Емил Петров Денчев е роден през 1962 г. в град София. През 1988 г. завършва специалност Икономическа информатика в УНСС – София. След това в продължение на 6 години работи в Университетския компютърен център на УНСС като програмист и проектант. От 1990 г. е хоноруван асистент към катедра „Информатика“ на УНСС, а през 1994 г. постъпва като редовен асистент в катедрата. Успешно защитава докторска дисертация през 2002 г. Емил Денчев е титуляр на дисциплините Операционни системи и Програмно осигуряване на ФСД. Научните му интереси са съсредоточени главно в областта на операционните системи, компютърните мрежи и счетоводните продукти. Автор е на редица научни публикации по тези проблеми.

ИНТЕРНЕТ (WEB) ЗАЩИТА НА СЧЕТОВОДНАТА ИНФОРМАЦИЯ

гл.ас. д-р Емил Денчев

1. ВЪВЕДЕНИЕ

Интернет като глобална компютърна мрежа предлага редица услуги, чрез които счетоводната информация (СИ) може:

- да се изпраща до един или повече получатели чрез услугите електронна поща (e-mail) и файлов трансфер (FTP[1]);
- да се публикува в сайт (WWW[2]);
- да се обсъжда на фирмено равнище чрез услугата .Net Messenger[3]. Тази онлайн (on-line) услуга позволява пренос на текст, глас и видео по фирмената компютърна мрежа, базирана на Интернет. Реализирана е с програмите Windows Messenger за MS Windows XP и MSN Messenger за MS Windows 98 Second Edition (SE) и MS Windows Millenium Edition (ME).

Нормативно тези възможности са регламентирани в Закона за счетоводство (ЗС). Така например:

- извеждане на „електронни документи“ или „вторични документи“ [8, чл. 6, ал. 1, т. 2];
- публикуване в Интернет, на фирмен сайт или на сайт на Интернет доставчик (ISP[4]) на справките от Годишния финансов отчет, включващ: Счето-

[1] File Transfer Protocol.
[2] World Wide Web.
[3] Услугата изисква наличието на .NET Passport (http://www.passport.com).
[4] Internet Services Provider.

воден баланс, Отчет за приходите и разходите, Отчет за паричните потоци, Отчет за собствения капитал и приложение [8, чл. 40 ал. 2];

- от 01.01.2004 г. Данъчната администрация на Република България има готовност да приема по Интернет електронно подписани:

- данъчни декларации за дължимите данъци;

- справките за ДДС – Дневник за покупките, Дневник за продажбите и Справка Декларация, за регистрираните фирми по Закона за данък добавена стойност (ЗДДС) може да се изпращат ежемесечно (до 14. число на месеца) до съответната териториална данъчна администрация (ТДУ);

- В момента две софийски митници – Столична митница и митницата на Аерогара – София, приемат по Интернет електронно подписани митнически декларации с гарантирани: самоличност на подателя, цялост и конфиденциалност на информацията в документите, съгласно изискванията на Закона за електронния документ и електронния подпис (ЗЕДЕП) [9, чл. 13, ал. 1, т. 1].

Свързването на бизнеса с Интернет (Web) технологиите предоставя много допълнителни предимства, но и определени рискове, свързани с възможността за:

- нерегламентиран отдалечен достъп на споделена СИ;
- достъп до предаваната СИ по каналите за връзка на фирмените мрежи, базирани на Интернет.

2. МЕТОДИ ЗА ИНТЕРНЕТ ЗАЩИТА НА СЧЕТОВОДНАТА ИНФОРМАЦИЯ

2.1. Програмни методи

Програмните методи за защита са базирани на средствата на приложното и системно програмно осигуряване. Защитата се реализира чрез:

- задаване на пароли за достъп до „споделена“ (Shared) по мрежата СИ;
- определяне на права за отдалечен достъп до споделена СИ;
- архивиране на СИ в реално време – on-line архивиране;
- on-line актуализиране на антивирусните програми (Live Update);
- актуализиране на операционната система (Update);
- защитни стени (Firewall);
- виртуални частни мрежи (VPN[1]);
- on-line сканиране на работното място.

2.1.1. Пароли за достъп до споделена (Shared) по мрежата СИ

СИ като информационен ресурс може да се споделя и достъпва отдалечено по фирмената компютърна мрежа от други потребители. Защитата от нерегламентиран достъп до споделена СИ се осъществява чрез пароли за достъп.

По отношение на паролите за достъп съгласно изискванията на международния стандарт за сигурност С2 се препоръчва:

[1] Virtual Private Network – виртуална частна мрежа.

- да не „говорят“ за потребителя, т.е. като пароли не трябва да се използват общоизвестни неща за потребителя като имена и рождени дати, тъй като те са известни на голям кръг хора;
- да се състоят от минимум 8 символа – целта е да се увеличи броят на възможните комбинации, които друг потребител трябва да въведе за „отгадване“ на съответната парола;
- да се състоят от комбинация от букви, цифри и специални символи (всички останали) – целта е отново да се увеличи броят на възможните комбинации.

Особености:

- тъй като полето, в което се описва и въвежда съответната парола, е „чувствително“ (case sensitive) към регистъра на буквите – главни, малки, и типа им – кирилица, латиница, се препоръчва използване на букви с различен регистър и/или тип с цел нарастване на възможните комбинации – например Qw48#2$R;
- променят се периодично – през определен период или при промяна на служебното положение. Целта е да се прекрати неразрешеният достъп, ако съответната парола е била отгатна;
- не се повтарят при промяната им, тъй като старата парола може да е станала известна, т.е. препоръчва се спазването на т.нар. „история“ на паролите;
- не се използват едни и същи пароли при работа с различните приложения – счетоводни продукти, програми за електронна поща (e-mail), за диалогови разговори (.NET Messenger, ICQ, IRC) и т.н.;
- съхраняват се на сигурно място – на технически носители, различни от твърдия магнитен диск – например дискета, магнитно-оптичен диск или смарт карта.

Във връзка с това се използват програми за генериране и съхраняване на пароли, каквато е програмата Password Safe на компанията Counterpane Labs Systems. Тя може да се свали (download) безплатно от Интернет от сайта на компанията (Web адрес – http://www.counterpane.com).

2.1.2. Определяне на права за отдалечен достъп до споделена СИ

Правата за отдалечен достъп до споделена СИ се задават на равнище потребител (главен счетоводител) или група от потребители (счетоводители, касиери, материалноотговорни лица, администратори и т.н.). Правата за достъп за група от потребители се задават еднократно, след което включването на нов потребител в групата води до „наследяването“ от него на тези права. Задават се права за достъп до извършване на определени действия със СИ:

- четене (read only) – СИ може да се чете от друг потребител, но не и да се променя, изтрива, архивира и т.н.;
- разпечатване (print) – СИ може да се разпечатва под формата на справки. Например счетоводител може да изведе справката „Хронологичен опис на операциите“, но материалноотговорно лице не;
- променяне (update) – например счетоводител може да сторнира счетоводно записване или да добавя нов елемент към дадена номенклатура;
- изтриване (delete) – например изтриване на елемент от наменклатура „Клиенти“ от групата на счетоводителите;

- архивиране (back up) – СИ се архивира под формата на „текущ“ или „постоянен“ архив от групата на администраторите;
- без достъп – съответният потребител може да получи забрана за достъп до определено действие, свързано със съществена промяна на СИ. Например само главният счетоводител може да приключва счетоводния период, а останалите потребители не.

2.1.3. Архивиране на СИ в реално време – on-line архивиране

Архивирането на СИ е средство за защитата ѝ от разрушаване по технически причини. Тъй като не се препоръчва съхраняване на магнитния архив върху локалния твърд магнитен диск, като една от алтернативните възможности се използва т.нар. „архивиране в реално време“ (on-line). Осъществява се по Интернет върху диск на сървър за данни. От него СИ може да се възстанови при загуба или разрушаване по технически причини.

2.1.4. On-line актуализиране на антивирусните програми (Live Update)

Антивирусните програми са средство на защита на СИ от разрушаване от компютърни вируси. Поради голямата динамика в разпространението на нови компютърни вируси и поради това, че част от потребителите не знаят за периода на актуализация на файловете с вирус дефинициите, фирмите, разработили антивирусни програми, предлагат on-line (live update) актуализиране на тези файлове. Извършва се по Интернет от сайта на фирмата.

2.1.5. Актуализиране на операционната система (Update)

Една от причините за актуализиране на операционните системи е отстраняването на т.нар. „пробойни“ в сигурността им. Фирмите, разработили операционни системи, периодично пускат „програми – кръпки“ (Patch), с които се решават тези проблеми. Например през 2003 г. фирмата Microsoft разработи „patch“ за програмите Internet Explorer и Outlook Express за Windows XP поради възможността за нерегламентиран отдалечен достъп до компютърните ресурси, в т.ч. и СИ.

2.1.6. Защитни стени (Firewall)

Защитните стени са средство за защита на информацията, в т.ч. и СИ, съхранявана в работни места от фирмена компютърна мрежа, базирана на Интернет. MS Windows XP и MS Windows Server 2003 поддържат вградени защитни стени (ICF[1]), които предпазват от входящи „атаки“, но не следят изходящия трафик. Това носи риск от проникване на компютърни вируси – „червеи“ или „троянски коне“, чрез електронната поща, които след активирането си изпращат информация навън. Една от популярните защитни стени в момента е Norton Personal Firewall 2003 на фирмата Symantec (http://www.symantec.com).

[1] Internet Connection Firewall.

2.1.7. Виртуални частни мрежи (VPN)

Създаването на виртуална частна мрежа е възможност за една фирма да се свърже надеждно със своите клонове или с други фирми и да обработва и предава СИ, използвайки Интернет.

Във виртуалните частни мрежи, базирани на Интернет, се използват и средства, поддържани от Windows 2000 Server, Windows XP Professional и Windows Server 2003 [2], [5], [6], [7], [10]:

- **Kerberos** е протокол за достъп, чрез който фирмените служители се включват (Logon) веднъж, но получават достъп до ресурсите (информационни, приложни и технически) в цялата мрежа. Протоколът е стандартен и дава възможност за взаимна проверка на кореспондентите, за засекретяване на сесиите при пълна съгласуваност с останалите стандартни приложения. Всичко това означава, че фирмените служители ще трябва да запомнят една-единствена парола. Ползването на една-единствена парола значително улеснява администрирането на компютърната мрежа и на достъпа до споделените в нея ресурси.
- **Authenticode** е технология за защита, реализирана в MS Internet Explorer. Позволява цифрово подписване на архивите със СИ. Тези подписи могат да се използват за проверка както на създателя на архива, така и на целостта на съдържанието му в момента на възстановяване на СИ.
- **Кодираната файлова система** – (EFS[1]), е разширение на файловата система NTFS и предоставя защита на СИ чрез кодирането на файлове и папки с използването на публични ключове. Употребява се за защита на споделена СИ при отдалеченото ѝ достъпване по мрежата.
- **On-line сканиране на работното място** – извършва се с цел тестване на уязвимостта на системата. Web сайтове, от които може да се извърши on-line сканиране и тестване, са http://scan.sygate.com и https://grc.com/x/ne.dll?bh0bkyd2.
- **Microsoft Baseline Security Analyzer (MBSA)** е разработен с цел извършване на оценка на степента на защита на един или повече компютри от VPN мрежата, базирани на Windows. MBSA определя дали вградените в тях системи за защита не са остарели и трябва да се актуализират.

2.2. Криптографски методи

Криптографските методи за защита на СИ се прилагат при предаването ѝ по канали за връзка. Това се налага при обработката на СИ в режим на разпределена обработка, при който СИ се обработва локално в поделенията на фирмата и периодично се обобщава в централата на фирмата посредством предаването ѝ по канали за връзка на фирмената компютърна мрежа.

Една от технологиите за криптиране на СИ, използвана в Република България, е технологията „Инфраструктура публичен ключ“ (PKI[2]). Реализира се чрез използване на цифрови сертификати, издавани от „Доставчици на удостоверителни услуги“ (ДУУ), наричани още и Certificate Authority (CA). В момента лицензирани ДУУ в Република България са:

---

[1] Encrypted File System – криптираща файлова система.

[2] Public Key Infrastructure – инфраструктура публичен ключ.

- фирма „Информационно обслужване“;
- Банк Сервиз, която обслужва банките и застрахователните компании;
- Българска стопанска камара.

Чрез технологията „Инфраструктура публичен ключ“ се реализират следните свойства:

- конфиденциалност – СИ е достъпна само за този потребител, за когото е предназначена тя, т.е само за получателя ѝ;

- удостоверяване на самоличността на подателя – позволява на подателя на СИ да докаже своята идентичност на получателя ѝ;

- цялост на СИ – означава запазване на съдържанието на СИ спрямо вида, в който тя е изпратена. Или процесът гарантира целостта на счетоводната информация от нерегламентирана промяна (модификация) при прехвърлянето ѝ по канала за връзка;

- защита от повторение – процес, който не позволява прихващане на СИ, свързана с подател – получател по мрежата и по-късното ѝ използване за неразрешен достъп до счетоводната информация.

