Semnatura Digitala

profesor indrumator
Stefan Stancescu

student
Bogdan Cismariu

1. Introducere

1.1. Ce este semnatura digitala?

Iata o sintagma care este cunoscuta probabil celor mai multi dintre voi: “Factura a fost stampilata? S-a semnat documentul de catre partenerul de afaceri?” Practic, semnarea si stampilarea reprezinta modurile prin care documentele tale capata recunoastere juridica.

In fiecare zi, oamenii semneaza scrisorile si alte documente, demonstrand ca sunt de acord cu continuturile lor. Totusi, semnaturile manuale sunt vulnerabile pentru ca e posibil sa fie reproduse si ca documentele sa fie modificate dupa ce au fost semnate. Semnaturile digitale si cele manuale sunt ambele bazate pe faptul ca e foarte greu sa gasesti doua persoane cu aceeasi semnatura.

Derularea afacerilor prin intermediul retelei Internet si schimbul de date pe suport electronic necesita existenta aceluiasi sentiment de incredere si securitate al partenerilor care incheie o tranzactie la fel ca in cazul comertului "clasic". Acest sentiment poate fi dat acum de folosirea semnaturii digitale. Semnatura electronica (sau digitala) este pentru documentele electronice ceea ce este o semnatura olografa pentru documentele tiparite.

Semnatura electronica reprezinta informatii in format electronic si care sunt atasate sau logic asociate unor documente, in forma de asemenea electronica, si serveste ca metoda de identificare a semnataruiui si este inmagazinata pe suport magnetic securizat.

Cu alte cuvinte, semnaturile digitale permit autentificarea mesajelor digitale, asigurand destinatarul de identitatea expeditorului si de integritatea mesajului, furnizand astfel un grad mult mai mare de securizare decat semnatura olografa.

Destinatarul mesajului semnat digital poate verifica atat faptul ca mesajul original apartine persoanei a carei semnatura a fost atasata cat si faptul ca mesajul n-a fost alterat, intentionat sau accidental, de cand a fost semnat. Mai mult, semnatura digitala nu poate fi negata; semnatarul documentului nu se poate disculpa mai tarziu invocand faptul ca a fost falsificata (Documentele "parafate“ cu o semnatura electronica au valabilitate juridica in instanta, iar emitentul acesteia este identificat fara putinta de tagada).

2. Prezentare generala

2.1. Cui ii este dedicata semnatura digitala?

Semnatarul este definit ca fiind acea persoana care detine un dispozitiv de creare a semnaturii electronice si care actioneaza fie in nume propriu (persoana fizica) fie in numele unui tert (persoana juridica, de exemplu).

Semnatura electronica se aplica unui document in format electronic, redactat sau obtinut prin intermediul programelor informatice, de exemplu:

- Documente MS Word (contracte, documente, notificari, etc.) ;
- Spread-sheet Excel (rapoarte financiare, state de plata a salariilor, etc.);
- Documente Adobe Acrobat;
- Fotografii digitale (constatari, mostre, comanda de produse, etc.);
- Programe expert de gestiune a documentelor;
- Documente rezultate din prelucrarea datelor contabile si fiscale.

2.2. Asocierea semnaturilor digitale si criptarea

Semnatura electronica este creata prin mijloace controlate exclusiv de semnatar. Este legata de documentul in forma electronica la care se raporteaza in asa fel incat orice modificare a documentului, ulterioara semnarii, sa duca automat la invalidarea semnaturii.

Schemele semnaturilor digitale tip cheie publica se bazeaza pe criptarea in cheie publica. Astfel, fiecare utilizator are cate o pereche de chei: una publica si una privata. Cheia publica este distribuita liber, iar cheia privata este tinuta secreta de catre utilizatorul ei. Cheia privata este un dispozitiv specializat (de obicei un sir de caractere) cu caracter de unicitate. Cheia publica este tot un cod digital, dar este perechea cheii private si este necesara verificarii semnaturii electronice. Alta cerinta este aceea ca ar trebui sa fie practic imposibil sa afli cheia private din cea publica.

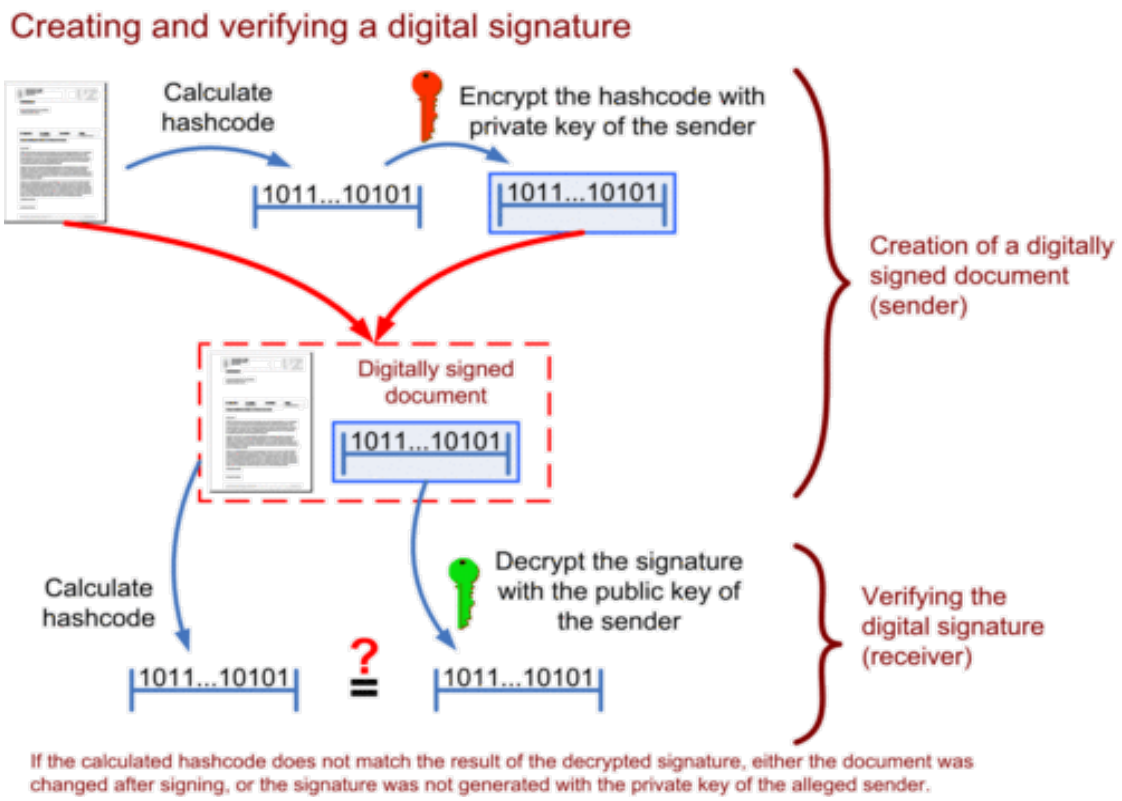
In general, schemele semnaturilor digitale includ 3 algoritmi:
- un algoritm de generare de cheie;
- un algoritm de semnare;
- un algoritm de verificare;

Atunci cand va dori sa transmita un document semnat digital de catre el, semnatarul va proceda astfel:

Semnatarul va genera un hash al documentului care va fi apoi protejat prin criptare, folosind cheia sa privata. Astfel s-a creat documentul semnat digital care apoi va fi transmis catre destinatar. Daca pe parcursul transmisiunii documentului acesta este cumva interceptat de catre un tert, chiar daca acesta nu-l va putea citi, el ar putea in mod malitios alterarea documentului. Modificarea documentului nu va fi posibila insa fara sa se realizeze si modificarea hash-ului.

La destinatie, se va decripta semnatura folosind cheia publica a semnatarului, si de asemenea se va recalcula hash-ul. Rezultatele celor doua operatiuni vor trebui sa fie identice, altfel inseamna ca ori documentul a fost alterat pe parcurs, ori nu a fost semnat cu cheia private a semnatarului presupus. Daca insa acestea coincid, atunci destinatarul poate confirma ca documentul este cel criptat cu cheia privata a expeditorului (si implicit se presupune ca acesta este acea unica persoana care putea folosi acea cheie), si de asemenea ca mesajul nu a fost alterat din momentul in care a fost semnat.

