care vor accesa conținutul. Autorii utilizează caseta de dialog Permisiiune (Fișier | Permisiiune | Nu se distribuie sau Permisiiune  de pe bara de instrumente Standard) pentru a acorda utilizatorilor acces de Citire și Modificare și pentru a stabili datele de expirare pentru conținut.

De exemplu, Dan poate să-i acorde lui Sanda permisiunea să citească un document dar nu să-l și editeze. Dan poate să-i acorde lui Ion permisiunea să modifice documentul și să îl salveze. Dan poate, de asemenea, decide să limiteze accesul la document atât pentru Sanda cât și pentru Ion la 5 zile. Autorii pot să elimine permisiunea restricționată dintr-un document, dintr-un registru de lucru sau dintr-o prezentare făcând clic pe Acces nerestricționat din submeniul Permisiiune sau făcând clic din nou pe Permisiiune  de pe bara de instrumente Standard.

Suplimentar, administratorii pot să creeze pentru firme politici de permisiune care sunt disponibile în Microsoft Office Word 2003, Microsoft Office Excel 2003 și Microsoft Office PowerPoint 2003, din submeniul Permisiiune și să definească cine are acces la informații și ce nivel de editare sau abilități Office au utilizatorii pentru un document, un registru de lucru sau o prezentare. De exemplu, un administratorul de firmă definește o politică numită „Confidențial

firmă”, care specifică documentele, registrele de lucru sau prezentările care utilizează această politică și care pot fi deschise numai de utilizatori din cadrul domeniului firmei. Se pot afișa simultan până la 20 de politici de particularizare (în ordine alfabetică) în submeniul Permisiiune astfel încât autorii individuali pot să le utilizeze pentru conținutul pe care îl crează.

În Word, Excel și PowerPoint, pot să restricționeze permisiunea pentru documente, registre de lucru și prezentări, pe o bază per-utilizator sau per-document

Utilizatorilor sau grupurilor li se poate acorda un set de permisiuni în conformitate cu nivelurile de acces care le-au fost atribuite de autori utilizând caseta de dialog Permisiiune:

Utilizatorii cu acces Citire pot să citească un document, un registru de lucru sau o prezentare, dar nu au permisiunea să editeze, să imprime sau să copieze.

Modificare Utilizatorii cu acces Modificare pot să citească, să editeze și să salveze modificările într-un document, într-un registru de lucru sau într-o prezentare, dar nu au permisiunea să imprime.

Control total Utilizatorii cu acces Control total au permisiuni de autor complete și pot să facă cu documentul, cu registrul de lucru sau cu prezentarea tot ceea ce poate să facă un autor: să stabilească datele de expirare pentru conținut, să împiedice imprimarea și să acorde permisiuni pentru utilizatori. Autorii au întotdeauna acces Control total.

Politici de permisiune

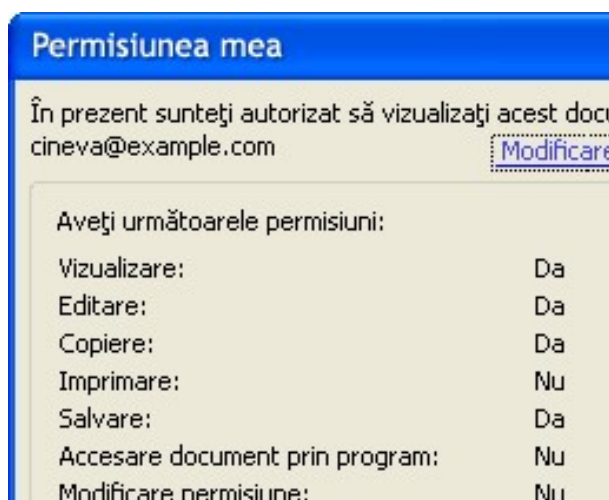
Permisiiunea pentru documente, registre de lucru și prezentări poate să fie restricționată prin utilizarea oricăror politici de permisiune particularizate care au fost create de administrator. Aceste permisiuni sunt disponibile în submeniul Permisiiune.