Реализирането на тези свойства се постига с кодиране (криптиране) на счетоводната информация. „Криптографията е комплекс от математически техники за кодиране и декодиране на данни, така че те да се прехвърлят по мрежата сигурно и да не се използват от неоторизирани потребители“ [5]. За да се постигне тази цел, при кодирането се използват алгоритми в комбинация от ключове – публичен и личен ключ, които са свързани математически.

Технологията реализира свойството „конфиденциалност“ на СИ, като:

- подателят придобива публичния ключ на получателя;
- публичният ключ на получателя може да се придобие, като получателят на СИ го изпрати на подателя или подателят изтегли публичния ключ на получателя, използвайки услугите на ДУУ;
- подателят криптира съобщението с публичния ключ на получателя и му го изпраща по канала за връзка.
- получателят декриптира съобщението със своя личен ключ.

При кодирането не се използва личният ключ на подателя, защото кодираното съобщение може да се декодира от трето лице с общоизвестния публичен ключ на подателя.

Свойството „цялост“ на СИ се постига чрез изчисляване на т.нар. „профил“ (message digest). За кодирането на профила подателят използва своя личен ключ. При получаване на СИ получателят декодира профила, използвайки публичния ключ на подателя. След това получателят изчислява нов профил на СИ и го сравнява с получения и декодиран профил на подателя. Ако двата профила съвпадат, целостта на СИ е гарантирана. Ако двата профила не съвпадат, подателят не носи юридическа отговорност за верността на СИ.

Свойството „удостоверяване на самоличност“ се осъществява чрез кодирането на профила на СИ с личния ключ на подателя. Тъй като профилът се декодира само с неговия публичен ключ, получателят може да бъде сигурен, че СИ идва от собственика на двойката ключове, тъй като доставчикът на удостоверителни услуги (ДУУ) гарантира, че двойката ключове принадлежи на действителния подател, а не на някой, който се представя за него.

В точка 3 са разгледани възможностите на програмите **MS Outlook 98, MS Outlook Express 5 и Netscape Navigator** за цифрово подписване и кодиране (криптиране) на счетоводната информация.

2.3. Правни методи

Правните методи за Интернет защита на СИ са базирани на съществуващата нормативна база в Република България, включваща:

- Закон за електронния документ и електронния подпис;
- Наказателно-процесуален кодекс (НПК).

Тези нормативни актове регламентират правно защитата на СИ от неправомерно копиране, изтриване и промяна – действия, които вече са криминализирани с поправките в НПК.

2.4. Технически методи

Техническите методи за Интернет защита на СИ включват използването на технически средства за ограничаване на достъпа до СИ като:

- **Smart-картите** – това са носители с размерите на кредитните карти и могат да се използват за съхранение на публичния ключ, личния ключ и копие на сертификата на потребителя, издаден от ДУУ (СА). Те са по-сигурен начин за защита и управление на потребителските ключове от съхранението им на компютъра. Като използват смарт-карти, на хората във фирмата няма да им се налага да помнят множество пароли, а само един PIN-код (ПИН), който може да бъде използван и за много други нужди – например цифрово подписване на СИ при изпращането ѝ по електронна поща.
- **Хардуерно реализирани защитни стени (Hardware Firewall)** – това са технически средства (маршрутизатори), включени към сървърите от фирмената компютърна мрежа, базирана на Интернет, с цел филтриране и ограничване на нерегламентиран отдалечен достъп до съответните ресурси, в т.ч. и СИ като информационен ресурс.

3. ЦИФРОВО ПОДПИСВАНЕ И КОДИРАНЕ (КРИПТИРАНЕ) НА СЧЕТОВОДНАТА ИНФОРМАЦИЯ

3.1. MS Outlook 98

Програмата MS Outlook 98 е клиентска програма на фирмата Microsoft за достъп до услугата „Електронна поща“ (E-mail).

След като се получи цифровият сертификат от доставчика на удостоверителни услуги (ДУУ), чрез програмата MS Outlook 98 счетоводната информация (СИ) може да се изпраща на един или няколко получателя като „прикачен“ или „прикачени“ файлове (Attach file), като се подписва цифрово и се кодира (криптира). Тези две операции са различни – може да се подписват цифрово и/или кодират (криптират) съобщенията, съдържащи СИ.

Цифрово подписване на СИ, изпращана чрез „Електронна поща“

В програмата за електронна поща MS Outlook 98 може да се конфигурира начинът за цифрово подписване на СИ:

1. Всеки път, когато се изпраща електронна поща (т.е. когато се съставя, отговаря се или се пренасочва дадено съобщение с „прикачена“ СИ).

2. Или само когато потребителят иска да направи това, щраквайки с мишката върху означения бутон.

Процедурата за подписване използва „личен ключ“, който е необходим за:

- удостоверяване (потвърждаване) самоличността на всеки един участник в електронното общуване – подател – получател.
- гарантиране на „целостта“ на съдържанието на СИ.
- гарантиране „неотменяемостта“ на електронното общуване.

Т.е. когато се подписва съобщение, получателят може да бъде сигурен, че това съобщение идва от точно определен подател.

Подписването на съобщението не засяга съдържанието на съобщението или не го защитава от прихващане и прочитане от друг (трето лице) освен от получателя. За да се гарантира, че само получателят може да прочете съобщението, т.е. за да се реализира свойството „конфиденциалност“, то трябва също така да се кодира (криптира).

Кодиране (криптиране) на СИ, изпращана чрез „Електронна поща“

При изпращане конфиденциалните съобщения трябва да се кодират (криптират).

За да се кодира съобщение, така че само получателят да може да го прочете, подателят трябва да разполага в адресната си книга с копие от цифровия сертификат на получателя.

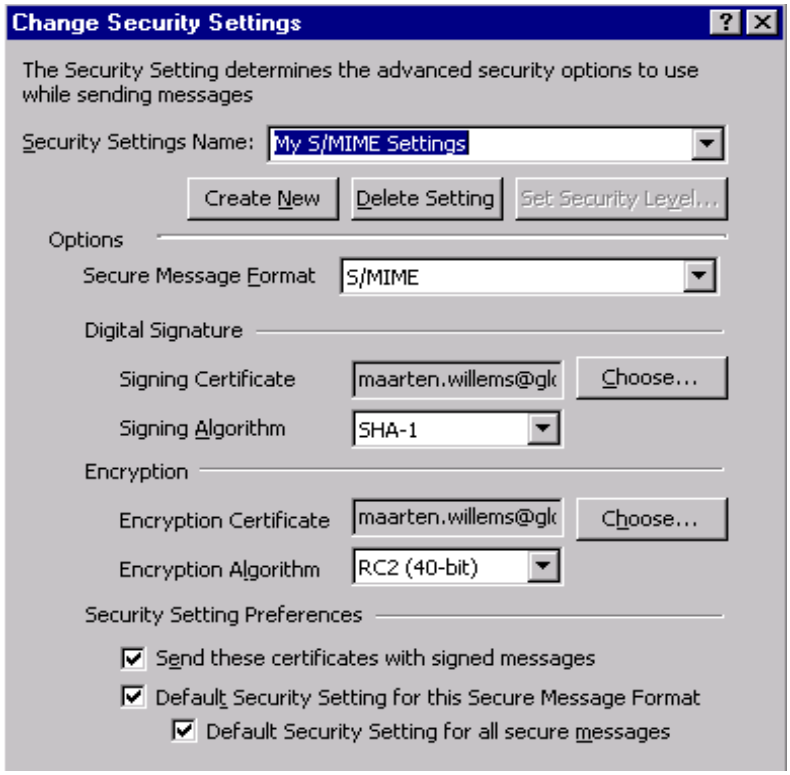
За да се получи този сертификат (на получателя), подателят може да поиска от него да изпрати подписана „електронна поща“ (е-поща), която ще съдържа сертификата му и приложен към него публичен ключ, или да открие сертификата „он-лайн“ (On-line) в публичния указател на Доставчика на удостоверителни услуги (ДУУ).

Инсталиране на личен цифров сертификат и настройка за сигурност

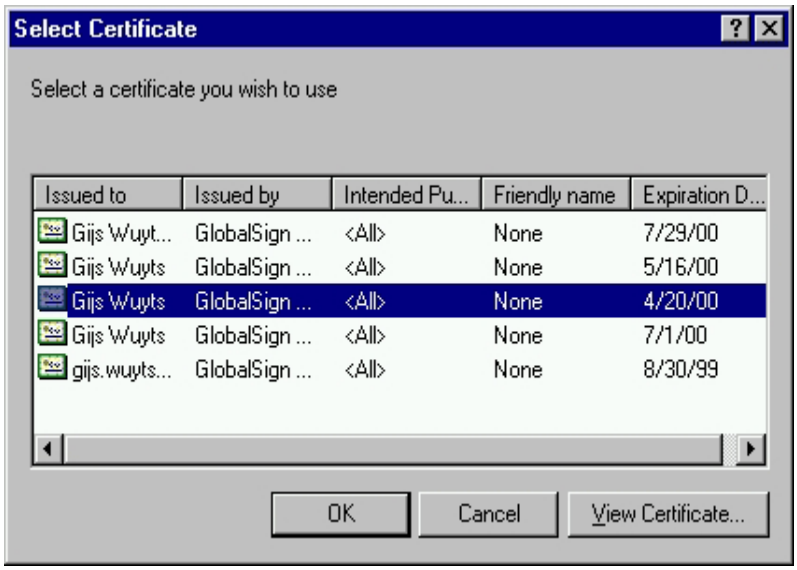
Активира се приложението MS Outlook 98 и се изпълняват функциите Options/Security от менюто Tools на MS Outlook 98. С бутона Change Settings се визуализира следващият прозорец.

Може да се създадат различни настройки за сигурност и да се съхранят под различни имена.

- Формат на защитено съобщение (тип „е-поща“) – Secure Message Format (Type of e-mail).
- Настройки за цифров подпис – Digital Signature Settings.
- Настройки за кодиране – Encryption Settings.
- Security Setting Preferences (Setting defaults).

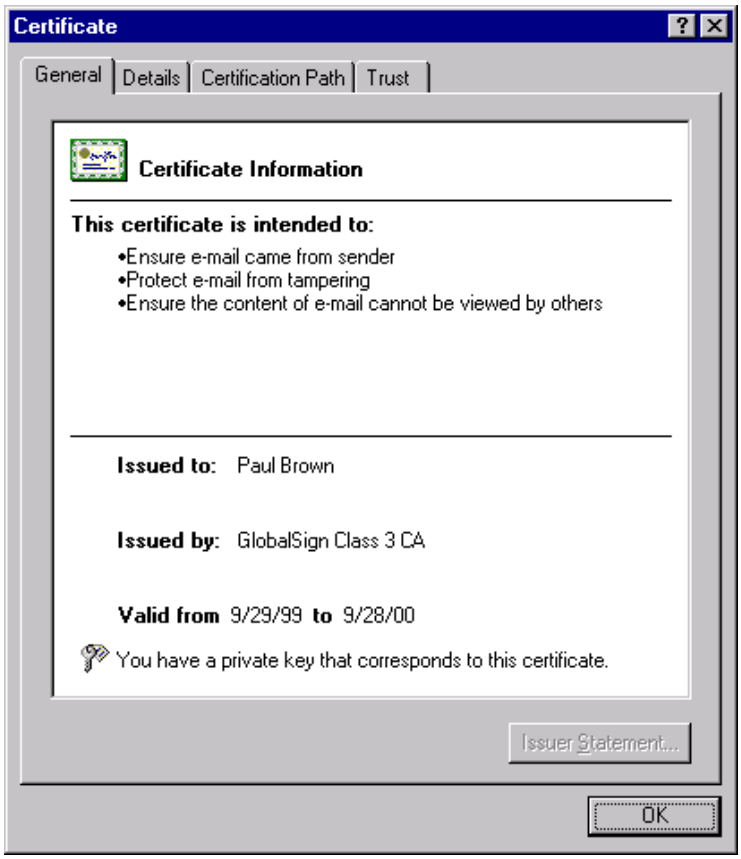


Настройките за цифров подпис (Digital Signature) позволяват да се избере сертификат, който ще се използва за подписване на „е-пощата“. С бутон Choose се визуализира следният прозорец:



Този прозорец позволява да се определи кой сертификат ще се използва в настройките с цел подписване.