Nici un destinatar nu poate fi absolut sigur ca presupusul expeditor este intradevar cel care a semnat, deoarece este posibil ca sistemul de criptare sa fi putut fi spart, sa se fi putut copia cheia, sau sa se fi evitat toata schema prin inginerie sociala.



Algoritmii si protocoalele pt semnatura digitala nu pot oferi o certitudine cu privire la data si ora la care documentul in cauza a fost semnat. Semnatarul poate sau nu sa includa si data o data cu semnatura, sau este posibil ca documentul insusi sa aiba o data mentionata pe el, dar cineva care l-ar putea citi mai tarziu nu ar putea fi sigur daca semnatarul nu a decalat cumva data semnaturii. Aceste probleme pot fi inlaturate prin folosirea unui “time stamp” pe langa semnatura digitala.

Masuri de securitate aditionale

Toate sistemele de criptare in cheie private/publica depind in totalitate de tinerea sub secret a cheii private. O cheie privata poate fi stocata in computerul utilizatorului, si protejata de exemplu de o parola locala, insa acest lucru are doua dezavantaje: utilizatorul poate semna doar documente pe acel calculator particular si de asemenea, securitatea cheii private depinde complet de securitatea computerului, fiind de notorietate faptul ca nu putem baza pe majoritatea PC-urilor si sistemelor de operare din punctual acesta de vedere.

O alternativa mult mai sigura este sa stocam cheia privata pe un smart card. Multe smart card-uri au fost create in mod special urmarindu-se sa fie cate mai rezistente. In implementarea tipica, hash-ul calculat din document este

trimis catre smart card, al carui CPU cripteaza hash-ul utilizand cheia private stocata si il returneaza. Tipic, un utilizator trebuie sa-si activeze smart card-ul prin introducerea numarului de PIN (ceea ce obliga la o autentificare dubla). Aceasta solutie reduce schema de securitate la PIN-ul sistemului, dar este fara indoiala o alternativa mai sigura decat majoritatea PC-urilor.

2.3. Cum se foloseste o semnatura digitala?

Pasul I:

Persoana interesata sa semneze electronic documente trebuie sa se prezinte cu cartea de identitate sau buletinul la un furnizor de servicii de certificare in domeniul semnaturii electronice. Furnizorul de servicii de certificare joaca rolul unui martor virtual care confirma identitatea unei persoane.

Pasul II:

In urma platii unei sume stabilite de furnizor veti intra in posesia un dispozitiv securizat, necesar pentru a va putea semna electronic, ca, spre exemplu, eToken sau smart card. Pentru a accesa aceste dispozitive tastati un cod PIN, pe care puteti sa il schimbati si care e cunoscut doar de dvs.

Pasul III:

Conectati dispozitivul securizat fie la calculatorul furnizorului de servicii de certificare, fie la calculatorul dvs. sau la orice alt calculator. Accesati site-ul furnizorului si completati formularul pentru obtinerea certificatului digital. Veti primi prin e-mail un cod de identificare care va permite eliberarea acestuia.

Pasul IV:

De asemenea, veti primi un certificat digital care atesta dreptul dvs de a va semna electronic si care contine: cheia dumneavoastra publica, datele dvs personale. Certificatul digital emis este semnat electronic de catre furnizorul de servicii de certificare, cu cheia lui privata. Certificatul digital leaga persoana de cheia publica.

Certificatul dvs. digital va fi disponibil pentru accesare pe site-ul furnizorului pentru care ati optat. Durata valabilitatii unui certificat este de maximum 1 an de la data comunicarii catre client.