Vizualizarea de conținut cu permisiune restricționată

Utilizatorii care primesc sau deschid conținut cu permisiune restricționată trebuie numai să deschidă documentul, registrul de lucru sau prezentarea așa cum ar face-o cu conținut fără permisiune restricționată. Dacă utilizatorii nu au instalat pe computer Office 2003 sau ulterior, au posibilitatea să descarce un program care le permite să vizualizeze conținutul.

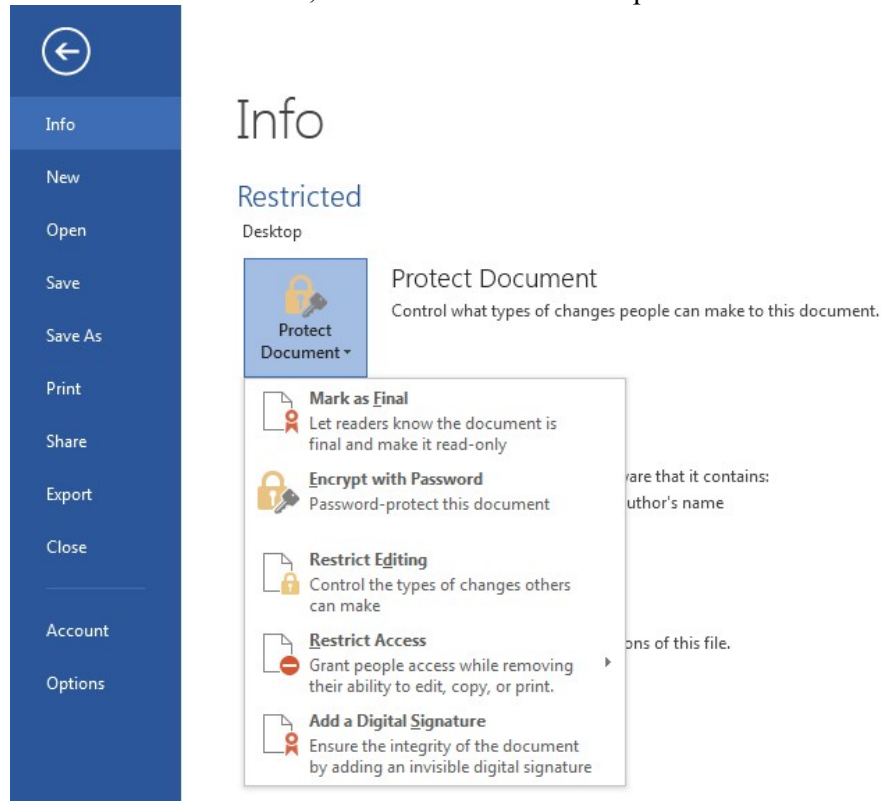
- Vizualizarea permisiunilor în Word, Excel sau PowerPoint

În Word, Excel sau PowerPoint, utilizatorii, în caseta de dialog Permisiiune proprie, pot să vizualizeze permisiunile care le-au fost acordate:

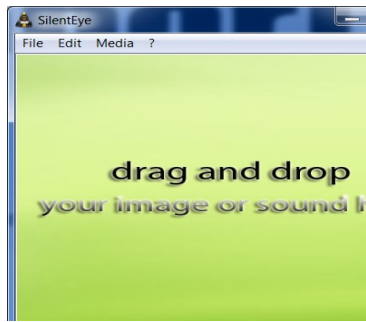


Sursa: <http://office.microsoft.com/ro-ro/word-help/despre-information-rights-management-HP006220859.aspx?CTT=1>