С бутон View Certificate… се визуализира екран, който показва общия вид на сертификата:



Разделът за настройките на цифровия подпис позволява също да се определи кой вид „Hash“ алгоритъм ще се приложи за създаване на подписите – (SHA-1, MD5).

Настройките за кодиране (Encryption Settings) позволяват също да се избере сертификат, който ще се използва за подписване на „е-пощата“.

Изпращане на защитена СИ с MS Outlook 98

1. Взема се личният цифров сертификат от Уеб сайта (Web Site) на ДУУ, представител на GlobalSign България.
2. Използва се цифровият сертификат да се подпише цифрово и/или кодира (криптира) „е-пощата“.

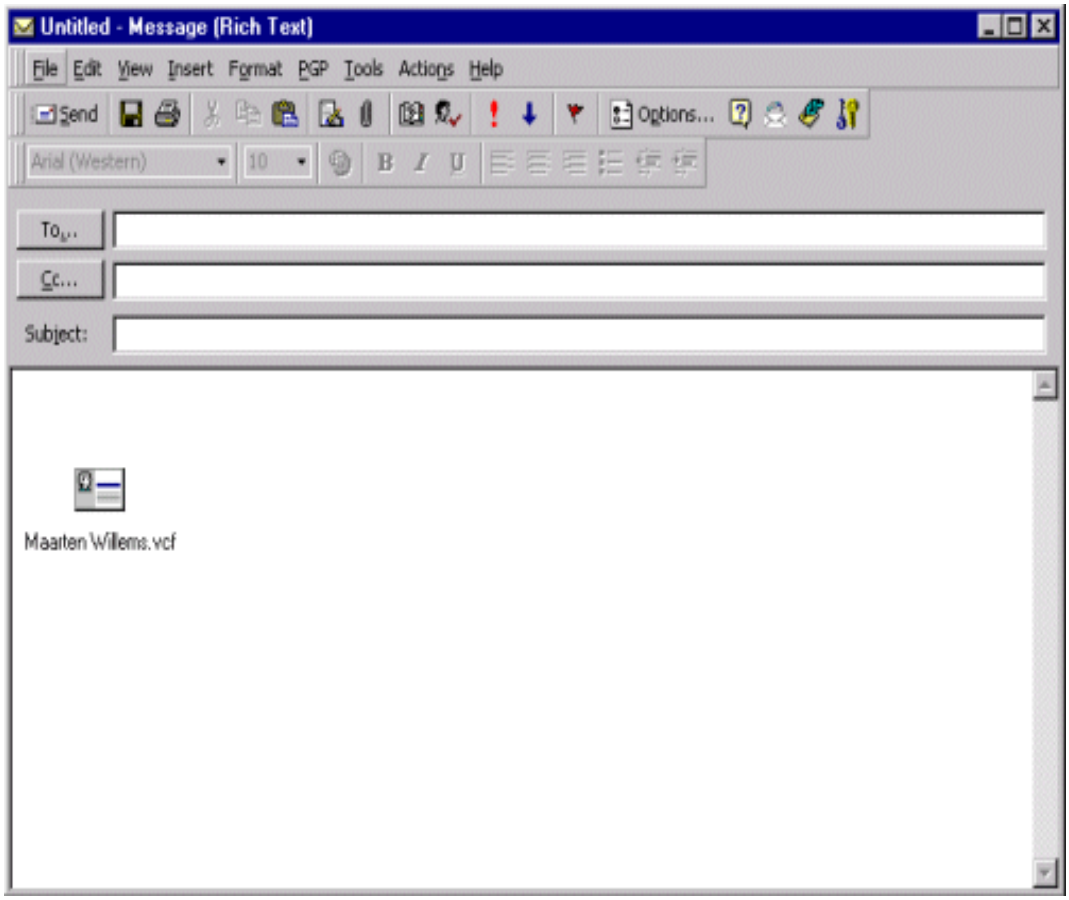
Практика – цифрово подписване на СИ, предавана по електронна поща с MS Outlook 98

Ако получателят на подписаното съобщение използва пакета „S/MIME“, той би могъл да прочете съобщението. В този случай цифровият подпис на подателя

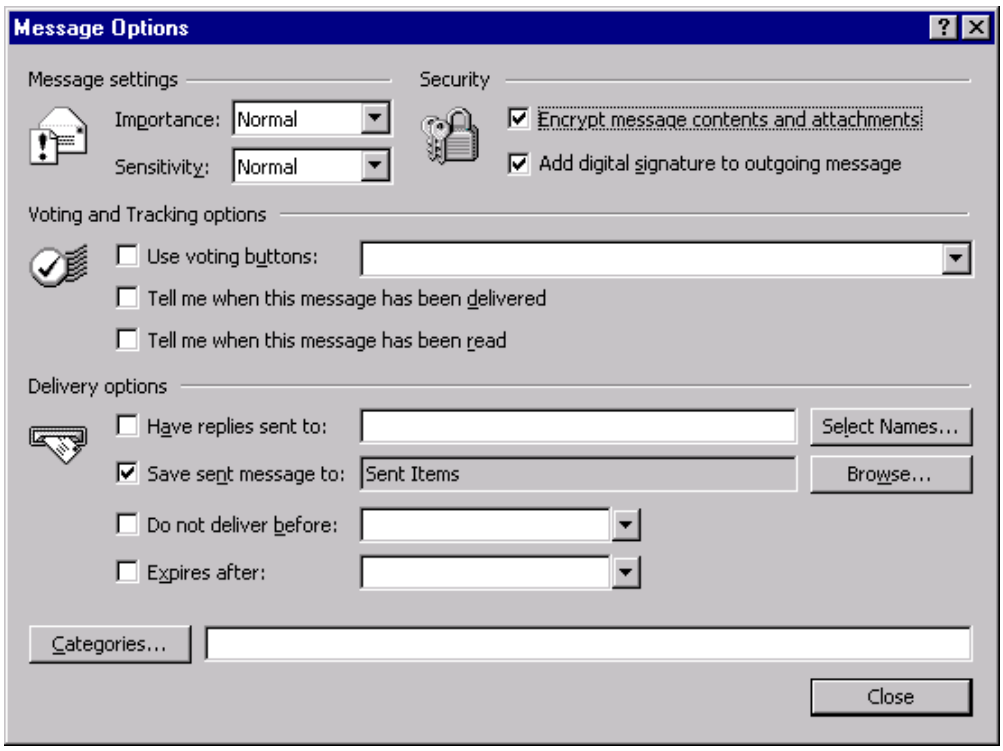
се показва като приложение. Иконата за „**подписан**“ показва, че полученото съобщение е подписано.

Иконата за подпис без доверие показва, че полученото съобщение е било подписано от сертификат, издаден от доставчик, на който все още не се гласува доверие (защото не е инсталиран неговият главен /root/ сертификат). В този случай иконата ще изглежда по следния начин:

Може да се подписват съобщенията всеки път, когато подателят иска да ги подпише, или може да се конфигурират настройките за сигурност (както бе описано по-горе), за да подписва, като се използва специфичен сертификат. За да се подпише е-пощата индивидуално, се използва бутон Options… в прозореца на електронната поща:



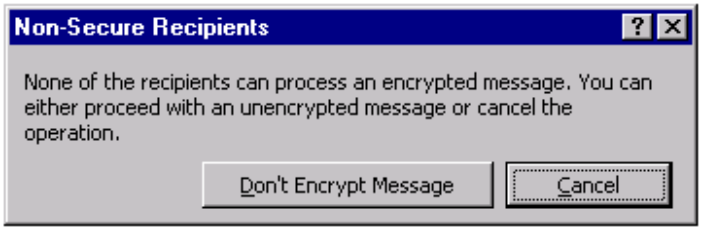
Визуализира се следният прозорец:



Този прозорец позволява да се използват специфични опции за електронна поща, която ще се изпраща. Опциите включват: дали електронната поща трябва да се кодира (криптира) и дали трябва да се добави цифров подпис към съобщението в изходящата поща (т.е. подписване на „е-поща“). Тези настройки се прилагат към пощата, която ще се изпраща.

Кодиране (криптиране) на е-пощата с MS Outlook 98

Втората стъпка за защита на съобщенията в електронната поща е те да се кодират (криптират). Кодирането с MS Outlook 98 се извършва подобно на „подписването“.



За да се кодира (криптира) съобщение, трябва да е налице копие от цифровия сертификат на получателя. Като се получи подписано съобщение, получателят

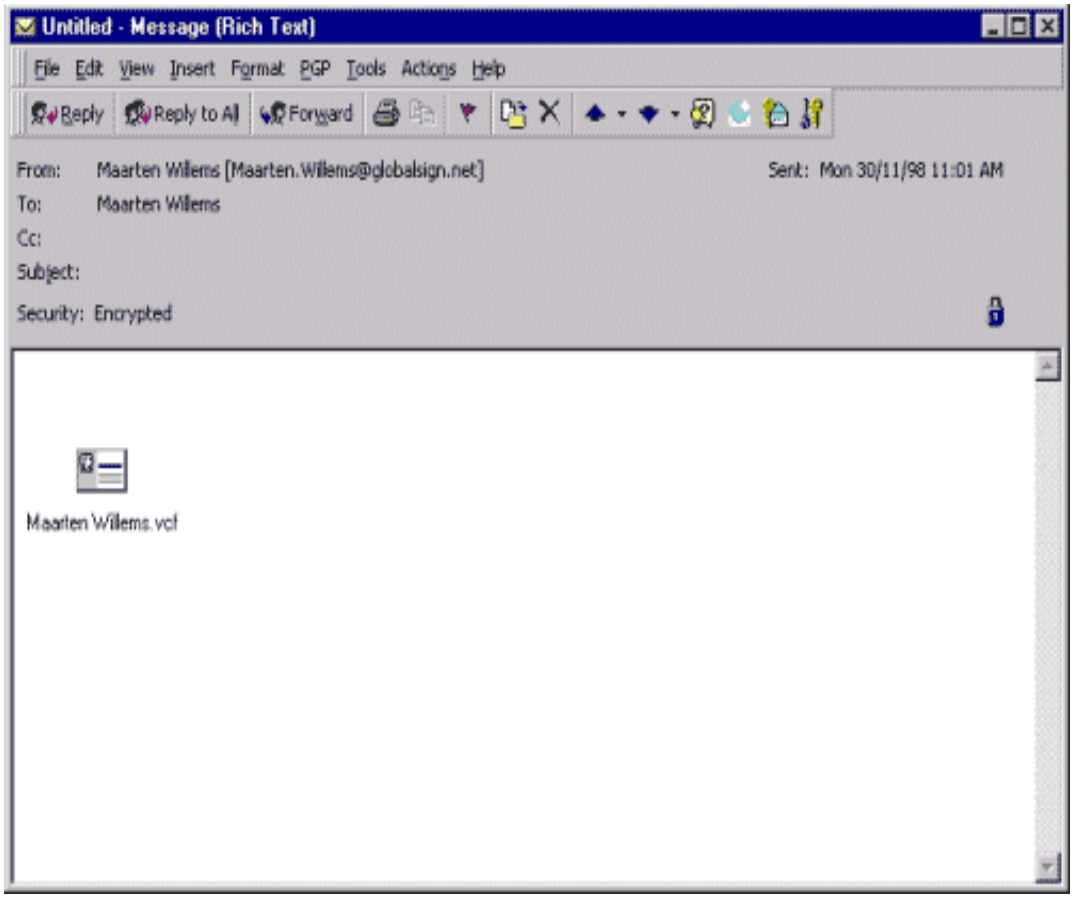
може да запази сертификата на подателя в адресната си книга. Това е необходимо, ако трябва да се изпраща кодирана (криптирана) електронна поща до това лице.

Може също така да се открие цифров сертификат в он-лайн (On-line) указателя на ДУУ (Информационно обслужване, БСК, Банк Сервиз).

Като се получи електронна поща, „**кодираната**“ икона посочва, че съобщението е било кодирано (криптирано). Тази икона се появява в долния десен ъгъл на изписания адрес. Процесът на кодиране се извършва автоматично.

Може да се кодират съобщенията всеки път ръчно, когато се налага това, или може да се конфигурират опциите за сигурност, така че съобщенията да се кодират (криптират) автоматично, щом цифровият сертификат на получателя да присъства в адресната книга на подателя.