3. Aplicatii software

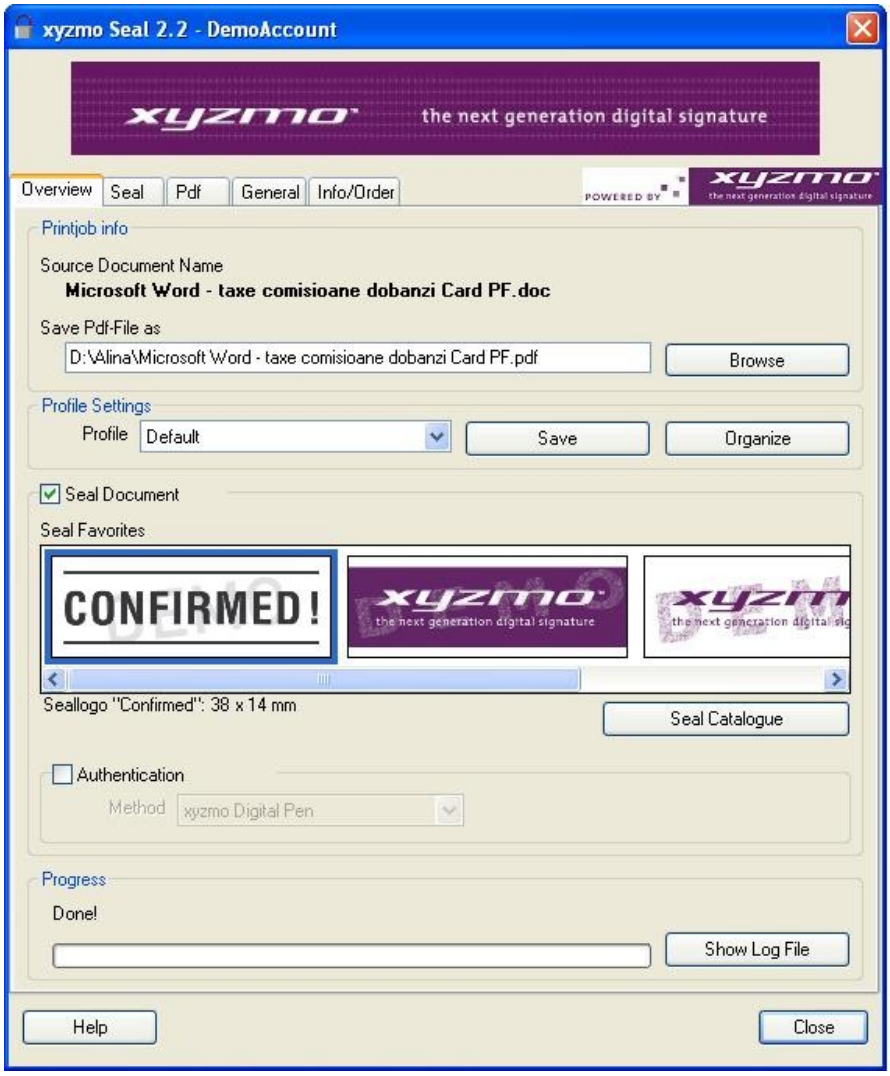
3.1. XYZMO

- *xyzmo® Seal Client- xyzmo® Seal for Windows*

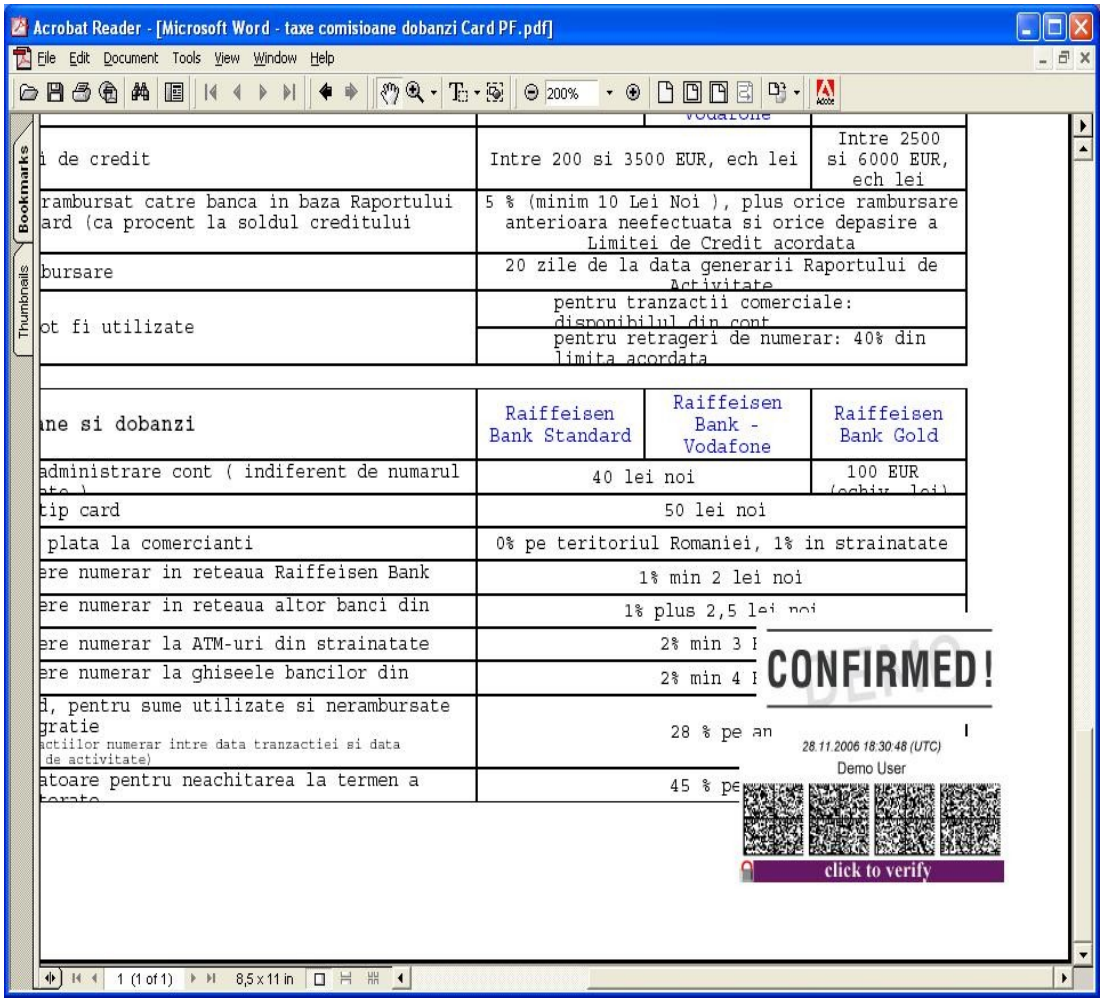
xyzmo® Seal Client reprezinta punctul de intrare in lumea xyzmo® a semnaturilor digitale. xyzmo® Seal for Windows permite protejarea proprietatii intelectuale si urmarirea drumului comunicatiilor de afaceri. Produsul are un design simplu si se foloseste ca si o imprimanta pentru Windows.

Pasii ce trebuie urmati pentru semnarea digitala a unui document folosind xyzmo, sunt:

- Deschiderea documentului pe care dorim sa il semnam;
- Urmand comanda standard “Print”, se va alege in sectiunea de imprimante (printer) “xyzmo® Seal”;
- Selectarea unui logo din fereastra urmatoare;

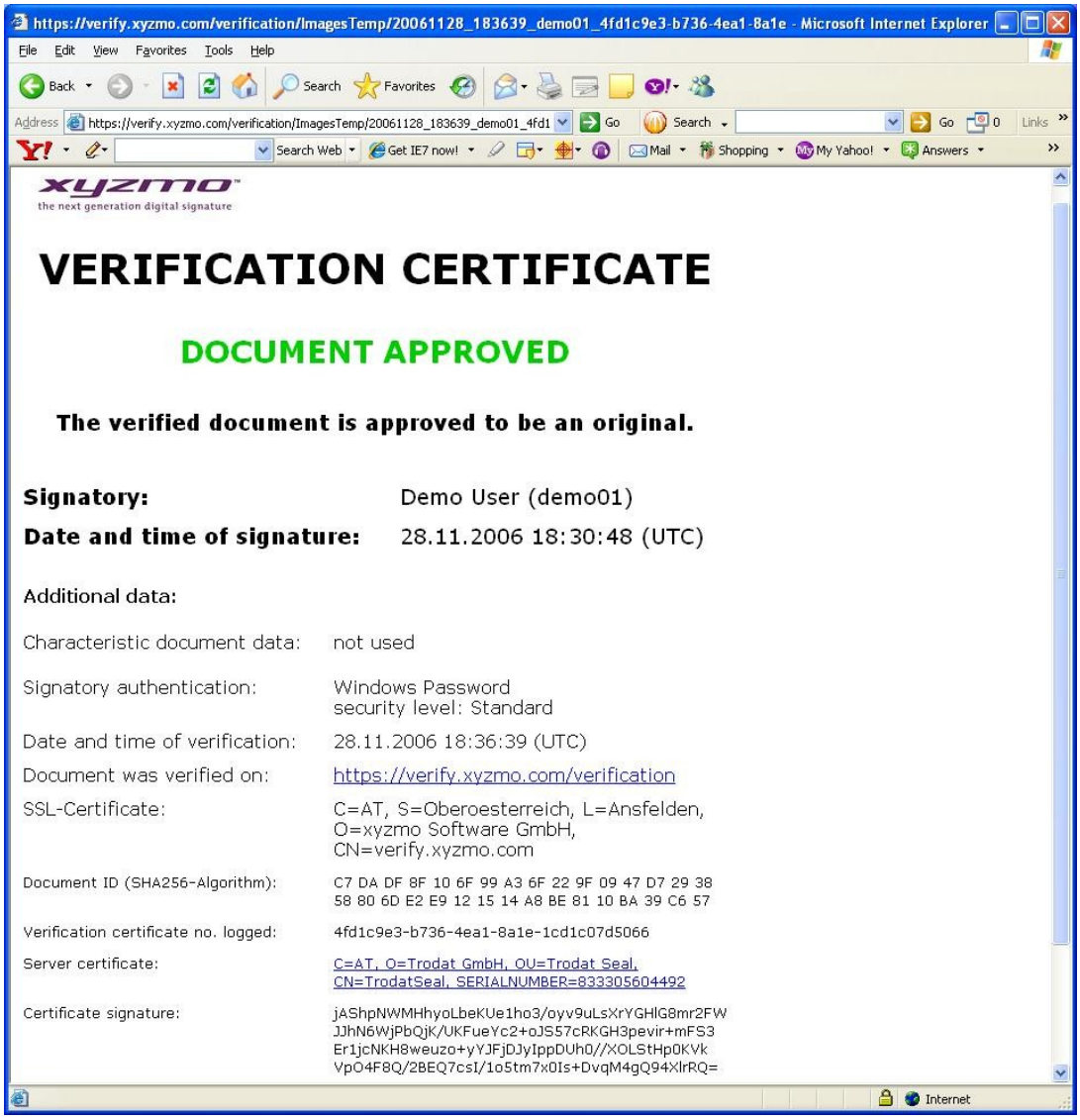


- Urmatorul click transforma documentul intr-un document PDF semnat digital- acest document reprezinta acum originalul;



Documentul rezultat poate fi acum arhivat sau trimis. La primirea unui document astfel semnat, destinatarul poate determina identitatea autorului si se poate asigura de integritatea acestuia. Tot ce este necesar a fi facut este un click pe linkul de test din semnatura (“click to verify”), si, in cateva secumde se va emite un certificat ce contine informatia referitoare la autenticitatea si identitatea semnatarului.

xyzmo® Seal for Windows este potrivit pentru semnarea digitala individuala sau multipla, cat si pentru verificarea individuala si multipla a documentelor semnate. Semnatura digitala poate fi evidentiata in toate formatele, in format digital ca si semnatura electronica, pe hartie ca o asa-numita “digital to paper hard copy”, si, natural ca si microfilm. In plus, o semnatura manuala digitala poate fi integrata ca si un nivel in plus de securitate. Semnarea are loc in mod conventional.



xyzmo
the next generation digital signature

VERIFICATION CERTIFICATE

DOCUMENT APPROVED

The verified document is approved to be an original.