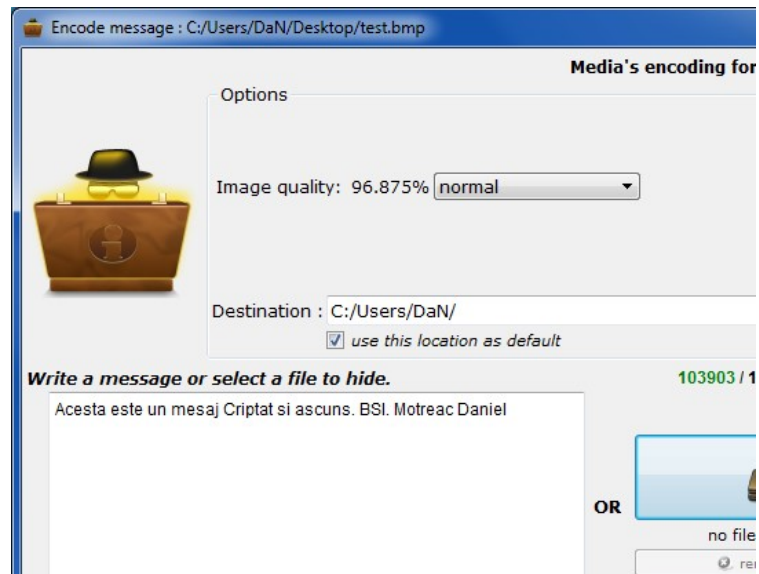
Cu opțiunile preinstalate în pachetul OFFICE am creat un fișier .doc ce are restricții la editare, sau în general restricții la vizualizare, fiind astfel securizat cu o parolă



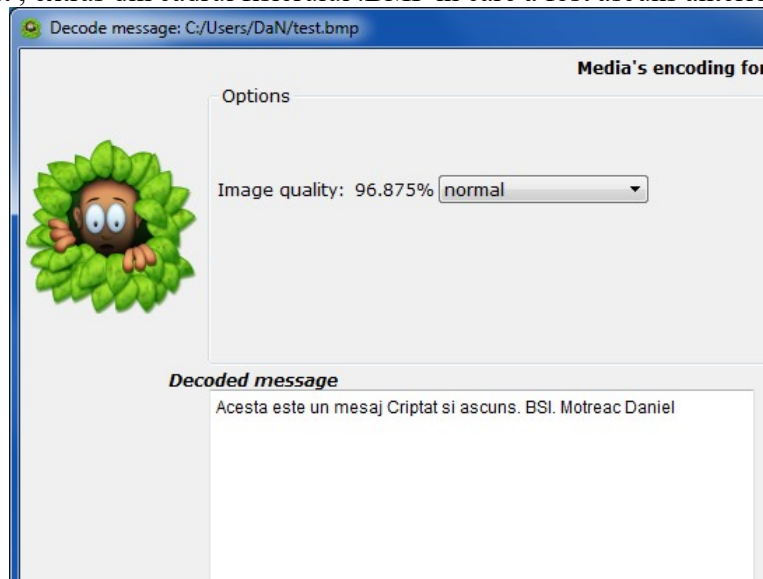
Steganografie provine din grecescul *steganos* (secret) și *graphein* (reprezentare grafică - scriere) și reprezintă operația prin care un mesaj text, imagine sau sunet poate fi încorporat într-un alt mesaj text, imagine sau sunet cu ajutorul unui algoritm implementat în așa fel încât procesul de ascundere să nu fie bănuț sau detectat nici de ochiul uman, dar nici de un program specializat în acest sens. De ex. softul gratuit *SilentEye* de pe site'ul oficial <http://www.silenteye.org> ce ne permite în spatele pozelor să ascundem un text sau chiar și un fișier



Ascunderea si criptarea mesajului in cadrul unui fisier .BMP



Mesajul decriptat , extras din cadrul fisierului .BMP in care a fost ascuns anterior un mesaj



Possibilitati:

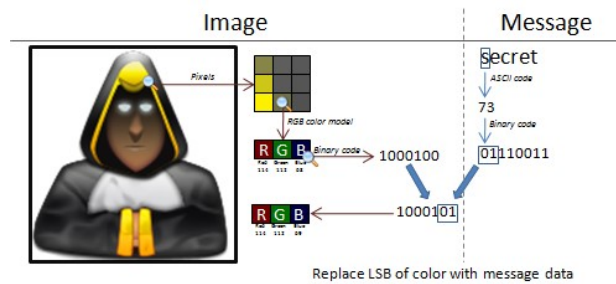
- Ascunde informatia in imagini si fisiere audio (LSB)
 - **JPEG**
 - **BMP**

- WAVE
- Cripteaza datele
 - AES128
 - **AES256**
- Capacitatea de ascundere a fileului, textului
- zlib compresare a mesajului
- Drag & Drop

Cum SilentEye ascunde mesajul in fisierul de tip .BMP?