Когато се получи кодирано съобщение, иконата за кодиране (криптиране) се появява на прозореца за електронна поща:



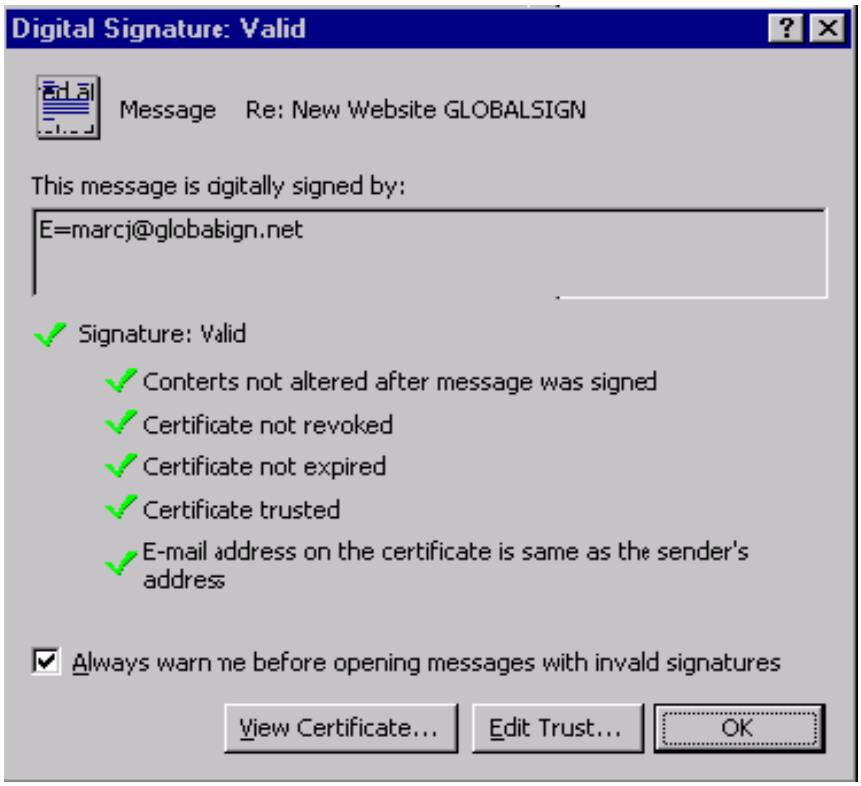
Управление на кореспондентските цифрови сертификати

За да се изпрати кодирано (криптирано) съобщение на някого, подателят трябва да разполага в адресната си книга с копие от цифровия сертификат на съответния получател. MS Outlook 98 дава възможност да се видят, добавят и отстранят цифрови сертификати.

Запазване на цифров сертификат от подписано съобщение

Когато се получи подписано кодирано съобщение, получателят може да си запази цифровия сертификат на това лице (подателя) в адресната си книга. За тази цел първо се щраква два пъти с мишката върху подписаната икона, представена като:

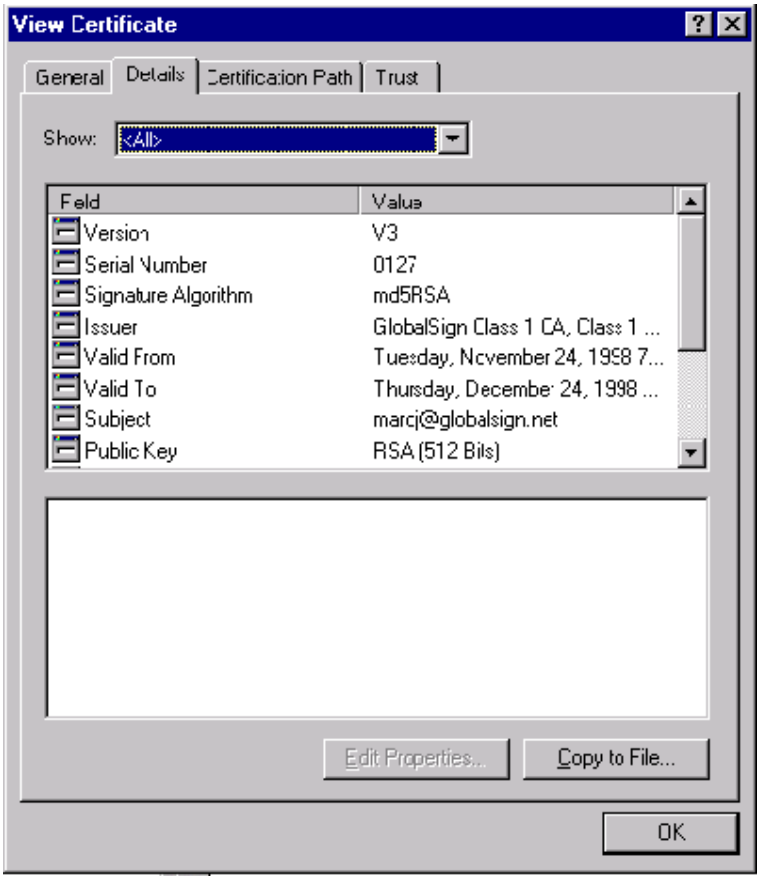
Визуализира се следният прозорец:



Този прозорец предоставя повече информация за сертификата, който е бил използван за подписване на „е-пощата“ от подателя (изпращача). С бутона View Certificate…. се визуализира следният прозорец:

С щракване с мишката върху страницата Details се визуализира следващият прозорец.

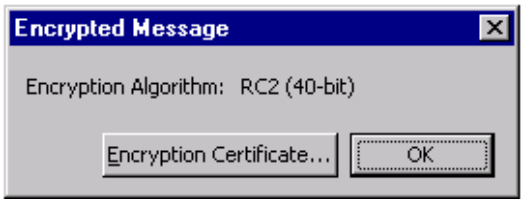
С бутон Copy to File… може да се експортира (съхрани) специфичният сертификат във файл. Сега вече може да се импортира този сертификат в адресната книга (както е описано по-нататък).



Запазване на цифров сертификат от кодирано съобщение

Когато се получи подписано кодирано съобщение, получателят може да запази в адресната си книга цифровия сертификат на подателя. За тази цел първо се щраква два пъти върху подписаната икона, представена като:

Визуализира се следният прозорец:



Този прозорец показва кой „хеш-алгоритъм“ е бил използван за създаване на цифровия сертификат, а също така позволява да се види сертификатът.

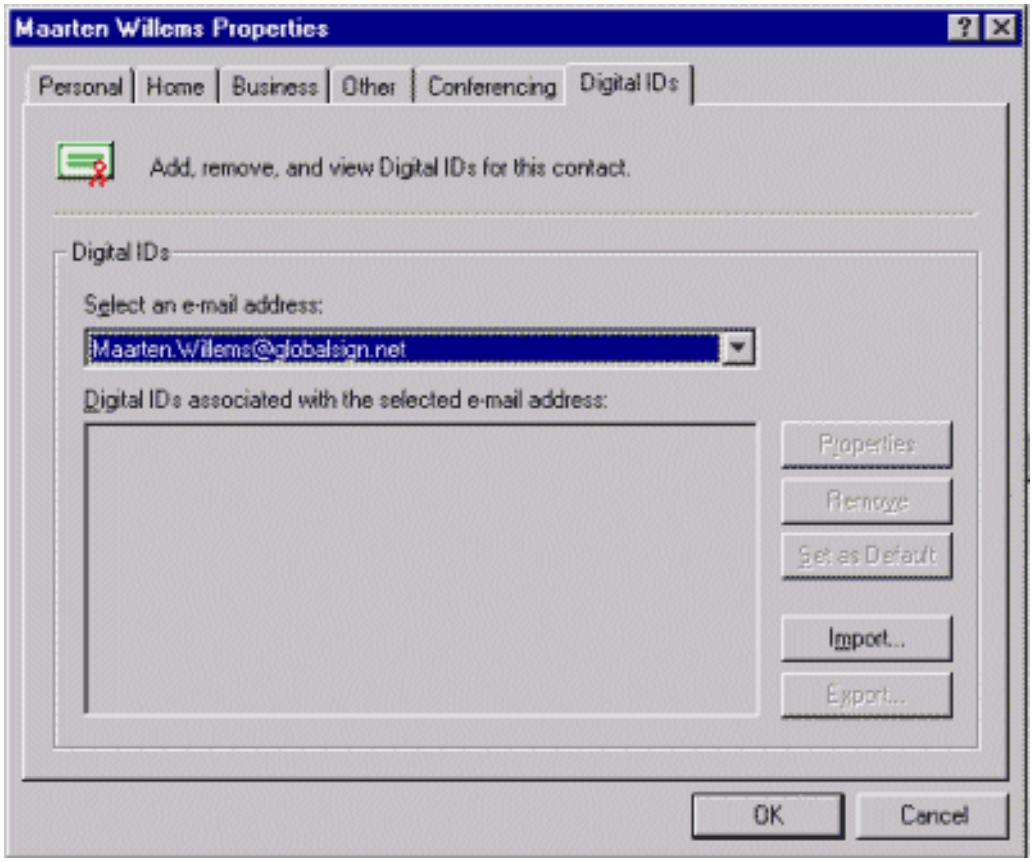
С бутона за кодиране – Encryption Certificate…, се визуализира прозорецът View Certificate, както беше показано по-горе. Този прозорец позволява да се копира сертификатът чрез бутона Copy to File…

Импортиране на зареден цифров сертификат

Може да се търси цифров сертификат в базата данни „он-лайн“ (On-line), да се зареди и да се добави в адресната книга, така че да може да се изпраща кодирано съобщение на съответното лице.

За импорт на зареден цифров сертификат в адресната книга:

1) създава се в MS Outlook 98 нов e-mail адрес или се отваря вече съществуващ адрес;
2) избира се цифровият ID – Digital IDs;
3) щраква се на бутон Import;
4) избира се зареденият файл с цифровия сертификат и след това се щраква на бутон Open.



За да се отстрани цифров сертификат от адресната книга:

1) отваря се адресът на лицето, за което ще се „сваля“ цифровият сертификат;
2) избира се страницата Digital Ids;

3) избира се сертификатът, който трябва да се отстрани;
4) щраква се с мишката върху бутон Remove.

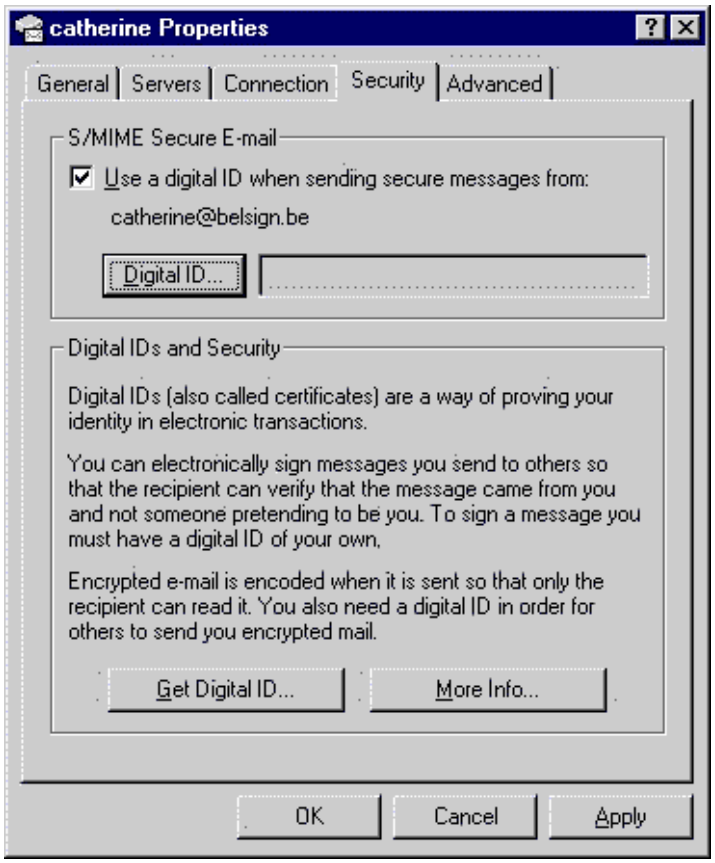
Когато даден цифров сертификат е отстранен, повече не може да се изпращат кодирани съобщения до това лице.

3.2. MS Outlook Express 5

Програмата MS Outlook Express 5 е клиентска програма на фирмата Microsoft за достъп до услугата „Електронна поща“ (E-mail).

Инсталиране на собствен цифров сертификат

1. При получаване на цифровия сертификат се изпълнява функцията Tools от менюто Accounts на MS Outlook Express.
2. Избира се страница Mail и се щраква с мишката върху бутоните Properties и Security.
3. Избира се параметърът Use a digital ID…, когато ще се изпращат съобщения от: name@mail-address.
4. Щраква се с мишката върху бутон Digital ID и се избира сертификатът, който ще се използва.



Изпращане на защитена електронна поща с Microsoft Internet Explorer

За да се изпрати защитена електронна поща, трябва да се използва приложението Microsoft Internet Explorer с неговия пакет за електронна поща Outlook Express.

1. Взема се цифров сертификат от уебсайта на ДУУ – например от GlobalSign Bulgaria: http://www.bia-bg.com/globalsign.bg/certificate.htm.

2. Цифровият сертификат се използва за цифрово подписване и/или криптиране (кодиране) на изпращаната електронна поща.