Signatory:	Demo User (demo01)
Date and time of signature:	28.11.2006 18:30:48 (UTC)

Additional data:

Characteristic document data:	not used
Signatory authentication:	Windows Password security level: Standard
Date and time of verification:	28.11.2006 18:36:39 (UTC)
Document was verified on:	https://verify.xyzmo.com/verification
SSL-Certificate:	C=AT, S=Oberoesterreich, L=Ansfelden, O=xyzmo Software GmbH, CN=verify.xyzmo.com
Document ID (SHA256-Algorithm):	C7 DA DF 8F 10 6F 99 A3 6F 22 9F 09 47 D7 29 38 58 80 6D E2 E9 12 15 14 A8 BE 81 10 BA 39 C6 57
Verification certificate no. logged:	4fd1c9e3-b736-4ea1-8a1e-1cd1c07d5066
Server certificate:	C=AT, O=Trodat GmbH, OU=Trodat Seal, CN=TrodatSeal, SERIALNUMBER=833305604492
Certificate signature:	jAShpNWMHhyoLbeKUe1ho3/oyv9uLsXrYGHlG8mr2FW JJhN6WjPbQjK/UKFueYc2+oJS57cRKGH3pevir+mFS3 Er1jcNKH8weuzo+yYJFjDJyIppDUh0//XOLStHp0KVk VpO4F8Q/2BEQ7csI/1o5tm7x0Is+DvqM4gQ94XlrRQ=

➢ *xyzmo® DIG2P Hardcopy*

Pentru situatiile in care este indispensabila si o copie de hartie a unui document semnat digital, xyzmo® a dezvoltat si produsul xyzmo® DIG2P Hardcopy. xyzmo® DIG2P Hardcopy permite printarea pe hartia pe care este printat documentul a unui cod de bare care contine toata informatia necesara. Citirea poate fi facuta in orice moment prin simpla scanare a codului de bare atatsat documentului, ceea ce permite convertirea in secventa de date ce reprezenta semnatura digitala.

- *xyzmo® SIGNificant*

Acest produs este deosebit de util in a evita printarea documentelor doar pentru a putea fi semnate. Majoritatea companiilor deja si-au automatizat procesul de desfasurare a activitatii lor, lasand astfel ca singur element ce necesita folosirea hartiei, stadiul de aprobare a documentelor. Procesul electronic este oprit numai pentru a obtine o semnatura, ceea ce necesita ca apoi acest document sa fie scanat pentru a fi adaugat in arhiva electronica.

Folosing *SIGNificant,* semnatura de mana devine o parte inerenta a fluxului de documente. *SIGNificant* este o aplicatie web-based, care permite semnarea unui document din orice locatie fizica, fara sa fie nevoie tiparirea acestuia. Semnarea unui document electronic cu *SIGNificant*, este la fel de simpla ca si o semnatura facuta pe hartie cu pixul. Pus si simplu “Click to sign” si foloseste un sitlou digital pe un TabletPC, display sau o desktop digital tablet. Semantura va aparea imediat pe document.

SIGNificant ataseaza documentului semnatura electronica, informatia referitoare la utilizator si parametrii biometrici ai semnaturii. Semnatura grafica poate fi vazuta atat pe ecran, cat si pe copia tiparita, si devine parte din intregul document.

SIGNificant este o aplicatie web-based, astfel, utilizatorii au nevoie doar de acces la internet. Nu este nevoie de instalare sau download pentru a putea functiona. Cei care calatoresc pot semna din orice locatie, evitand astefel amanarile aprobarilor.

- *xyzmo® Server* si *xyzmo® Appliance*

xyzmo® Server formeaza inima platformei xyzmo®, cuprinzand: interfete de comunicare, servicii de autentificare, livrare in siguranta a documentelor, serviciu de time stamping, formate de semnaturi standard, dar si de noua generatie, servicii de verificare a documentelor, tehonlogie DIG2P, formulare electronice.

xyzmo® Appliance este o solutie hardware out-of-the-box pentru server pentru orice tip de semnare in masa a documentelor. Folosind conectorii xyzmo® (*xyzmo® Connectors*) adecvati, sistemul utilizatorului poate comunica cu serverul si poate transfera documente pentru a fi semnate. Functiile *xyzmo® Appliance* sunt:

- semnarea documentelor;
- selectia pentru formatul semnaturii (*xyzmo® Seal*, Adobe PDF, CMS/PKCS#7, XMLDSIG) ;
- tipuri de semnaturi: semnatura simpla, semnatura avansata, semnatura calificata;
- procesare pe baza de reguli (de exemplu: o semnatura avansata este aplicata pentru toate documentele ce au la expeditor invoice@xyzmo.com, folosind procedura *xyzmo® Seal Signature*; apoi acestea sunt trimise prin e-mail si stocate pe file server)
- poate emite o cantitate de documente pentru semnat;
- concept Plug-in pentru formarea de legaturi cu oricati conectori xyzmo® (*xyzmo® Connectors*).

3.2. SILANIS

➢ *ApproveIt® Desktop*

Acest produs al companiei Silanis, permite realizarea procesului de aprobari in afaceri 100% in mod electronic.

Proiectat astfel incat sa functionze “out-of-the-box”, acest software pentru abrobari manageriale electronice poate fi usor integrat in procesele existente si instrumentele IT standard din afacere, eliminand nevoia de a printa documentele pentru semnare.

Organizatiile isi vor reduce astfel costurile imediat, vor micsora ciclurile de aprobare si vor mari viteza de reactie, fiind sigure utilizarea usoara si de de siguranta oferite de *ApproveIt Desktop,* dar si de valoarea sa in justitie. Mai mult, alegand Silanis ca si furnizorul lor de semnatura electronica, organizatiile au garantia unei tehnologii flexibile si scalabile, care se va dezvolta o data cu nevoile intreprinderii.

Asigurarea unei solutii sigure, prietenoase si cu valoare legala:

Mutarea procesului de aprobare din afaceri in lumea electronica necesita asigurarea un echilibru intre tehnologie, proces si aplicatie. Pentru a asigura o implementare de success, *ApproveIt Desktop*, combina securitatea tehonlogiei semnaturii digitale cu un proces de semnare electronica cu valoare legala. Solutia face un pas mai departe incorporand optiuni avansate pentru aprobarea electronica pentru a asigura usurinta in folosire, adoptare pe scara larga de catre consumatori si support pentru aplicatiile business de zi cu zi.

Securitatea:

O data ce un document sau formular este semnat in mod automat folosind *ApproveIt Desktop*, integritatea datelor este securizata si o ruta de audit este atasata in mod permanent la document. Semnatura electronica rezultata este invalidata in mod clar, daca sunt facute cumva modificari neautorizate. Solutia poate fi de asemenea combinata cu o varietate de solutii pentru autentificarea utilizatorului, incluzand PKI sau smart cards.

Valoare legala:

ApproveIt Desktop satisface toate cerintele legale cu privire la semnatura electronica. Solutia capteaza intentia unei persoane de a semna un document si ataseaza in mod permanent consimtamantul acesteia, in forma unei semnaturi electronice in document. Aceasta informatie, care este permanent legata de documentul final creeaza un process de aprobare ce poate fi verificat oricand. Utilizatorii pot salva o copie electronica, sau pot printa copii “hard” pentru registrele lor.

Utilizarea:

ApproveIt Desktop necesita eforturi minime pentru invatare. Iconitele pentru semnare apar in toolbar-ul aplicatiei, permitand utilizatorilor sa isi adauge semnatura electronica in mod intuititv, cu un singur click. O imagine a semnaturii olografe a fiecarei persoane este de asemenea securizata in interiorul documentului. Acest lucru reproduce felul in care arata un document semnat de mana atat pe ecran, cat si la tiparire. Automatizarea avansata cuprinde de asemenea procese complexe de semnare care implica suport pentru mai multi useri intr-o aplicatie electronica.

Suportul oferit proceselor business complexe ce implica mai multi utilizatori:

Un proces de aprobare in afaceri nu este intotdeauna la fel de simplu cum ar parea. Procesul devine din ce in ce mai complex cu cat exista mai multe persoane care semneaza, care isi asuma responsabilitatea pentru diferite parti ale documentului sau formularului si care apoi fac modificari autorizate asupra continutului semnat.

Un process de aprobare in lumea electronica trebuie astfel sa ofere cu mult mai mult decat o semnatura electronica si capacitate de autenticitate a datelor. De asemenea trebuie sa administreze si sa automatizeze semnaturile ca si parte dintr-un proces intreg atutentificat de aprobare in afaceri.

Nici o semnatura digitala sau electronica nu s-ar putea apropia de capacitatea de a suporta asemenea procese fara niste programare in plus. Editarea sau adaugarea de informatie la un document semnat, chiar daca este doar adaugarea datei sau a numelui sau titlului unei persoane, poate invalida documentul, caci tehnologiile sunt programate sa detecteze toate modificarile ce sunt aduse documentului.

Tehnologia semnaturii inteligente:

ApproveIt Desktop este construit pe baza tehonologiei semnaturii digitale si electronice, si aduce in plus facilitati de automatizare pentru a reda nuantele proceselor de aprobare din lumea real ape cat de fidel posibil, mentinand in acelasi timp autenticitatea documentului de-a lungul procesului.