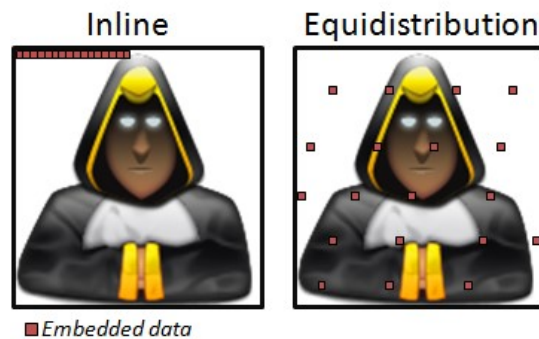
SEFormatBMP plug-in foloseste cel mai putin semnificativ bit pentru a pastra datele in reprezentarea RGB a pixelului. Bitmap nu este un format compresat deci nu exista riscul de pierdere a informatiei.

Diagrama:



Ce semnificatie are "distribution" pentru SilentEye ?

Distribution mode



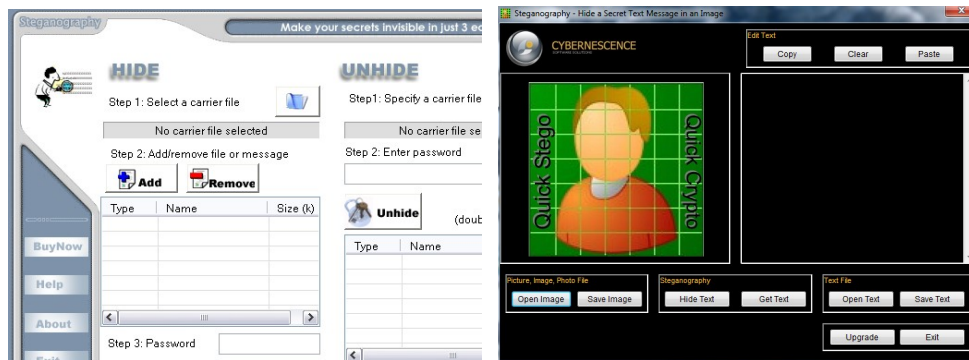
Ce semnificatie are "header" pentru SilentEye ?

„Header” reprezinta 32biti rezervati pentru ascunderea informatiei in cadrul imaginii, deasemenea putem specifica locul unde dorim ca informatia sa fie stocata, la nivel de bit in harta de pixeli

Header position



Softul Steganography:



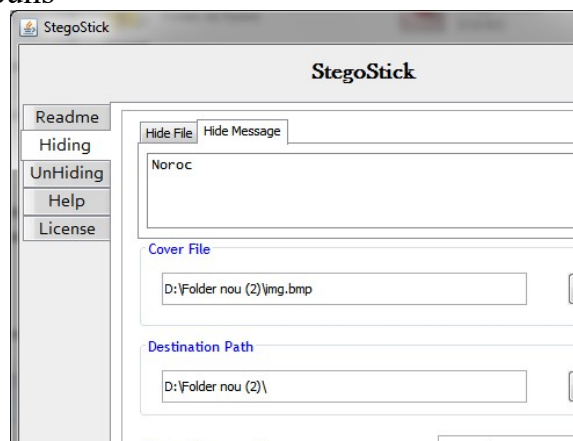
StegoStick

Stego Stick este un instrument steganographic care permite a ascunde orice fișier în orice fișier. Ea se bazează pe imagini, audio, video Steganography care ascunde orice fișier sau un mesaj într-o imagine (BMP, JPG, GIF), audio / video (MPG, WAV, etc) sau orice alt format de fișier (PDF, EXE, CHM, etc.)