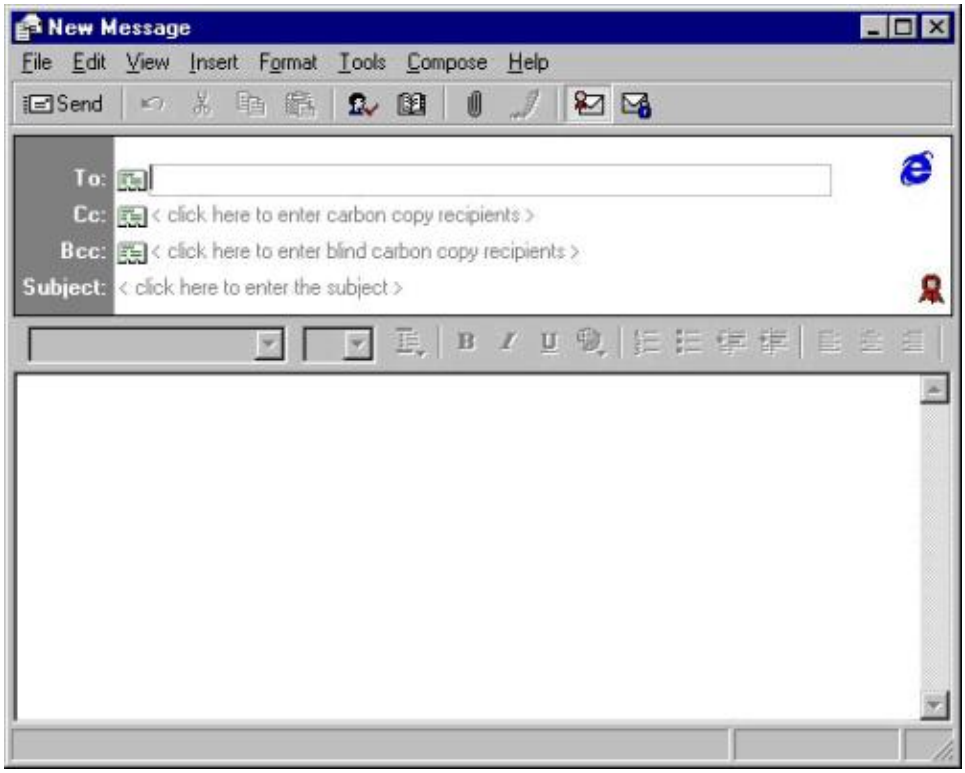
Цифрово подписване на съобщенията по електронната поща с Outlook Express

1. Съобщението, предавано по електронна поща, се подписва с цифровия сертификат. Цифровият подпис улеснява получателя на съобщението да се увери, че действително подателят е изпратил съобщението и че то не е било променено по пътя си.

В този случай цифровият подпис се показва като приложение.

Иконата за *подписан* показва, че полученото съобщение е подписано. Когато се подписва съобщението, иконата се появява в долния десен ъгъл на адреса.

Програмата за електронна поща автоматично проверява (верифицира) цифровия подпис.



Може да се подписват съобщенията всеки път или да се конфигурират опциите за сигурност по такъв начин, че съобщенията да се подписват автоматично.

Подписване на индивидуални съобщения

За да се подпише изходящо съобщение, се щраква два пъти с мишката върху иконата за цифрово подписано съобщение – The digitally sign message (плик с червен етикет), което се намира в прозореца на съобщението.

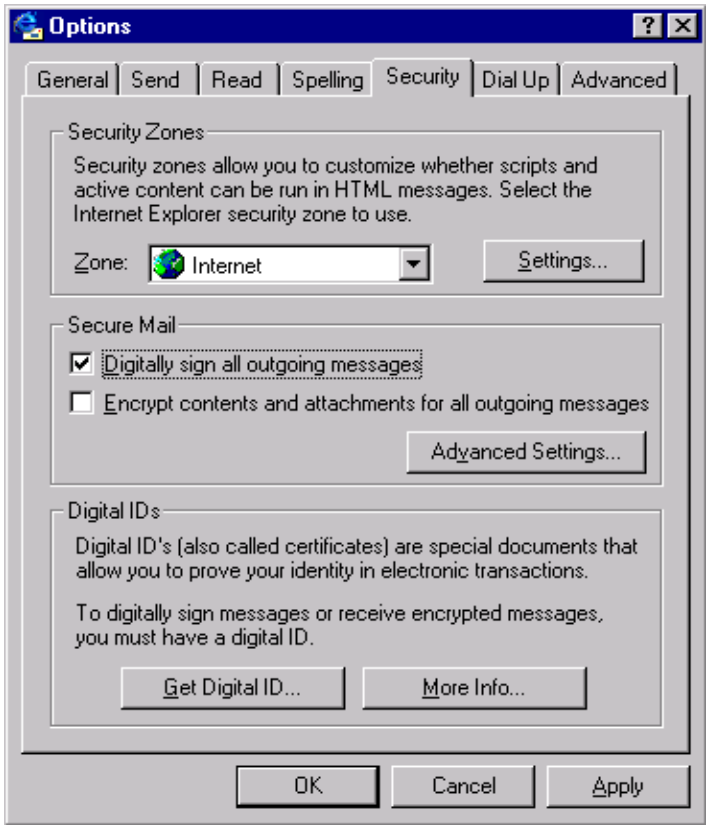
В долния десен ъгъл на адреса се визуализира иконата с подписа.

Ако отново се щракне два пъти с мишката върху цифрово подписано съобщение – Digitally sign message, цифровият подпис ще изчезне.

Автоматично подписване на изходящо съобщение

За да се конфигурират опциите на електронната поща:

1. В среда на Outlook Express се изпълнява функцията Options от менюто Tools.
2. Щраква се с мишката върху страницата Security.
3. Активира се параметърът за цифрово подписване на всички изходящи съобщения – Digitally sign all outgoing messages.



Криптиране (подготвяне) на съобщенията в е-поща с MS Outlook Express

Втората стъпка за защита на съобщенията в електронна поща е да се криптират (кодират). Тъй като съобщението от електронна поща лесно може да се прихване и прочете от други хора, това може да се избегне, като то се кодира, така че само получателят на съобщението да може да го прочете. Кодирането с Outlook Express се извършва аналогично на подписването.

За да се кодира съобщение, трябва да е налице копие от цифровия сертификат на получателя. Това става, като се получи подписано съобщение и се запази сертификатът на подателя (изпратил съобщението) в адресната книга. Възможно е и да се открие този сертификат в он-лайн указателя на сертифициращa организация (ДУУ).

Кодираната икона, която се появява в долния десен ъгъл на изписания адрес, посочва, че съобщението е било кодирано.

Когато се получи кодирано съобщение, Outlook Express автоматично декодира съобщението и показва иконата „кодиран“.

Може да се кодират съобщенията всеки път ръчно или да се конфигурират опциите за сигурност така, че съобщенията да се кодират автоматично, щом цифровият сертификат на получателя да присъства в адресната книга.

Криптиране (кодиране) на отделни съобщения

За да се кодира изходящо съобщение, се щраква два пъти с мишката върху Encrypt message в прозореца на съобщението.

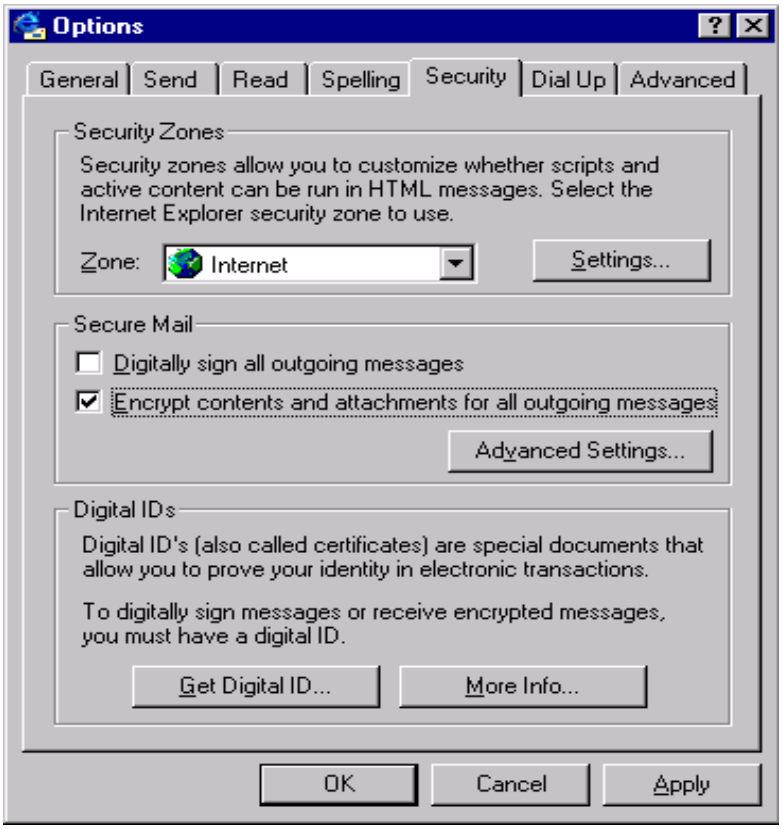
Визуализира се иконата „кодиран“ в долния десен ъгъл на адреса, което показва, че съобщението е кодирано.

Ако се щракне два пъти с мишката върху Encrypt message, кодировката изчезва.

Автоматично криптиране (кодиране) на всички изходящи съобщения

За да се конфигурират опциите за електронна поща, така че изходящите съобщения автоматично да се кодират, когато цифровият сертификат на получателя (адресанта) е включен в адресната книга:

1. Активира се приложението Outlook Express.
2. Изпълнява се функцията Options от менюто на Tools.
3. Избира се страница Security.
4. Щраква се с мишката върху параметъра за кодиране на съдържанието и приложенията за всички изходящи съобщения – Encrypt contents and attachments for all outgoing messages.



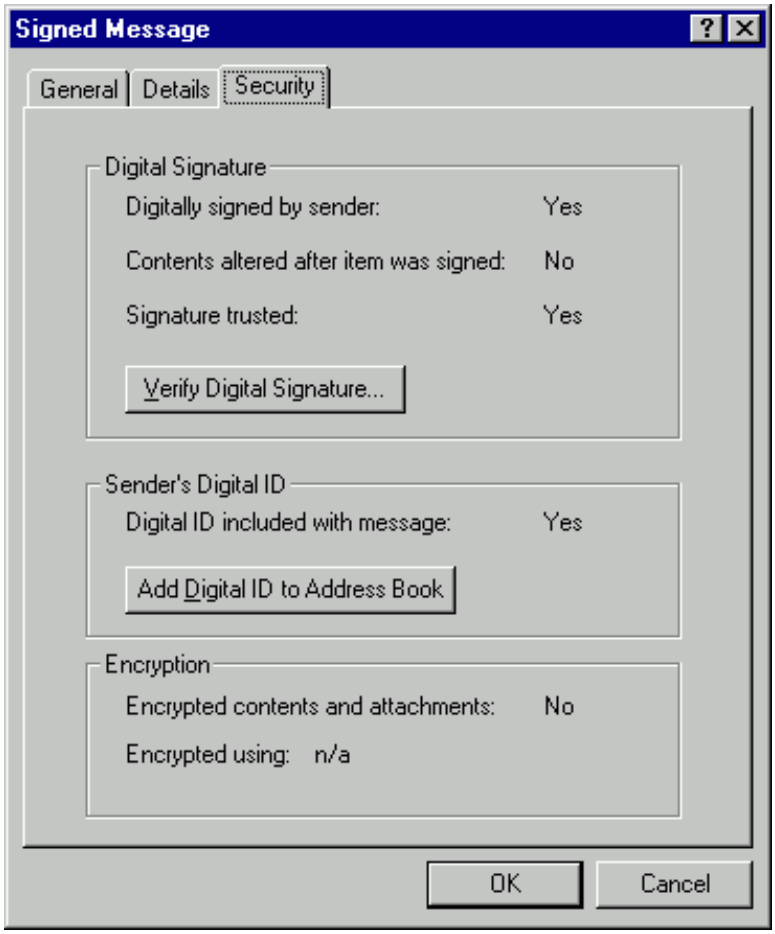
Управление на кореспондентските цифрови сертификати

За да се изпрати криптирано (кодирано) съобщение на определен получател, подателят трябва да разполага в адресната си книга с копие от цифровия сертификат на това лице. Outlook Express дава възможност да се видят, добавят и отстранят цифрови сертификати.

Запазване на цифров сертификат от подписано съобщение

Като се получи кодирано съобщение, получателят може да запази цифровия сертификат на подателя в адресната си книга по следния начин:

1. Отваря се подписаното съобщение.
2. Изпълнява се функцията Properties от менюто File.
3. Избира се страницата Security.
4. Щраква се с мишката върху бутона Add Digital ID to Address Book.