Solutia recunoaste continutul si autentifica in mod inteligent documentele a semnate de catre fiecare persoana si pentru care sunt responsabile. Acest lucru permite adaugarea de semnaturi multiple la document, efectuarea de adaugari si modificari, si acelasi tip de flexibilitate in semnare pe care o ofera hartia.

Aceste caracteristici tip plug-and-play sunt disponibile “out of the box” cu *ApproveIt Desktop*, si pot fi adaugate la orice document sau process indiferent de complexitatea sau de numarul de semnaturi necesare.

ApproveIt Desktop permite semnarea unui document oricand, oriunde si de catre oricine. Indiferent daca procesele de aprobare ale unei organizatii au loc intre cei patru pereti ai acesteia sau in fata clientilor, *ApproveIt Desktop* le poate rezolva.

Procesul de semnare poate avea loc la calculatorul propriu, pe un laptop sau la o statie de semnare special desemnata pentru aplicatii interfata cu clientul. O semnatura electronica este aplicata toturor documentelor folosind un fisier electronic ce contine semnatura olografa a semnatarului, sau folosind un “pad” de semnare care capteaza semnatura “live” a persoanei.

ApproveIt Desktop poate fi combinata cu alte produse de autentificare pentru terti, incluzand certificate digitale PKI, CAC, sau smart-card-uri.

- *ApproveIt Web Server* - Semnarea “Sever Based”

Silanis reprezinta o solutie si in cazul in care organizatiile doresc sa ofere clentilor, partenerilor sau furnizorilor posibilitatea de a semna documentele prin intermediul internetului.

Impartind acelasi motor de semnare ca si *ApproveIt Desktop, ApproveIt Web Server* permite prezentarea, revizuirea si semnarea documentelor obisnuite prin intermediul unui browser web fara sa fie nevoie ca utilizatorii sa downloadeze software additional.

- *ApproveIt XHMTL Server*

Folosid de asemenea acelasi motor pentru semnare, *ApproveIt XHMTL Server*, permite completarea electronica si aprobarea formularelor XHTML prin intermediul unui server de retea.

3.3. ArticSoft – FileAssurity Open PGP

ArcticSoft are un singur obiectiv: sa ofere costuri scazute, calitate inalta, software pentru criptare si semnatura digitala usor de utilizat. Compania are o experienta de peste 34 de ani in domeniul securitatii calculatoarelor, si 19 ani experienta in securizarea informatiei pe calculatoare personale. Steve Mathews, CEO, este unul dintre autorii ISO/IEC 17799 si este bine cunoscut in indusria securitatii.

Produsul codifica si semneaza digital fisiere, foldere, documente, mesaje instant si e-mail-uri. De asemenea, le sterge in mod securizat.

- **Caracteristici:**

- Protejarea fisierelor

Spre deosebire de produse care folosesc mecanisme slabe bazate pe parola care pot fi usor sparte cu programe care se gasesc pe internet, FileAssurity foloseste tehnologia puternica PKI. Fisierele sunt criptate folosind algoritmi standard. Orice tip de fisier poate fi criptat si/sau semnat digital, indiferent de extensia sa. A codifica fisiere inseamna ca numai destinatarul le poate vedea continutul. A semna digital fisierele asigura destinatarul ca acele fisiere provin de la un anumit emitator. Fisierele pot fi codificate pentru anumite

persoane sau pentru un grup.

- Mesaje instant si e-mail-uri securizate

Trimite e-mailuri si mesaje instant in mod sigur indiferent de clientul de e-mail utilizat de catre emitator si destinatar. Pentru a trimite mesaj text securizat poti crea sau copia text “Editorul de texte securizat” si FileAssurity il va securiza automat.

- Stergerea securizata a fisierelor

- Arhive securizate

Se pot codifica mai multe fisiere si foldere intr-o arhiva care foloseste standardul zip de compresie. Aceasta este o alternativa sigura la utilizarea fisierelor zip si ofera o gestionare facila a fisierelor si folderelor.

FileAssurity costa o patrime din pretul lui PGP (Pretty Good Protection) , produs al firmei PGP si asigura o protectie mai buna, fiind in acelasi timp mai usor de utilizat. Se pot genera propriile chei ca si in PGP sau pot fi importate de la majoritatea Autoritailor de certificare. Produsul ofera posibilitatea generarii, importarii, exportarii cheilor X.509 si PGP si de asemenea decriptare/criptarea , semnarea/verificarea fisierelor compatibile OpenPGP.

FileAssurity foloseste algoritmul aprobat AES la puterea sa maxima(256 biti) si pentru comunicatia cu useri PGP v5.x si v6.x foloseste TDES(192 biti).

➢ FileAssurity OpenPGP- Screenshots

Diagrama1: Optiunile meniului Windows Explorer

Aici se pot selecta fisiere pentru criptare si/sau pentru semnare digitala, se pot sterge fisiere securizate, se poate crea text, gestiona cheile si schimba setarile implicite.

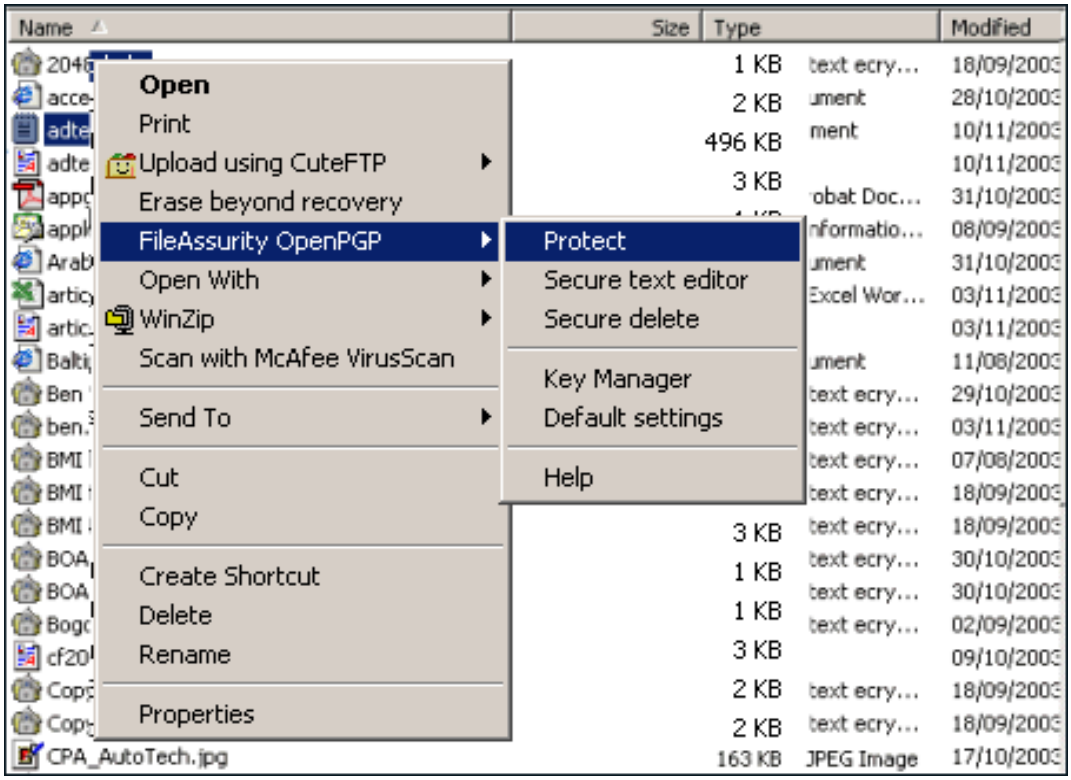


Diagrama 2: Bara de protectie

Aici se pot selecta cheile de criptare si semnare si specifica daca se doreste arhivarea securizata a fisierelor, trimiterea prin e-mail sau crearea de text securizat.

Diagrama 3: Editorul de text securizat

Se poate crea text securizat pentru inserare in orice aplicatie. FAOPGP copiaza automat acest text in clipboard sau o insereaza direct in aplicatia de posta electronica.