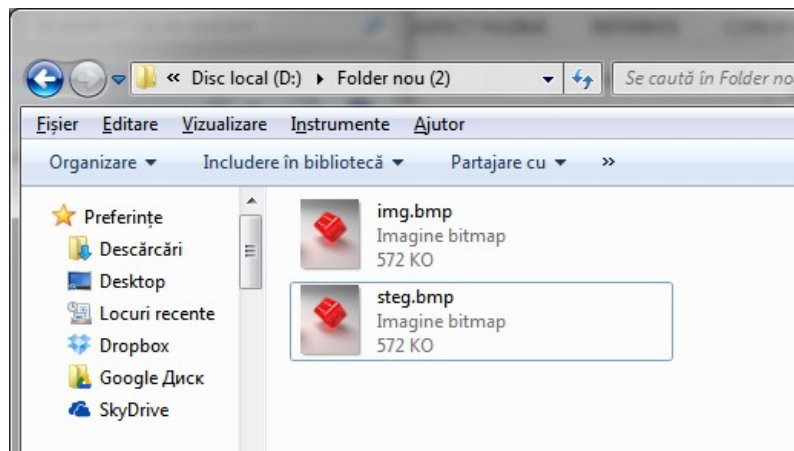
Exemplu de ascundere a unui mesaj: Alegem modul de criptare a mesajului



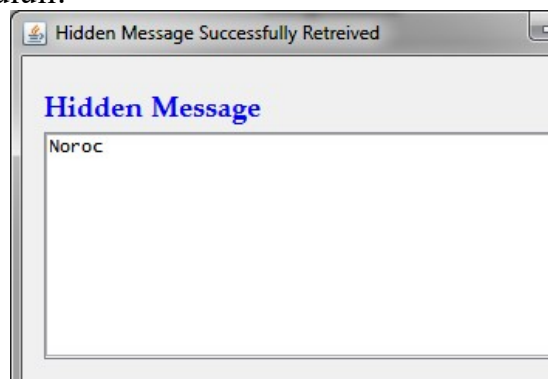
Tastam mesajul și alegem fișierul în care va fi ascuns și dosarul unde va fi creat fișierul cu mesajul ascuns



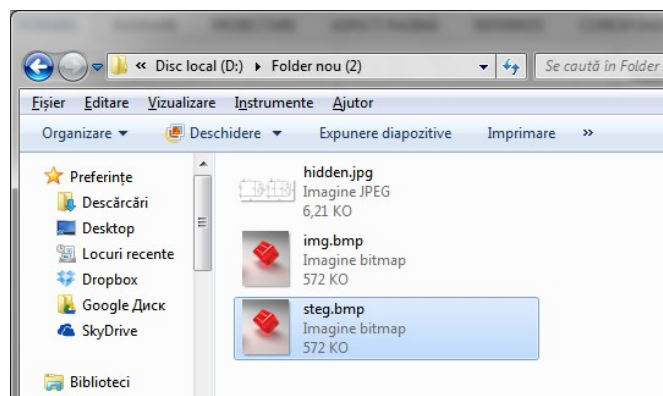
Observăm crearea unui fișier steg.bmp cu aceeași dimensiune



Descoperirea mesajului:



În cazul descoperirii unei imagini în directorul respectiv se va crea fișierul hidden.*.



Filigranarea(Watermarking)

Un filigran este un model distinct încapsulat într-un document, imagine, video sau audio de către cel care se află la originea datelor. Filigranul poate avea câteva scopuri, printre care:

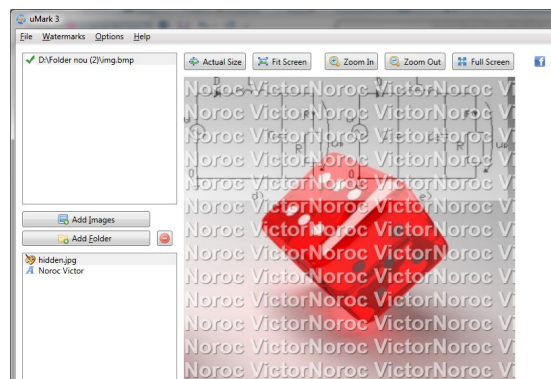
- indicarea proprietarilor datelor;
- ținerea evidenței copiilor datelor;
- verificarea integrității datelor.