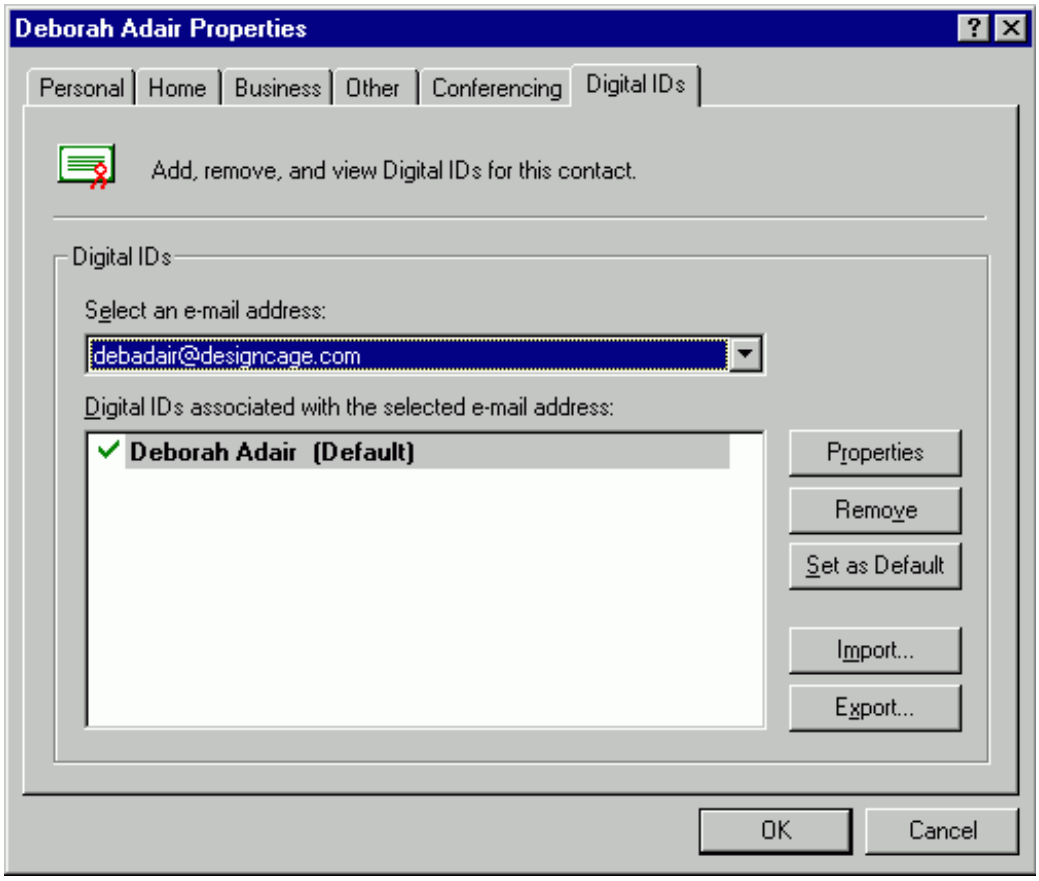


Импортиране на зареден (downloaded) цифров сертификат

Може да се търси цифров сертификат и в база данни он-лайн, да се зареди и да се добави в адресната книга, така че да може да се изпращат кодирани съобщения до това лице.

За импорт на заредения цифров сертификат в адресната книга:

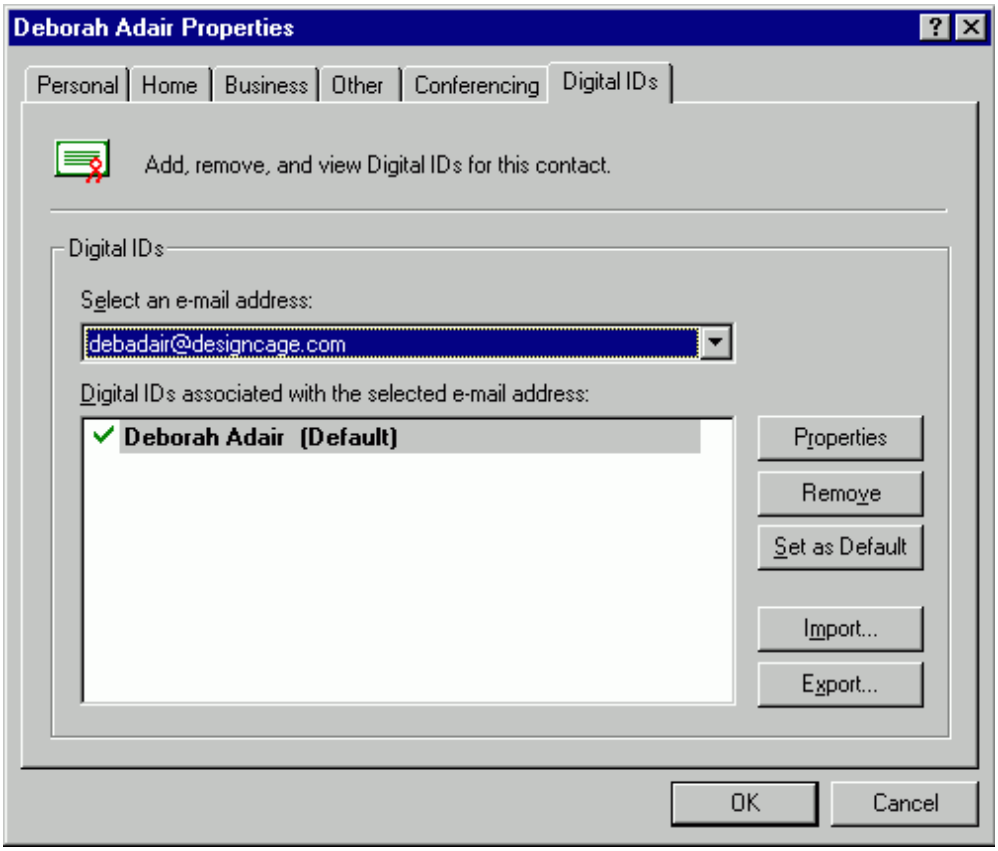
1. Създава се в Outlook Express нов адрес или се отваря вече съществуващ адрес.
2. Избира се страницата Digital Ids.
3. Щраква се на бутон Import.
4. Избира се зареденият файл с цифровия сертификат и след това се щраква на бутон open.



Управление на цифровите сертификати в адресната книга
За да се види един от цифровите сертификати:
1. Отваря се в адресната книга адресният запис за съответното лице.
2. Избира се страницата Digital Ids.
3. Избира се съответният сертификат.
4. Щраква се на бутон Properties.

За да се изтрие (отстрани) цифров сертификат от адресната книга
1. Отваря се адресът на лицето, чийто сертификат ще се изтрива.
2. Избира се страницата Digital Ids.
3. Избира се сертификатът, който ще се изтрива.
4. Щраква се с мишката върху бутон Remove.

След като се отстрани цифров сертификат, повече не може да се изпращат кодирани съобщения на това лице.



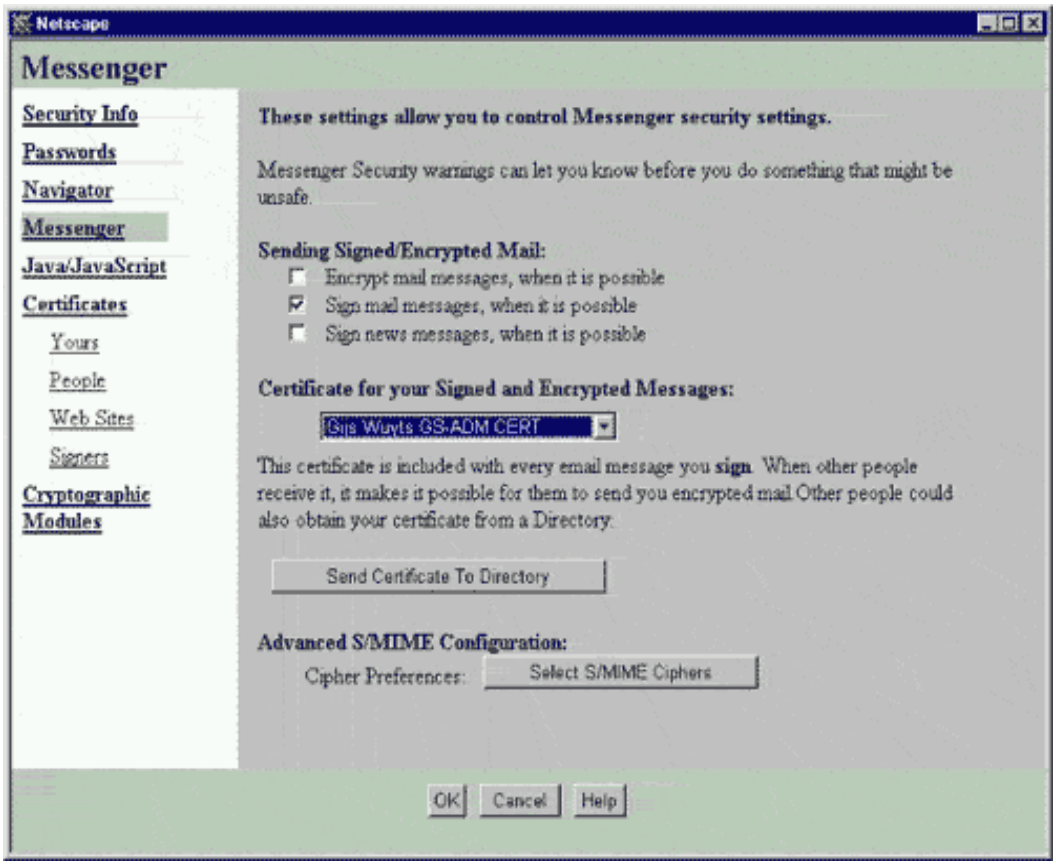
3.3. Netscape Navigator

Програмата Netscape Navigator е браузър за достъп до услугата WWW на фирмата Netscape Communicator.

Инсталиране на цифров сертификат

След получаване на цифровия сертификат от ДУУ се изпълнява функцията Security от менюто Toolbar и се щраква с мишката на „Messenger“. След това се избира „сертификат“.

В този „Security Advisor's Messenger Security Settings“ лесно може да се използва всичко, което е необходимо за цифровите сертификати.



За да се изпрати защитена електронна поща с Netscape Messenger:

1. Трябва да се използва версия на Netscape Navigator с пакета за Messenger електронна поща.

2. Получава се цифров сертификат от уебсайта на ДУУ – например от GlobalSign: http://www.secure.globalsign.net/bg/find/index.cfm [4].

3. Той се използва, за да се подпише и/или криптира (кодира) цифрово електронната поща;

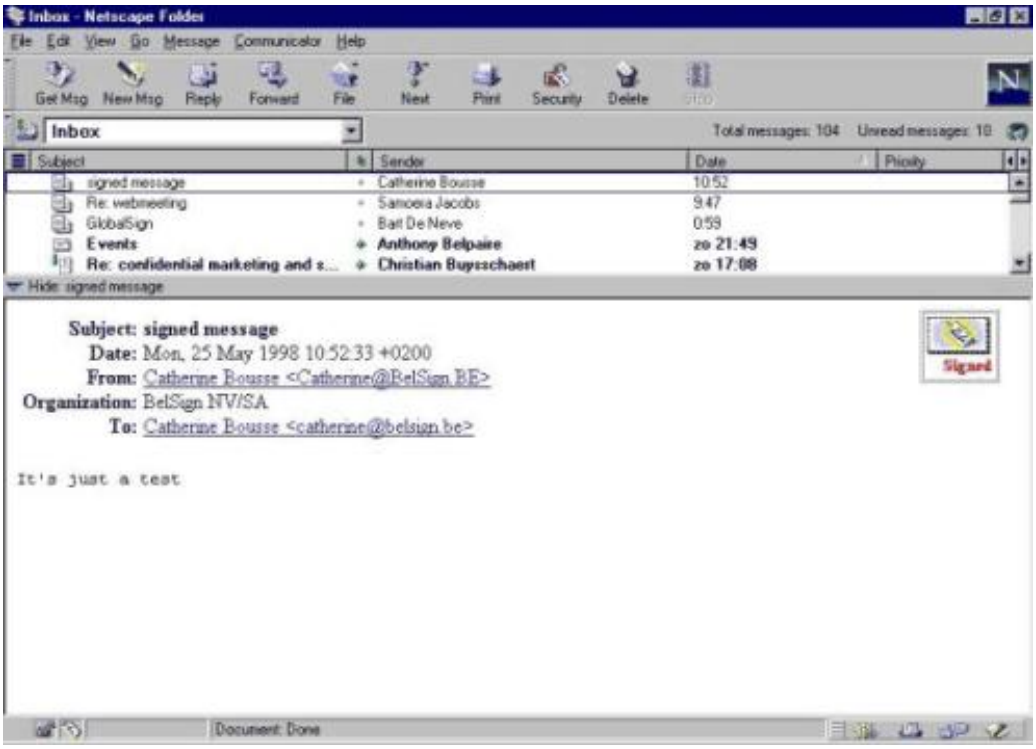
Цифрово подписване на електронната поща с Netscape Messenger

Първата стъпка, с която се осигурява защитата на съобщенията по електронната поща, е те да се подпишат с цифровия сертификат на подателя.

Иконата *подписан (signed)* показва, че съобщението е подписано.

Програмата за електронна поща потвърждава цифровия подпис автоматично.

Netscape Messenger също така автоматично съхранява цифровия сертификат на подателя (изпращача), което прави възможно кодирането на бъдещи съобщения, изпращани до това лице.

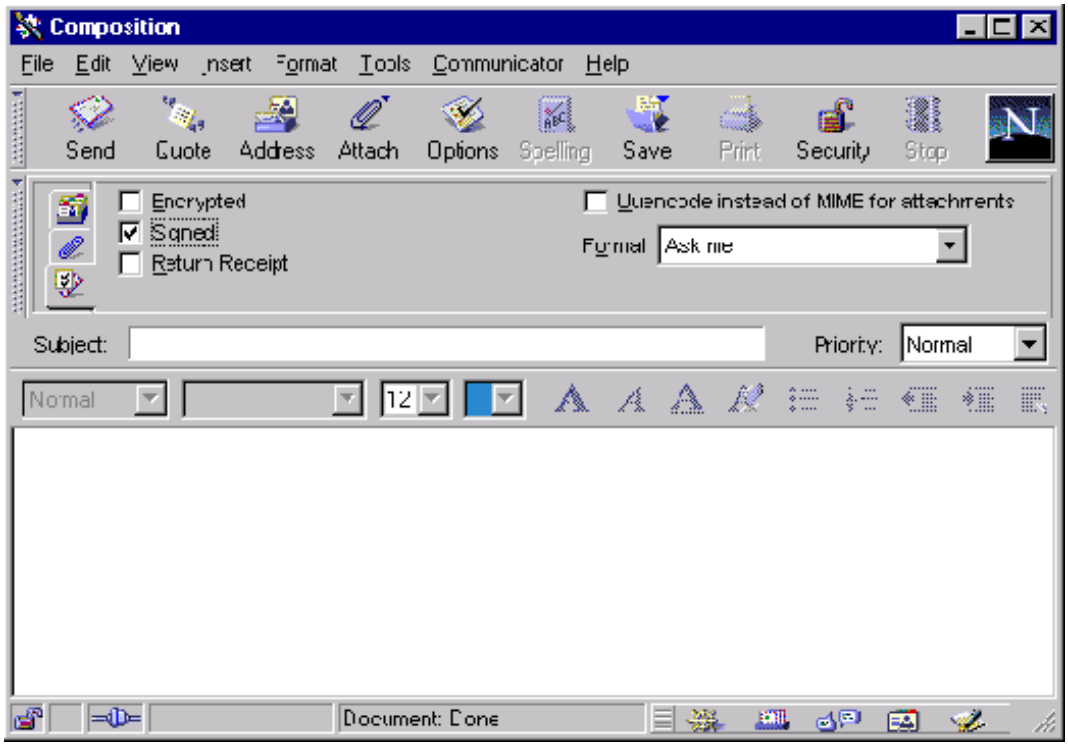


Може да се подписват съобщенията всеки път ръчно или да се конфигурира защитната опция така, че съобщенията да се подписват автоматично.

Подписване на отделни съобщения

За да се подпише изходящо съобщение:

1. Щраква се с мишката върху опцията за изпращане на съобщения Message sending options в прозореца за съобщения.
2. Активира се параметърът Signed.



Автоматично подписване на всяко изходящо съобщение

За да се конфигурира настройката (Messenger Security Settings) за автоматично подписване на изходящите съобщения:

1. Щраква се с мишката върху иконата security от лентата с бутоните или се активира функцията Security info от менюто Communicator.
2. Щраква се с мишката на бутон messenger, за да се визуализира Messenger Security Settings.
3. За автоматичното подписване на съобщенията се активира параметърът Sign mail messages, when it is possible.

Криптиране (кодиране) и обработване на съобщения по електронната поща с Messenger

Втората стъпка за осигуряване защита на съобщенията по електронната поща е тяхното кодиране.

За да се кодира съобщение, е необходимо копие от цифровия сертификат на получателя. Когато се получи подписано съобщение, Netscape Navigator автоматично ще запази цифровия сертификат на подателя (изпращача).

Може да се открие също така даден цифров сертификат в он-лайн указателя на сертифициращата организация (ДУУ).

Когато се получи кодирано съобщение, Messenger автоматично ще го декодира. Визуализира се една икона, която посочва, че съобщението е било кодирано при изпращането или е подписано и кодирано.

Кодирано и подписано

Само кодирано

Може да се кодират съобщенията всеки път ръчно или да се конфигурират параметрите за сигурност за автоматично кодиране на всички съобщения по електронната поща, чиито цифрови сертификати се съхраняват в адресната книга.

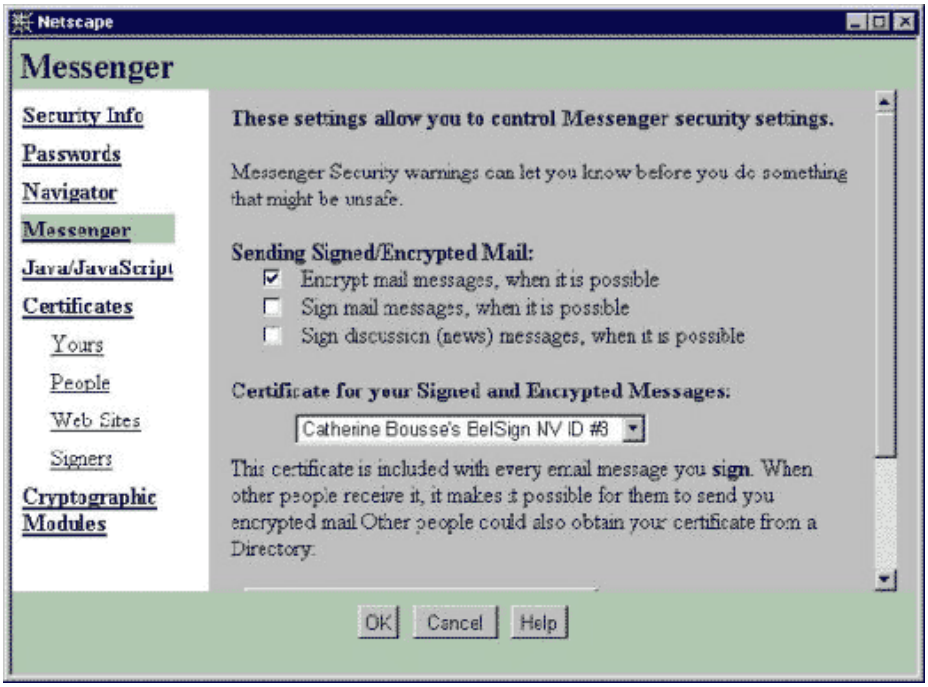
Кодиране на отделни съобщения:

1. Щраква се с мишката върху опцията за изпращане на съобщения Message sending options в прозореца на съобщенията.
2. Щраква се на иконата кодирано Encrypted.

Автоматично кодиране на изходящи съобщения

За да се конфигурира Messenger Security Settings за автоматично кодиране на изходящи съобщения до получателите, чиито цифрови сертификати се съхраняват в адресната книга:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security от лентата с бутоните или като се активира функцията security info от менюто Communicator;
2. Щраква се с мишката на бутон Communicator, за да се визуализира Messenger Security Settings.
3. Активира се параметърът – кодирайте пощенски съобщения, когато е възможно (encrypt mail messages, when it is possible).



Управление на цифровите сертификати на кореспондентите

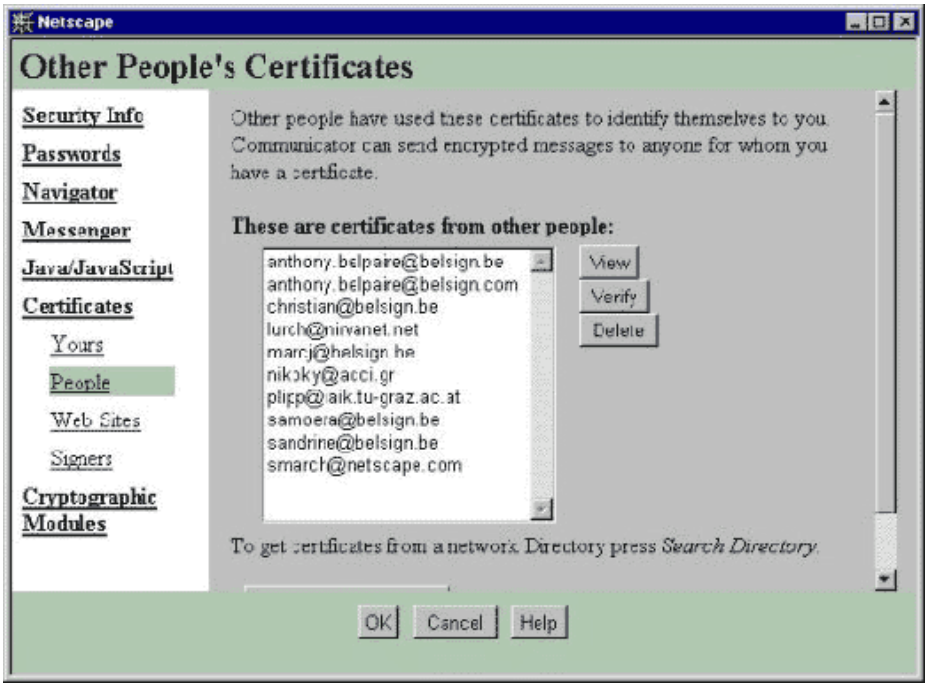
За да се изпрати кодирано съобщение на даден получател, е необходимо копие от цифровия му сертификат в адресната книга. Когато се получи подписано съобщение, Navigator автоматично съхранява цифровия сертификат на подателя (изпращача). Необходимо е така също да се открие даден цифров сертификат в он-лайн указателя, като по този начин може да се изпрати кодирано съобщение до получател, без първоначално да е получавано подписано съобщение от него.

Разглеждане на цифровите сертификати по Списъка за контакти

Когато се получи или зареди даден цифров сертификат, Navigator го съхранява в своя списък на сертификатите. Може да се изпраща кодирана електронна поща до всеки един получател от този списък.

За да се изведе списъкът на хората, чиито цифрови сертификати се съхраняват, се извършват следните стъпки:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security на лентата с бутоните или като се активира функцията Security Info от менюто Communicator.
2. Щраква се с мишката върху параметъра People в категорията Сертификати.



Управление на цифровите сертификати в списъка за контакти

За да се изведе един от цифровите сертификати за контакт:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security на лентата с бутоните или като се активира функцията Security Info от менюто Communicator.
2. Щраква се с мишката върху параметъра People в категорията Сертификати.
3. Избира се лицето, чийто цифров сертификат ще се разглежда.
4. Щраква се с мишката върху бутона View.

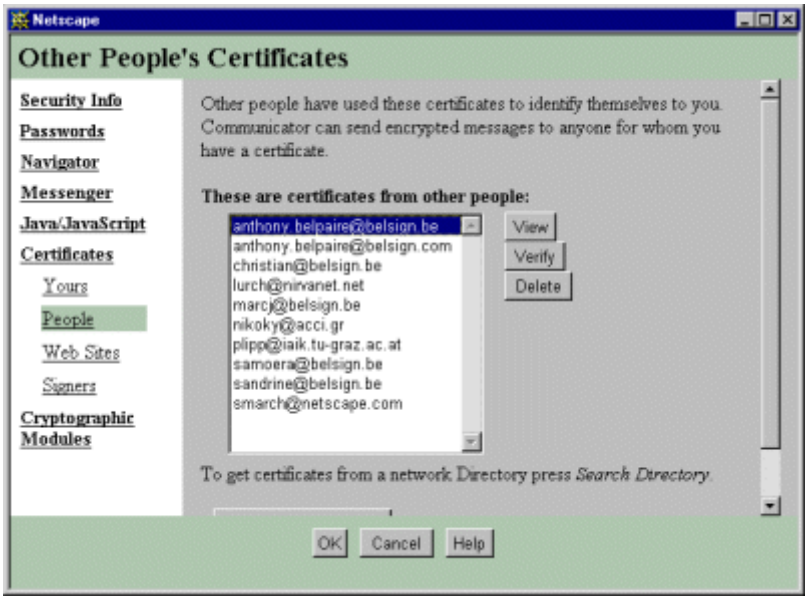
За да се провери (верифицира) един от цифровите сертификати за контакт:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security на лентата с бутоните или като се активира функцията Security Info от менюто Communicator.
2. Щраква се с мишката върху параметъра People в категорията Сертификати.
3. Избира се лицето, чийто цифров сертификат ще се верифицира.
4. Щраква се с мишката върху бутон Verify. Navigator проверява дали цифровият сертификат е бил издаден от призната сертифицираща организация, както и датата на изтичане на цифровия сертификат.

За да се изтрие цифров сертификат от списъка за контакти:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security от лентата с бутоните или като се активира функцията Security Info от менюто Communicator.

2. Щраква се с мишката върху параметъра People в категорията Сертификати.
3. Избира се лицето, чийто цифров сертификат ще се изтрива.
4. Щраква се с мишката върху бутон Delete. След като се изтрие даден цифров сертификат, повече не може да се изпраща кодирана електронна поща до това лице.

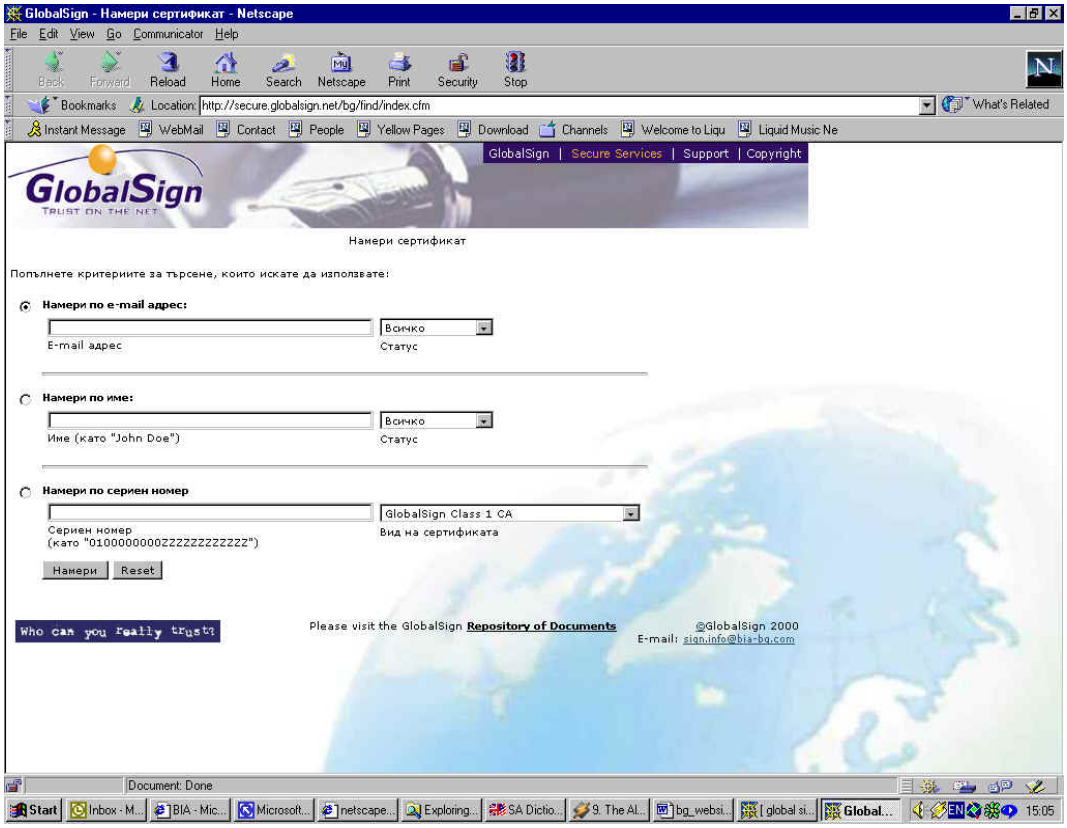


Откриване на даден цифров сертификат

Ако не е получавано подписано съобщение от дадено лице, на което се налага да се изпрати кодирано съобщение, може да се провери дали това лице фигурира в онлайн указателя. Ако фигурира, може да се зареди цифровият му сертификат оттам. За да се открие даден цифров сертификат, има две възможности:

А. Лицето, на което ще се изпраща кодирано съобщение, притежава GlobalSign цифров сертификат:

Влиза се в Web сайта на GlobalSign:
1. http://www.secure.globalsign.net/bg/find/index.cfm.
2. Въвежда се електронният адрес и/или името на лицето.
3. Щраква се с мишката върху бутон Find, за да започне търсенето.
4. Щраква се с мишката върху цифровия сертификат, който е открит.
5. Задава се къде ще се свали (Download) и запази цифровият сертификат.



Б. Лицето, на което ще се изпраща кодирано съобщение, има друг цифров сертификат:

1. Отваря се прозорецът Netscape Communicator Security Advisor, като се щракне с мишката върху иконата Security от лентата с бутоните или като се активира функцията Security Info от менюто Communicator.
2. Щраква се с мишката върху параметъра People в категорията Сертификати.
3. Щраква се с мишката върху Search Directory.
4. Избира се от падащото меню папката, в която ще се търси.

4. ЗАКЛЮЧЕНИЕ

Проблемът, свързан с Интернет защитата на СИ, споделена като информационен ресурс и достъпвана отдалечено по мрежата или предавана по канали за връзка, е актуален поради все по-масовото използване на услугите на Интернет като глобална мрежа от:

- фирмите, при обработката на СИ във фирмени компютърни мрежи, базирани на Интернет;
- държавната администрация на Република България като потребител на част от тази счетоводна информация.

Разгледаните методи за Интернет защита на СИ са достъпен и ефективен начин на реализирането ѝ, тъй като основно са базирани на средства на системното и приложно програмно осигуряване, т.е реализирани са чрез програмните и криптографските методи за защита на СИ. Реализирането на техническите методи за защита на СИ изисква допълнителни инвестиции, но комбинирането им с останалите методи за защита води до повишаване на степента на отказоустойчивостта на информационната система. Разгледаните програми за електронно подписване и криптиране на СИ са масово разпространени в нашата страна и са с доказани качества.

Терминологичен речник:

1. Internet Services Provider – доставчик на Интернет услуги.
2. Importing – прехвърляне на информация между приложенията.
3. Internet Connection Firewall – защитна стена.
4. Download – „сваляне“ на информация от Интернет.

Литература

1. Internet site http://www.microsoft.com/windows2000/techinfo/ planning/security/pki.asp.
2. Internet site http://www.microsoft.com/windows2000/techinfo/ proddoc/serverhelp.asp.
3. Internet site http://www.bia-bg.com/globalsign.bg/certificate.htm.
4. Internet site http://secure.globalsign.net/bg/find/index.sfm.
5. MCSE Training Kit Microsoft Windows 2000 Server, том 1 и 2, Софт Прес, София, 2000 г.
6. Upgrading to Windows 2000, Microsoft Press, 2000 г.
7. MCSE Microsoft Windows XP Professional, том 1 и 2, Софт Прес, София, 2002 г.
8. Закон за счетоводство, ДВ, бр. 98 от 16 ноември 2001 г., в сила от 1 януари 2002 г.
9. Закон за електронния документ и електронния подпис, ДВ, бр. 34 от 6 април 2001 г.
10. Honeycutt, J., Introducing Microsoft Windows Server 2003, Soft Press, Sofia, 2003.

ИНТЕРНЕТ (WEB) ЗАЩИТА НА СЧЕТОВОДНАТА ИНФОРМАЦИЯ

Резюме

Свързването на бизнеса с Интернет (Web) технологиите предоставя много допълнителни предимства, но и определени рискове, свързани с възможността за нерегламентиран отдалечен достъп на споделена счетоводна информация (СИ) и достъп до предаваната СИ по каналите за връзка на фирмените мрежи, базирани на Интернет. Разглежданите методи за Интернет защита на счетоводната информация са:

Програмни методи

Включват:

- пароли за достъп до „споделена“ (Shared) по мрежата СИ. По отношение на паролите за достъп се препоръчва спазването на изискванията на международния стандарт за сигурност С2;
- определяне на права за отдалечен достъп до споделена СИ. Тези права се задават на ниво потребител (главен счетоводител) или група от потребители (счетоводители, касиери, материалноотговорни лица, администратори и т.н.);
- архивиране на СИ в реално време – on-line архивирането е средство за защитата на СИ от разрушаване по технически причини. Осъществява се по Интернет върху диск на сървър за данни;
- on-line актуализиране на антивирусните програми (Live Update). Фирмите, разработили антивирусни програми, предлагат on-line (live update) актуализиране на файловете с вирус дефиниции;
- актуализиране на операционната система (Update). Целта е отстраняване на критични за сигурността на системата „пробойни“;
- защитни стени (Firewall). Те са средство за защита на СИ във фирмената компютърна мрежа, базирана на Интернет от „атаки“ отвън и отвътре;
- виртуални частни мрежи (VPN[1]). Използват се за надеждното свързване на фирмата с нейните поделения, използвайки Интернет с цел обработване и предаване на СИ;
- on-line сканиране на работното място – извършва се с цел тестване на уязвимостта на системата. Microsoft Baseline Security Analyzer (MBSA) е разработен с цел извършване на оценка на степента на защита на един или повече компютри от VPN мрежата, базирани на Windows. MBSA определя дали вградените в тях системи за защита не са остарели и трябва ли да се актуализират.

Криптографски методи

Криптографските методи за защита на СИ се прилагат при предаването ѝ по канали за връзка. Една от технологиите за криптиране на СИ, използвана в Република България, е технологията „Инфраструктура публичен ключ“ (PKI[2]). Чрез технологията се реализират свойствата конфиденциалност, удостоверяване на самоличността на подателя, цялост на СИ и защита от повторение.

Правни методи

Правните методи за Интернет защита на СИ са базирани на съществуващата нормативна база в Република България, включваща:

- Закон за електронния документ и електронния подпис;
- Наказателно-процесуален кодекс (НПК).

Технически методи

Техническите методи за Интернет защита на СИ включват използването на технически средства за ограничаване на достъпа до СИ като:

[1] Virtual Private Network – виртуална частна мрежа.

[2] Public Key Infrastructure – инфраструктура публичен ключ.

- Smart-картите.
- Хардуерно реализирани защитни стени (Hardware Firewall).

INTERNET (WEB) PROTECTION OF ACCOUNTING INFORMATION

Summary

Connection of business to Internet Technologies gives a lot of additional advantages but it leads to some risk. Risk connected with the possibility of unestablishe remote access to shared Accounting Information (AI) and access to the AI send by the connecting channels of company network, based on the Internet.

Programmer Methods

They include the use of:

- Password for access to the shared AI on the network. Concerning the passwords, observance of the International Security Standard C2 requirements is recommended,
- Determination of rights for remote access to the shared AI. These rights are defined on the level of a user (a chief accountant) or a group of users (Accountants, cashiers, material responsible staff, administrators),
- Archiving of the AI in virtual time – on-line archiving is means of the AI protection from destructions caused by technical reasons. It is carried out on the Internet on a server disk of data,

On-live updating of anti-virus programs (Live Update). Companies that have worked out the anti-virus programs, offer on-line (live update) files updating with virus definitions,

- Updating of the operating system (Update). The aim is eliminate the critical punches of the system security,
- Protective walls (Firewall). They are means of the AI protection in the company computer network, based on the Internet attacks from outside and inside,
- Virtual Private Networks (VPN). They are used for dependable connection of the company to its branches using the Internet. The aim is to process and send the AI,
- On-line scan of workplace. It is done on purpose of testing the system security ability. Microsoft Baseline Security Analyzer (MBSA) has been developed on purpose of evaluation of the protection degree of one or more computers from the VPN based on Windows. MSBA determines if the built-in security systems are outdated and had better be updated;

Cryptographic Methods

Cryptographic methods for the AI protection are applied while sending the information by the connecting channels. One of the technologies for the AI cryptography used in the Republic of Bulgaria is Public Key Infrastructure (PKI). Confidentiality, attestation of senders identify, AI completeness and protection from repetition are realized by this technology.

Legal Methods

Legal methods for the AI Internet Protection are based on the existing normative base in the Republic of Bulgaria, including:

- Electronic Documents and Signatures Protective Law,
- Criminal Procedure Code;

Technical Methods

Technical methods for the AI Internet Protection include technical methods for access restriction to the AI as:

- Smart cards,
- Hardware realized protective walls (Hardware Firewall).