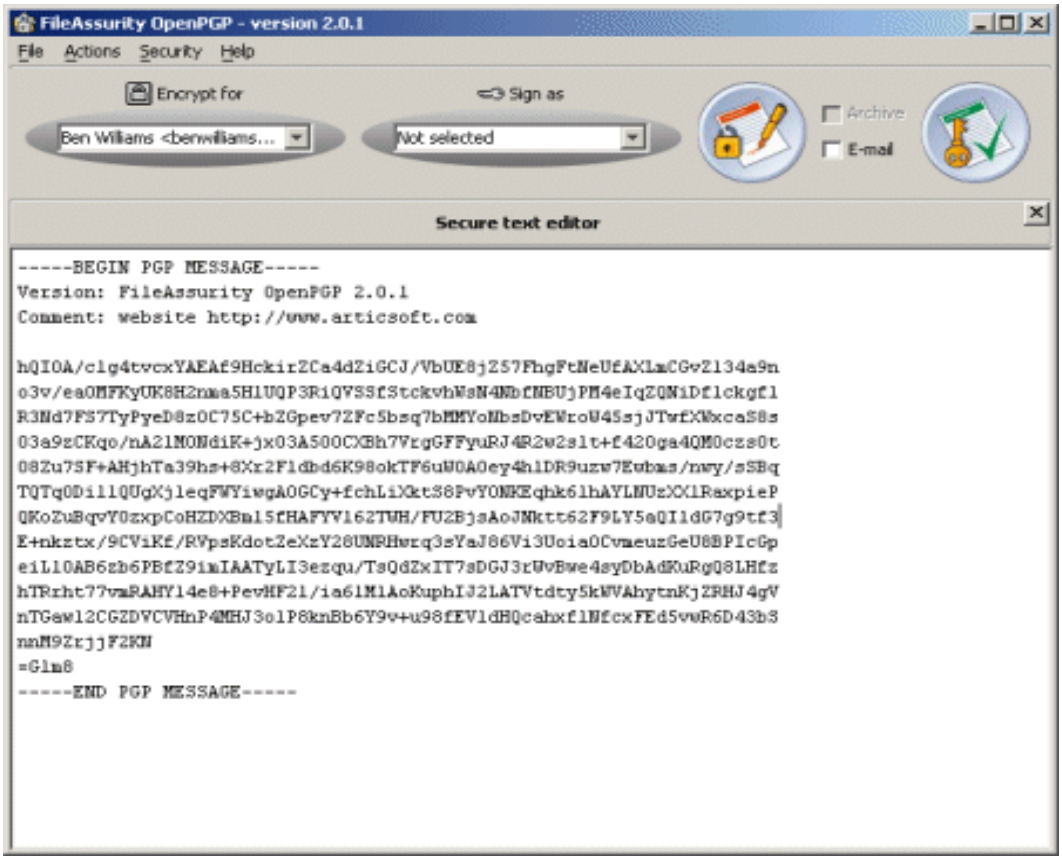


Diagrama 4: E-mail securizat

FAOPGP deschide automat aplicatia de e-mail cu textul securizat introdus in partea de mesaj, cu fisierele atasate si adresele de e-mail introduse in campurile specifice.

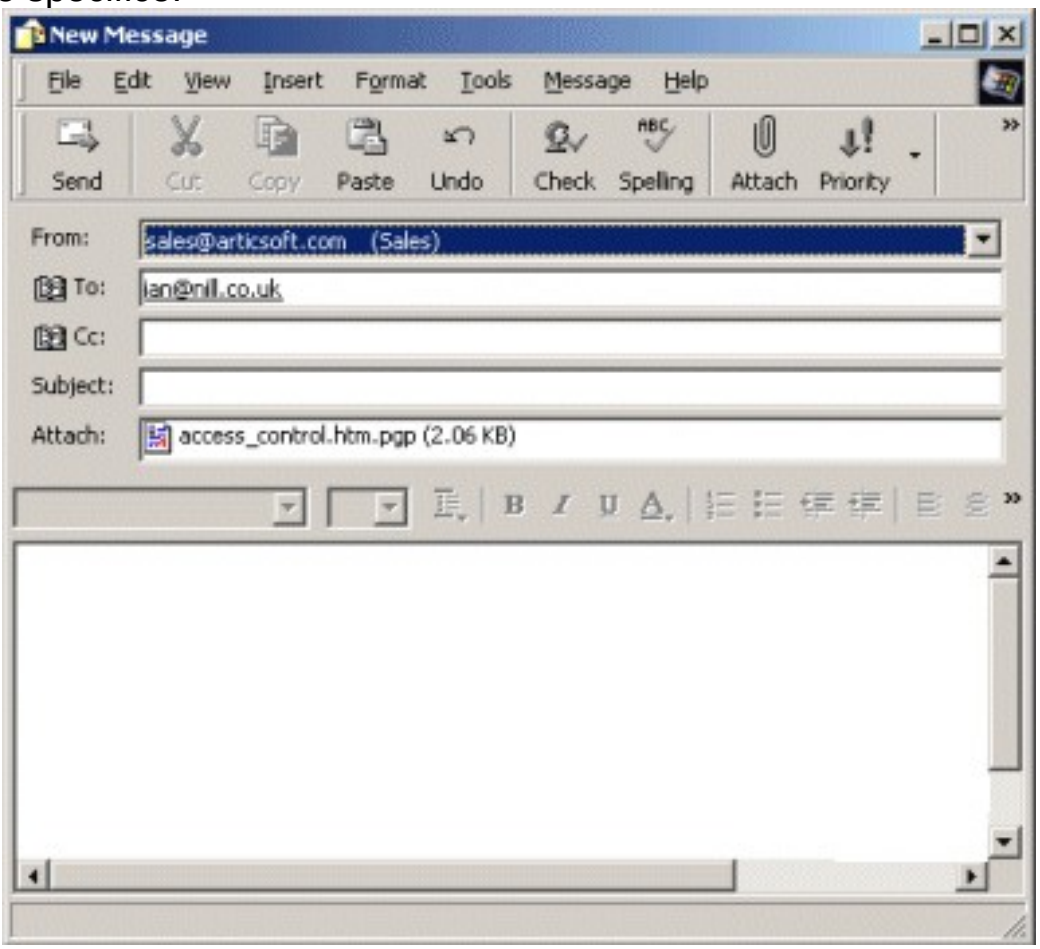


Diagrama 5: Gestionarul de chei al FileAssurity OpenPGP

Aici se pot gestiona propriile chei, precum si cele ale altor persoane si aloca utilizatorii in grupuri.

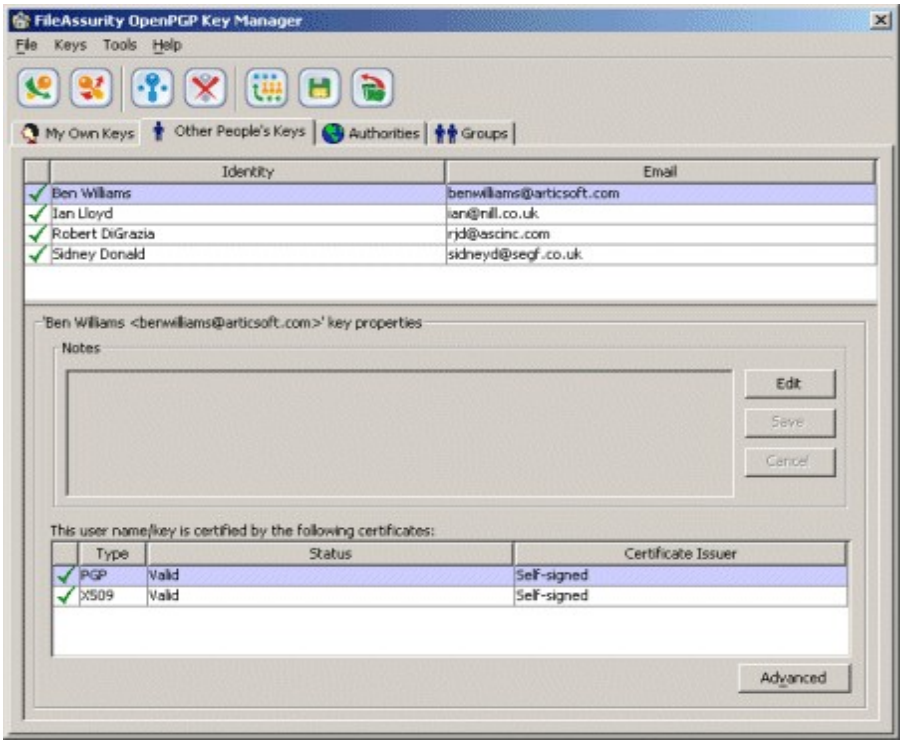


Diagrama 6: Gestionarul de chei al FileAssurity OpenPGP(Grupuri)
Alocarea utilizatorilor in grupuri pentru o mai buna gestionare si utilizare.

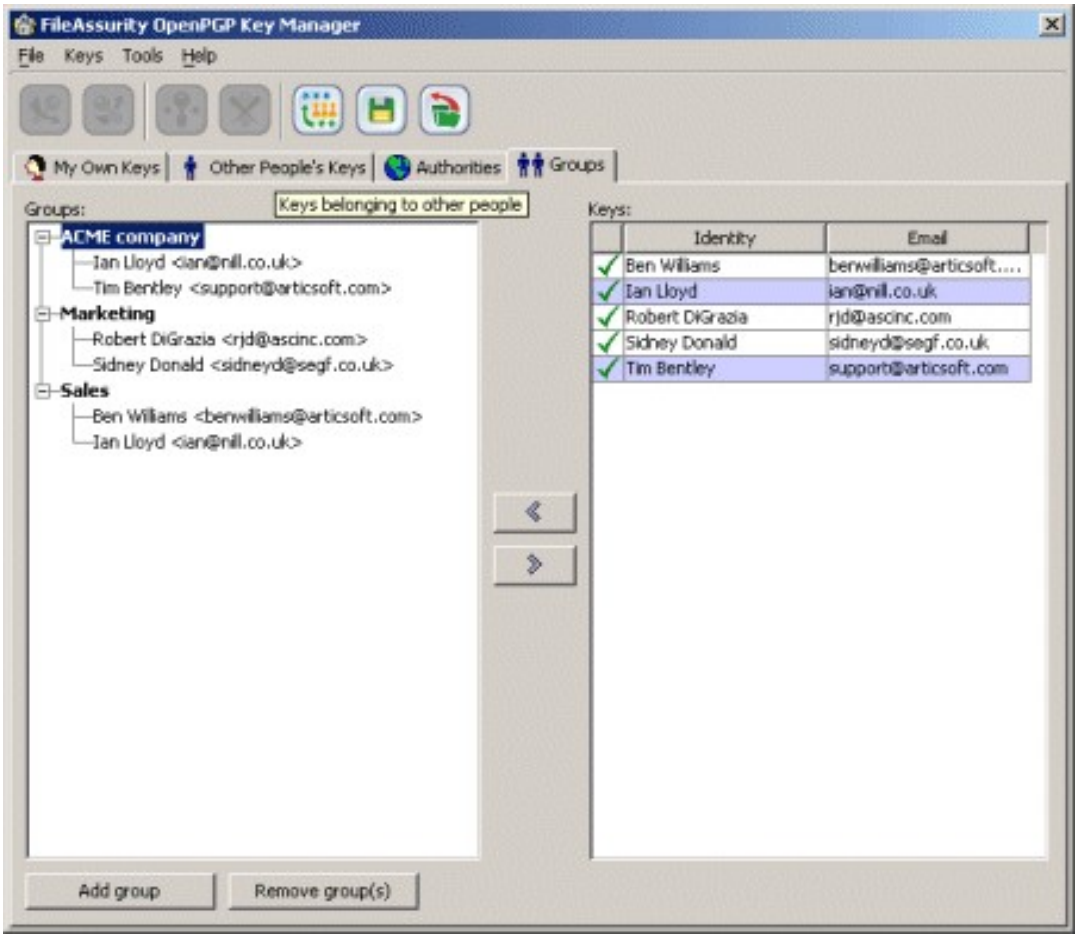
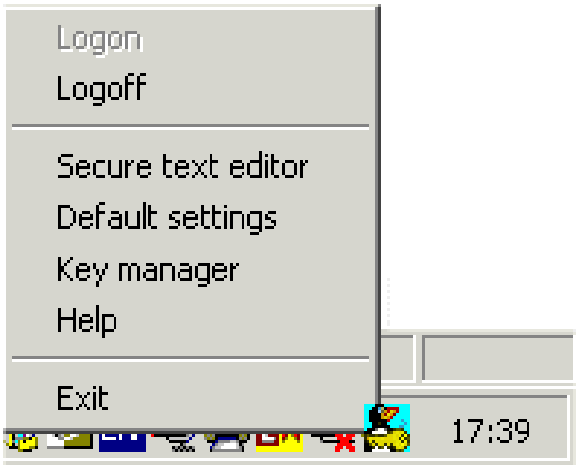


Diagrama 7: FileAssurity OpenPGP –Scurtatura din sistemul Windows
Scurtaturi pentru logare, delogare si facilitati FAOPGP.



- **FileAssurity OpenPGP - Specificatii tehnice**

Fisierele pot fi stocate securizat pe orice suport(local, retea sau memorie externa) sau distribuite securizat. Orice tip de fisier poate fi protejat indiferent de extensia sa.

Standarde: bazat pe OpenPGP(PGP,GnuPGP,etc.) si standarde PKI, ofera integrare completa cu sitemele existente si asigura faptul ca utilizatorul nu este blocat in tehnologii incompatibile.

Compatibilitate PGP:

-Criptarea fisierelor- versiunea 5 si mai noi ale PGP;Pentru versiunile 5.x si 6.x ale PGP, FAOPGP utilizeaza TDES pe 192 biti. Algoritmul AES cu o cheie pe 256 biti e utilizat pentru versiunile 7.x si mai noi.

-Decriptarea fisierelor- versiunile 5.x si mai noi ale PGP;

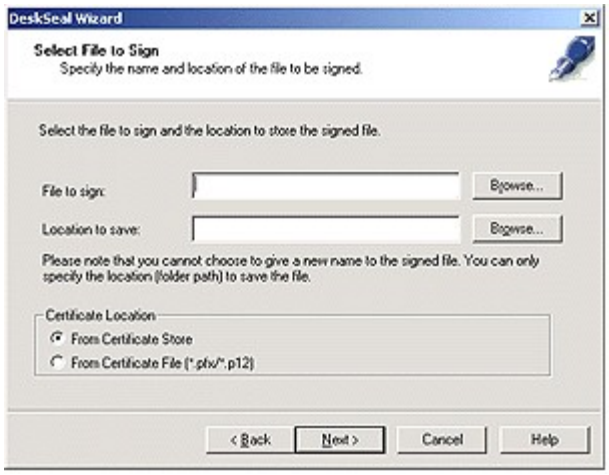
- **Utilizarea produsului:**

- Planuri si schite: Puteti semna digital planuri, schite si orice alt tip de document pentru a putea demonstra ca este autorizat, cine l-a autorizat si cand.
- Inregistrari medicale: Inregistrarile create utilizand orice aplicatie pot fi protejate astfel incat numai cei autorizati le pot vedea. Trebuie sa puteti demonstra cine a avut acces la inregistrari pentru ca acestea sa nu poata fi modificate niciodata fara cunostinta dumneavoastra.
- Contracte: Daca acestea sunt realizate electronic, pot fi semnate digital astfel incat semnatarul sa poata fi identificat, si de asemenea si timpul si data cand a a fost realizat astfel incat sa nu poata fi alterat continutul.
- Copii securizate: Fisiere si foldere pot fi copiate securizat mentinand structura originala intr-o singura arhiva.
- Schimb securizat de informatie: Se pot schimba fisiere indiferent de aplicatia de mail utilizata.

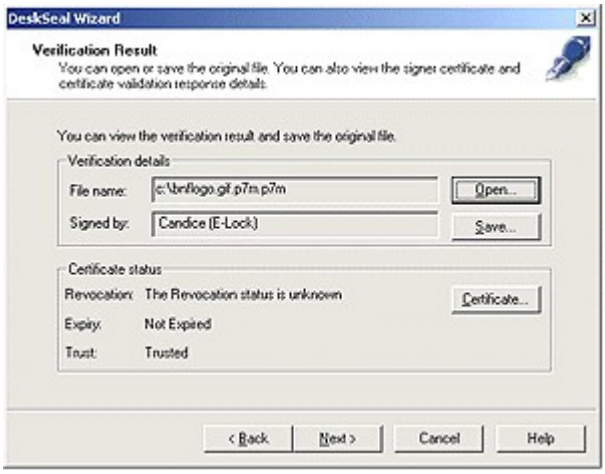
3.4. Altele

- *DeskSeal*

Pentru a utiliza acest soft clientul are nevoie de un certificate digital, salvat intr-un fisier, pe un cd sau un smartcard. *DeskSeal* da posibilitatea de a selecta certificatul din oricare din aceste locatii si de a-l folosi pentru a semna documente in orice format. Un wizard intuitiv ghideaza clientul in procesul de logare, pentru a putea fi utilizat cat mai usor chiar si de catre clientii care o fac pentru prima oara.



Se selecteaza fisierul care se doreste a fi semnat si apoi locatia certificatului care va semna documentul.

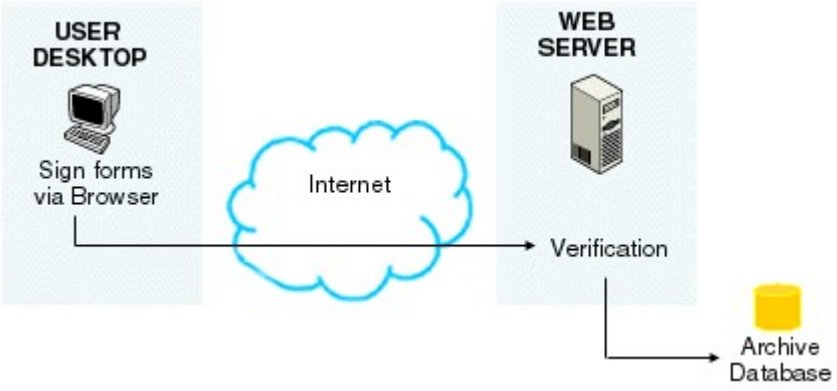


DeskSeal poate fi folosit de asemenea si la verificarea documentelor semnate. Verificarea presupune integritatea datelor (asigurarea ca continutul documentului nu a fost modificat dupa semnare), valabilitatea certificatului care a fost utilizat pt semnare, in cazul in care certificatul a expirat, softul va detecta

acest lucru si va informa corespunzator clientul.

- *FormSeal*

FormSeal este un instrument petru semnatura digitala care poate fi integrat intr-o aplicatie web existenta, si care permite semnarea si verificarea documentelor din cadrul aplicatiei respective. Semnatura se realizeaza pe partea de client, iar componenta client a *FormSeal* da posibiliatea utilizatorilor sa semneze digital documente are apoi sunt trimise serverului. In momentul in care primeste datele utilizatorilor, componenta server FormSeal verifica informatiile inainte de a le accepta si returneaza utilizatorului un mesaj referitor la tranzactia efectuata.Toate verificarile se realizeaza pe partea de server. Aceste verificari furnizeaza informatii referitor valabilitatea si veridicitatea certifiatului utilizat pentru semnatura.



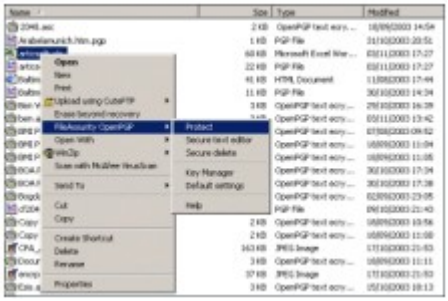
- *ProSigner*

ProSigner este un produs software pentru semnatura digitala care integreaza MS Word, Excel, Adobe si Acrobat. Ofera posibilitatea de a semna si cripta fisiere din Word sau Excel prin intermediul pictogramelor pe care le pune la dispozitie.

De asemenea, ProSigner se integreaza in mediul Windows, astfel incat, printr-un simplu click poate fi semnata sau criptata orice fisier din Windows Explorer sau de pe Desktop.

- *FileAssurity*

Acest produs asigura o comunicare securizata in mai putin de cateva minute. Prin criptarea fisierelor, se asigura ca cei neautorizati nu au acces la aceste fisiere. De asemenea, acorda posibilitatea de a semna digital fisierele pentru ca acestea san nu poata fi modificate sau alterate fara acordul proprietarului si ca ceilalti sa poata verifica autenticitatea fisierelor. Aceasta caracteristica ajuta si la protectia organiatiei impotriva virusilor. Stergerea securizata a fisierelor asigura ca ceilalti nu vor putea sa restaureze fisierele sterse pentru a nu avea acces la informatia privata.



- *Z1 SecureMail Gateway*

Acest soft este destinat cu precadere companiilor. *Z1 SecureMail Gateway* cripteaza si decripteaza emailurile din cadrul unei companii, ramanand transparent fata de expeditorul emailului. De asemenea protejeaza traficul email al intregii companii care il utilizeaza prin intermediul criptarii centralizate I al semnaturii digitale. Un avantaj enorm al utilizarii acestui soft il reprezinta faptul ca mai multe Z1 SecureMail Gateways pot rula in pararel sau sincronizat asigurand astfel o inalta performanta, scalabilitate si o securitate foarte buna chiar si pentru companiile foarte mare.

- *CryptBot*

CryptBot a fost creat pt a facilita securitatea e-Business-ului. Cu ajutorul sa se pot semna, cripta, transmite si stoca diverse tipuri de fisiere cu documente in format digital (.txt, .doc, .htm, .jpeg, .xml etc). Asigura confidentialitatea, integritate si autenticitata fisierelor. Reprezinta un instrument de criptare securizata, care ofera securizarea semnaturii, a transmiterii datelor si a stocarii acetora.

CryptBot combina atat tehnologiile PKY (Public Key Infrastructure) cat si cele PGP (Petty Good Privacy), ceea ce ii ofera o capacitate mare de protectie eficienta. Criptarea sau semnarea documentelor prin intermediul *CryptBot* se realizeaza prin simpla atasare a ubui document XML generat de catre *CryptBot* la fisierul de pe PC sau server, apoi selectarea optiunii dorite (semnatura, criptare).

Confidentialitatea si integritatea comunicarii electronice sunt indispensabile in comertul electronic deoarece increderea clientilor si a partenerilor depind de acestea.

- *DigiSign*

DigiSign S.A. este unul din principalii furnizori din domeniul serviciilor de infrastructura a cheii publice (PKI) si securitatea tehnologiei informatiilor, din Romania. Prin cooperarea cu ADACOM, membra a VeriSign Affiliate Trust Network, *DigiSign* SA ofera produse si servicii de varf pentru piata romaneasca si se recomanda ca partenerul dumneavoastra ideal pentru stabilirea locala a oricarui tip de solutii IT in domeniul PKI.

4. Concluzii

Semnatura digitala este un instrument deosebit de util si puternic totdata, care ofera urmatoarele facilitati:

- Permite semnatarilor unui document sa oficializeze acest act chiar daca se afla la mare distanta geografica fata de locul unde trebuie semnat documentul.

- Prin folosirea semnaturii digitale, destinatarul poate sa fie sigur de identitatea expeditorului.

- Prin faptul ca orice modificare, cat de mica a documentului semnat digital duce automat la anularea semnaturii, destinatarul are convingerea ca documentul a ajuns in stare nealterata.

- Pe de alta parte, un document semnat electronic se supune clauzei juridice de non-repudiere, adica semnatarul nu poate sustine ca nu a semnat acel document. Totusi, pierderea controlului asupra unei chei private de catre semnatar va insemna ca toate semnaturile digitale folosind acea cheie (deci primite “de la” acel utilizator) vor fi suspecte. O astfel de pierdere a controlului nu este o problema de criptare, ci una care tine de factorul uman. Datorita lipsei de protocoale pentru adresarea acestei probleme, semnaturile digitale nu pot oferi astfel non-repudiere completa.

- Orice document semnat digital poate fi tiparit la imprimanta, continand informatia ca documentul original e cel electronic si ca acesta poarta semnatura electronica a semnatarului.

- Implementarea semnaturii electronice aduce companiilor reducerea costurilor si cresterea randamentului

- Intr-o companie, semnatura digitala poate fi utilizata atat pentru procesele interne cat si pentru cele externe. Procesele interne implica interactiuni intre angjati sau departamente ceea ce determina rapoarte de vanzare, rapoarte financiare etc. Procesele externe presupun trenzactii cu clintii, furnizorii, agentiile, guvernul etc., cre mplica o multime de documente cum ar fi: facturi, ordine de plata, contracte legale, acorduri.

5. Bibliografie

[1] http://en.wikipedia.org/wiki/Digital_signature

[2] http://www.baniinostri.ro

[3] http://www.markmedia.ro

[4] https://www.digital-sealing.com/service/service.php?LANG=en

[5] http://www.xyzmo.com/index.php?id=2

[6] http://www.silanis.com

[7] http://www.regielive.ro