Filigranele folosite în bancnote au scopul de a întări încrederea posesorilor că se află în fața banilor originali și nu a unora contrafăcuți, scopul fiind de securizare împotriva falsificării. Un filigran poate fi invizibil cu ochiul liber sau insesizabil de

ureche, dar există mijloace de detectare și extragere a lui pentru a se verifica autenticitatea datelor sau sursa lor. Datele filigranate sunt o funcție a unui identificator și/sau cheie care este unică pentru autor. Aceste valori sunt necesare pentru detectarea sau extragerea filigranului. Dacă mai multe copii ale datelor sursă au fost filigranate separat, fiecare ele va fi prelucrată cu o cheie proprie, deci fiecare copie are amprenta ei. Prin ținerea evidenței fiecărei chei folosite pentru fiecare beneficiar este ușor de urmărit cine a încălcat drepturile de autor. Filigranele pot fi de două tipuri: fragile sau solide. Filigranele fragile sunt mai ușor de schimbat, dar sunt folosite doar pentru a vedea dacă datele au fost schimbate, în timp ce filigranele solide rezistă tuturor manipulărilor și manevrelor la care sunt supuse. Filigranarea este similară cu steganografia și se bazează pe tehnici de proiectare apropiate. În spațiul cibernetic, filigranele sunt folosite pentru stabilirea încălcării drepturilor de autor.

uMark

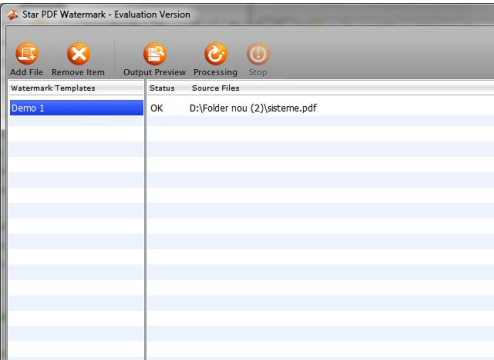
uMark Lite este un software gratuit filigran foto pentru adăugarea de filigrane vizibile la imagini digitale. uMark Lite poate adăuga text și filigrane imagine pe mai multe fotografii la o dată. Puteți seta textul filigran, stabilit stilul de font, culoare, culoare umbra și transparența pentru filigrane de text. Puteți plasa filigrane la data de 9 locații predefinite pe imagine.



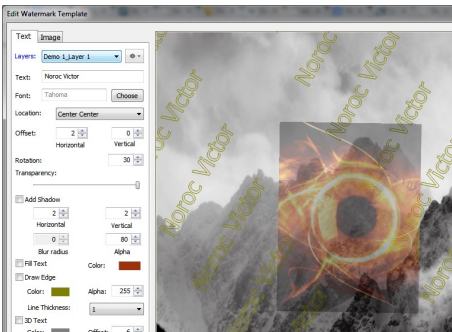
Star PDF Watermark

Star PDF Watermark este un instrument de filigranare PDF pentru Windows, puteți adăuga text sau imagini pe fiecare pagină a unui fișier Acrobat PDF, cum ar fi semnăturile add, numele companiei sau logo-ul companiei pentru a vă proteja drepturile de autor fișier PDF. Cu PDF Watermarking versiune de software gratuit, puteți adăuga text filigran pentru documentul PDF, cu versiunea achiziționată, puteți adăuga și imagini pe fișierul PDF. Cu interfața Smart Star PDF programului filigranului, avem multe posibilități de redactare a filigranului, cum ar fi trageți și plasați fișiere PDF pentru software-ul pentru a adăuga fișiere sursă, și faceți dublu clic pe template-uri filigran sau fișier sursă pentru a edita șablonul sau previzualizare rezultat filigranare PDF. De asemenea putem construi brand-ul companiei, prin care marcam logo-ul companiei pe toate fișierele PDF, pentru a evita copierea și a adăuga drepturi de autor.

Fereastra de lucru:



Editare filigran:



Documentul PDF filigranat:

