П Р Е З Е Н Т А Ц И Я

По Безопасност и Защита

Изготвил: Атанасис Авгеринудис
Ф.№ 7210, гр.№ 30

Тема:

Криптирането нашият личен пазач!

Криптиране и декриптиране

- Криптирането се използва, за да се осигури скриването на информацията от тези, за които тя не е предзначена.
- Процесът на преобразуването на оригиналния текст в скрит вариант се нарича криптиране.
- Процесът на преобразуването на кодирания текст в неговият оригинал се нарича декриптиране.

Цели на информационната защита чрез криптиране?

- Конфиденциалност
- Цялост на данните
- Идентификация на изпращача
- Доказване на авторството

Сигурност на личната Ви информация

Access Manager

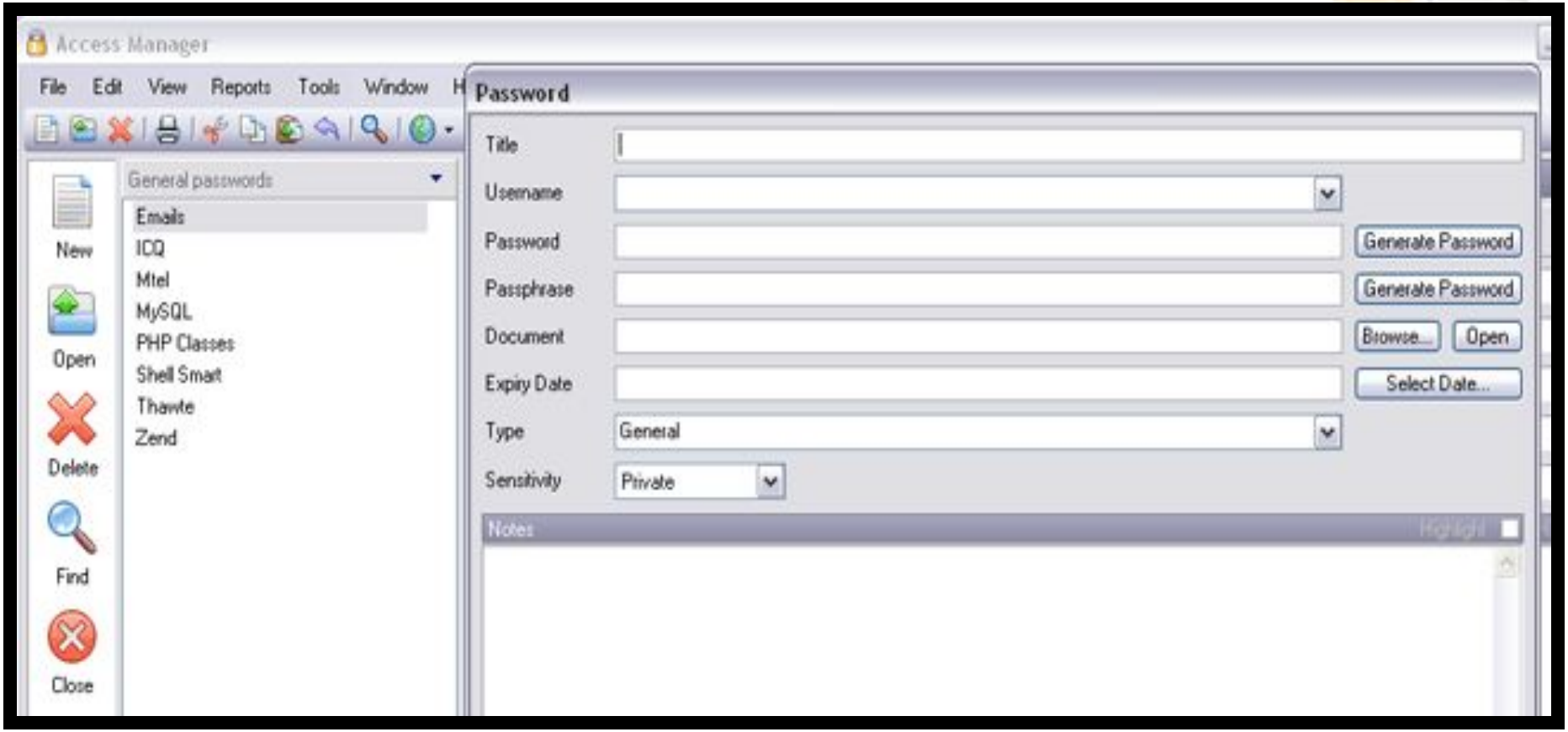
Access Manager е софтуерно приложение за Windows, чрез което можете лесно и сигурно да съхранявате ваша лична информация като пароли и т.н.. на вашия компютър и само вие да имате достъп до тях. Приложението има високо ниво на сигурност, информацията се съхранява криптирана, а същевременно е ***напълно безплатно*** и можете да си го изтеглите от Internet и инсталирате от адрес: *http://www.accessmanager.co.uk/*

Сигурност на личната Ви информация

При нуждата от достъп до вашите защитени данни стартирате Access Manager и той изисква от вас да въведете вашата парола за достъп.

Лица, които не знаят паролата не се допускат до информацията!

Сигурност на личната Ви информация



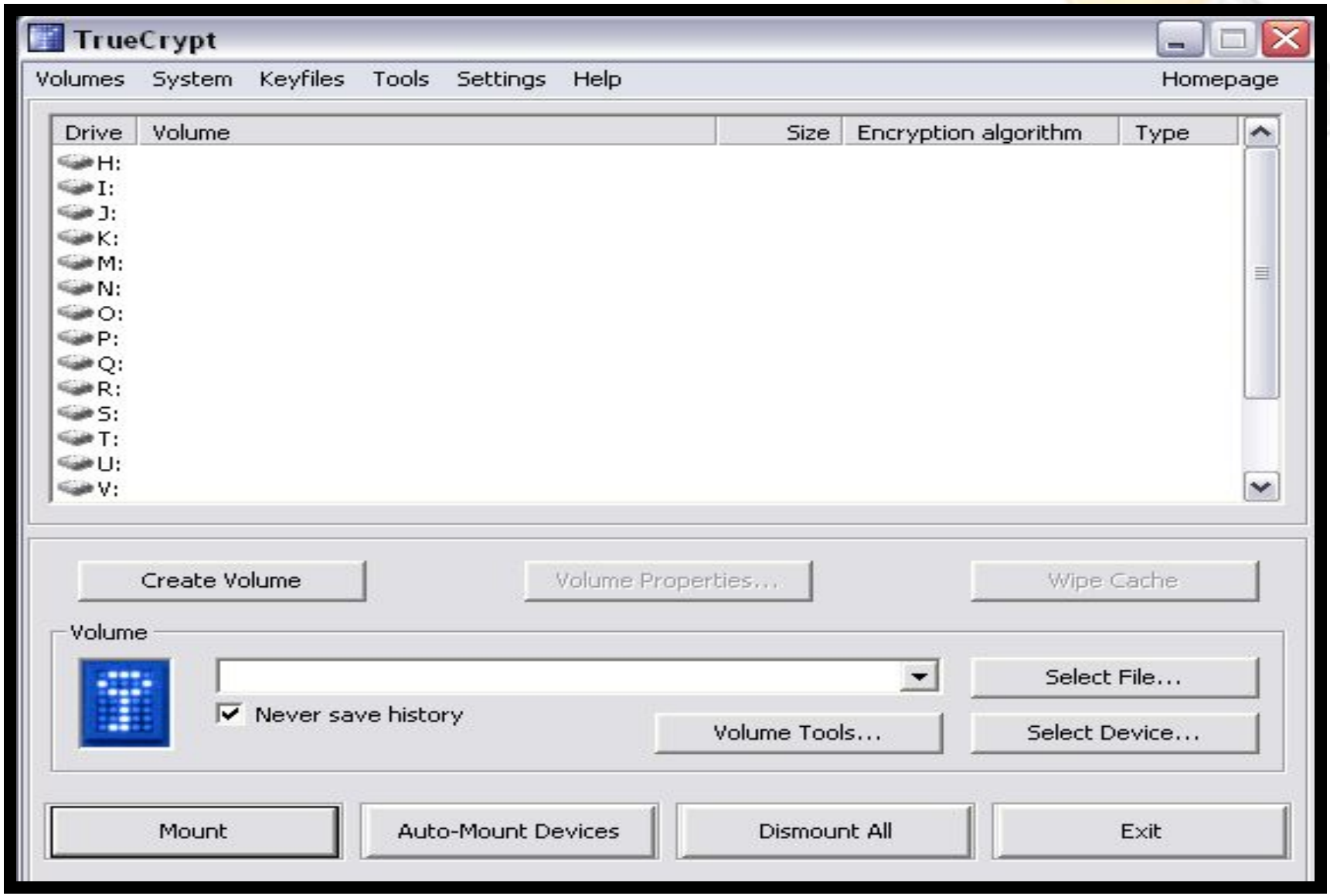
Сигурност на личната Ви информация

True Crypt

True Crypt е софтуерно приложение за Windows Vista/XP, Mac OS X, и Linux, което ви дава възможност да криптирате файлове, папки или цели дискови устройства на вашия компютър. По този начин важни за вас файлове се съхраняват криптирани и никой друг освен вас няма достъп до тях.

*Приложението е **напълно безплатно** и можете да си го свалите и инсталирате на вашия компютър от Internet адрес:*
http://www.truecrypt.org/

Сигурност на личната Ви информация

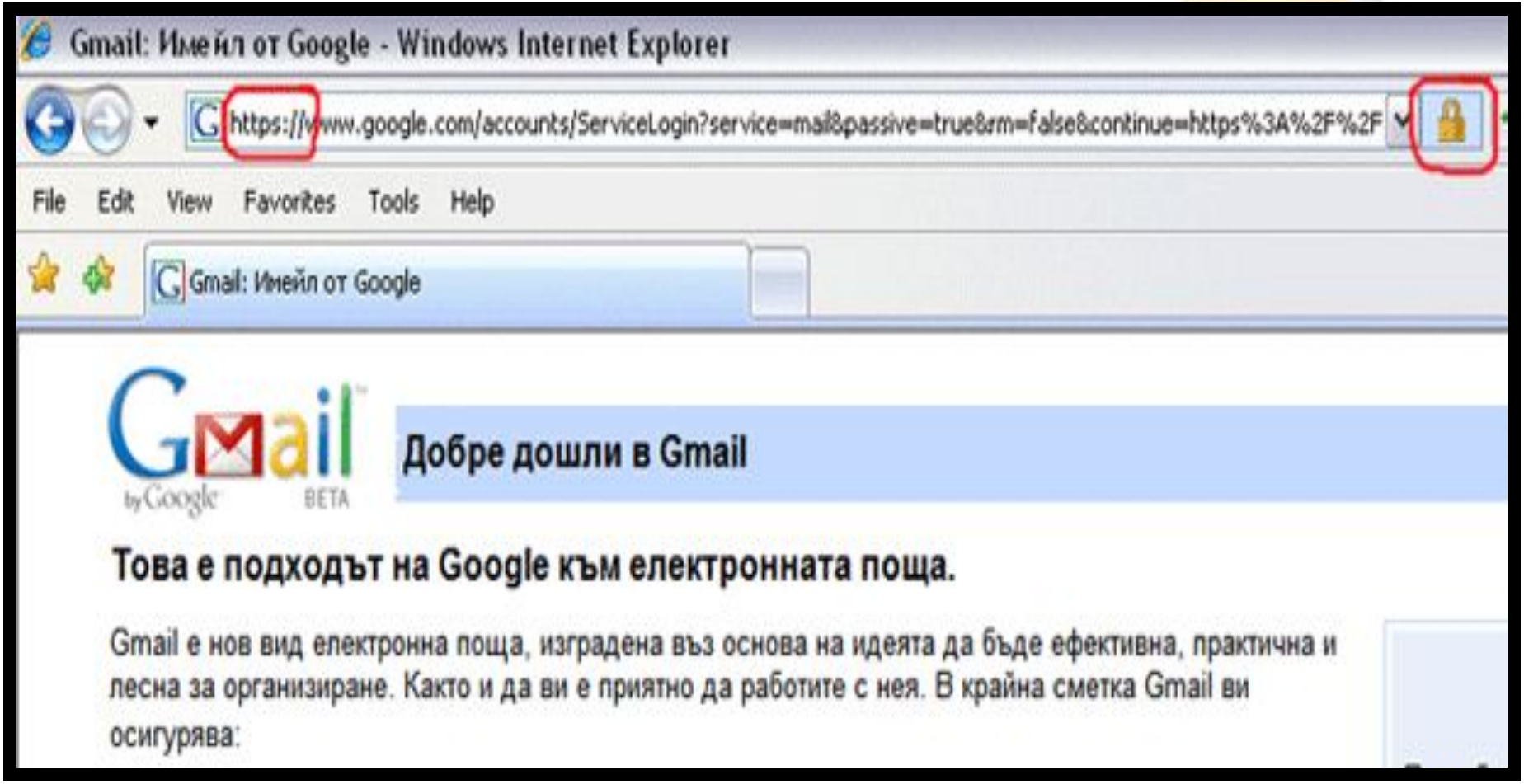


Сигурност при Уеб Сърфиране

В случай, че ползвате електронно банкиране или всякакви други уеб услуги, които изискват високо ниво на сигурност и конфиденциалност, обърнете внимание дали връзката се осъществява през криптирания ***SSL уеб протокол***.

В случай, че ползвате уеб базирани електронни пощенски услуги, изберете такъв email провайдер, който предоставя криптиран достъп до пощата ви през ***SSL уеб протокола***.

Сигурност при Уеб Сърфиране



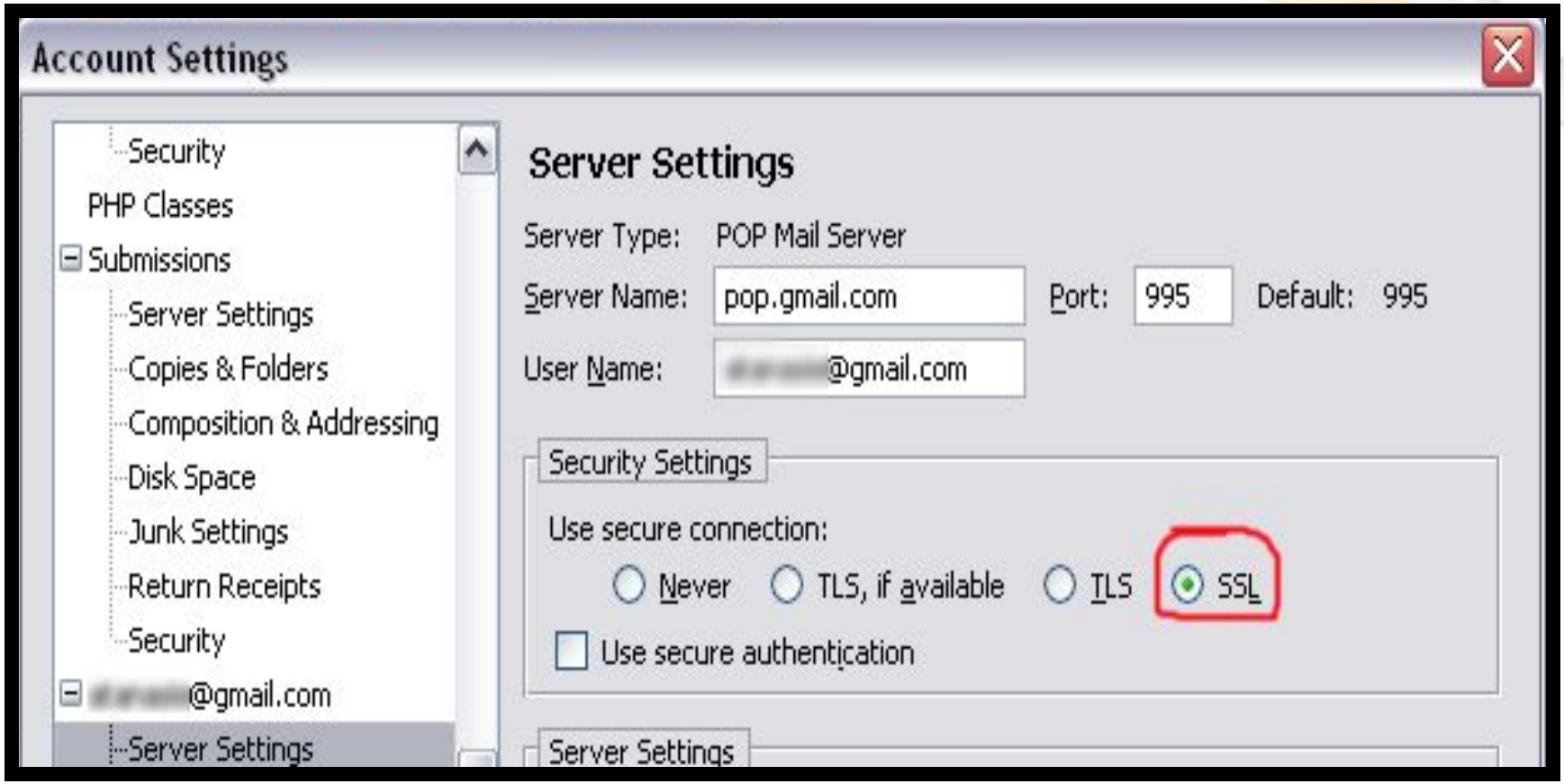
Обърнете вниманите на индикаторите, които показват, че ползвате криптирана връзка с уеб сайта - оградени са с червено.

Сигурност при Email Услугите

В случай, че ползвате електронна поща чрез email клиент инсталиран на вашият компютър или така наречения *POP3 Access*, изберете такъв email провайдер, които предоставя криптиран достъп до *POP3* и до *Outgoing Mailserver* за изпращане на писма.

В следващите две снимките можете да видите примерните настройки за ползване на *Gmail* през email клиента *Mozilla Thunderbird*.

Сигурност при Email Услугите



*Обърнете внимание на избора за използване на **SSL** криптиране връзка за комуникация с POP3.*

Сигурност при Email Услугите

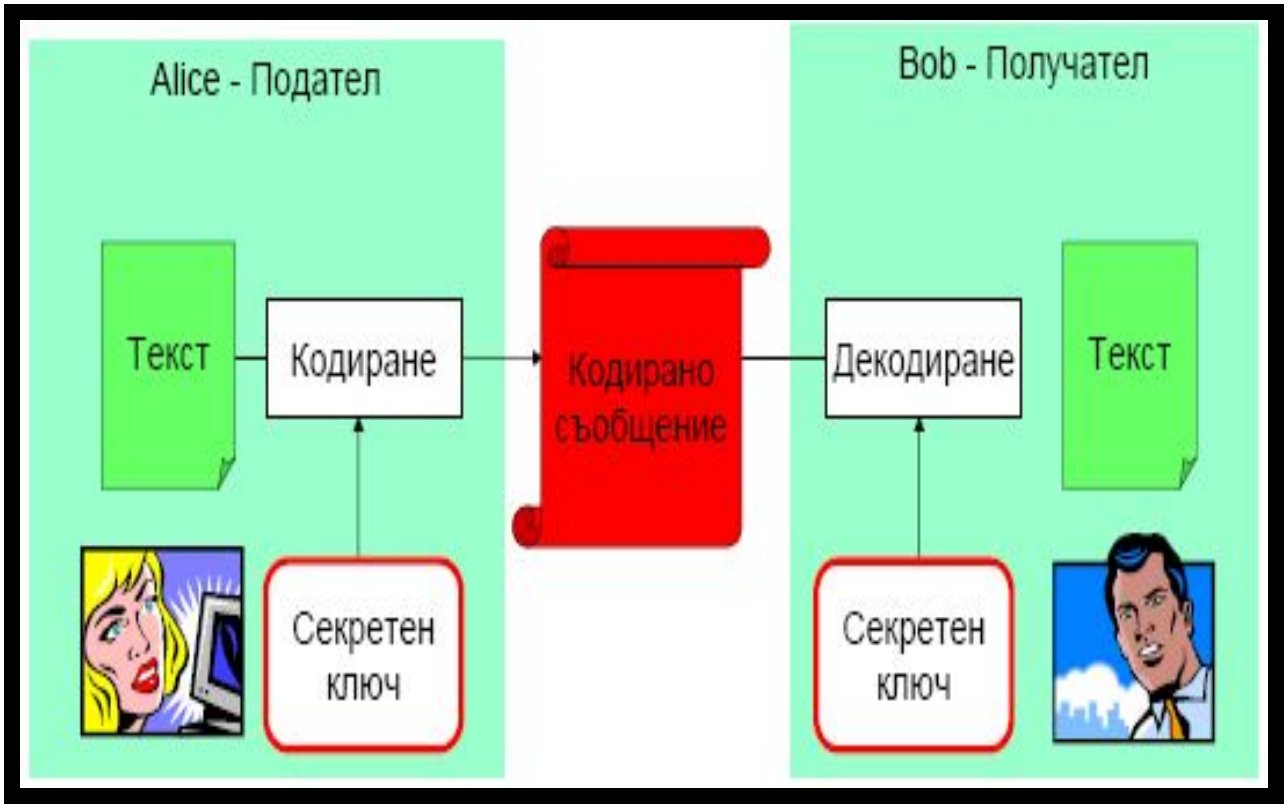
Обърнете внимание на избора за използване на **TLS** или **SSL** криптирана връзка за комуникация с SMTP Outgoing Mail Server.

Криптиране в Електронните Комуникации

В днешно време въпросът за сигурността и конфиденциалността на данните в електронните комуникации е изключително актуален. Разработени са различните методи за осигуряване на тази сигурност и за постигане на целите на информационната защита.

В този раздел ще се запознаем с различните методи за защита, както и нивото на сигурност, което те предоставят.

Криптиране със Симетричен Ключ



Конфиденциалност на данните - **ДА**

Цялост на данните - **ДА**

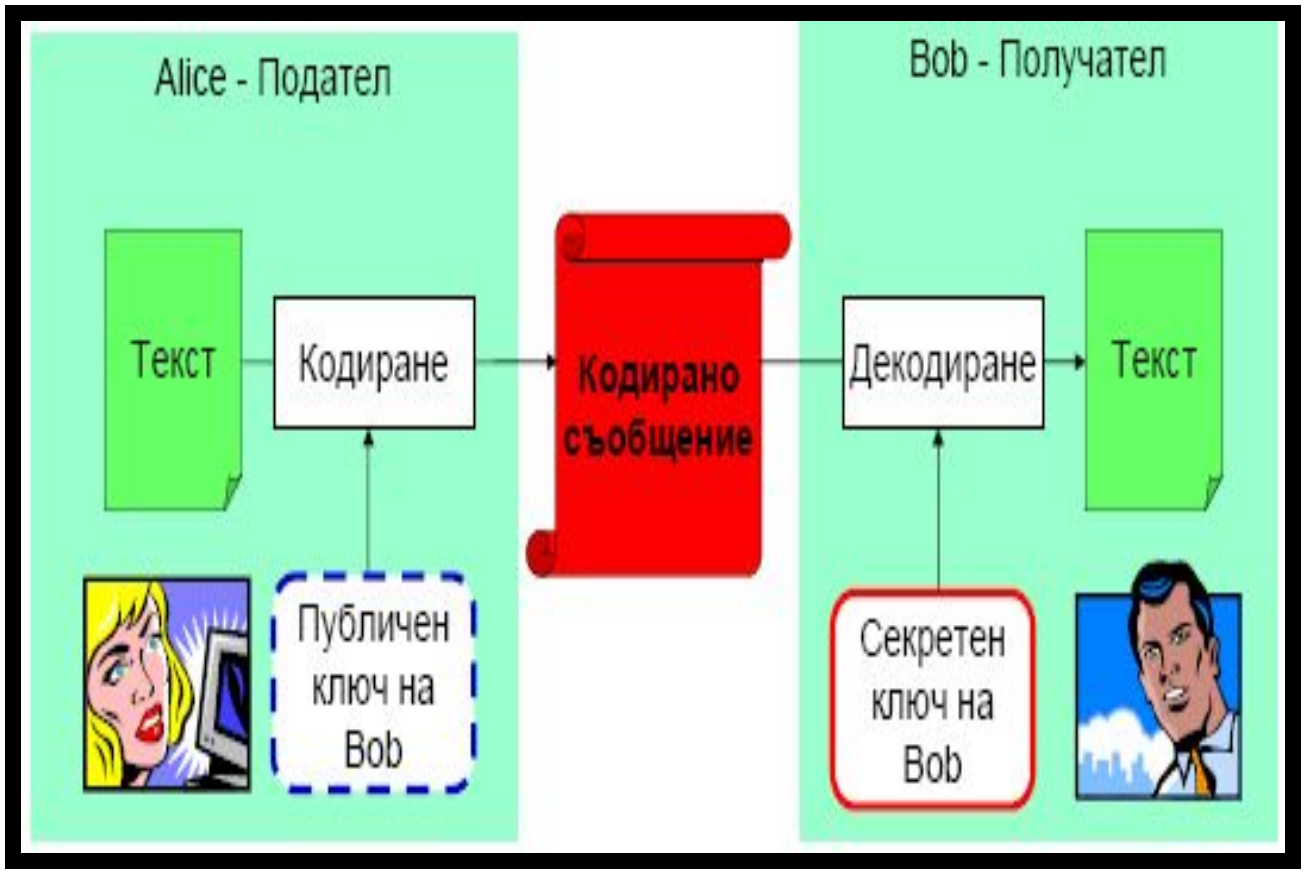
Идентификация на изпращача - **ДА**

Доказване на авторството – **НЕ**

Проблем е надеждното физическо разпространение на секретните ключове!

Криптирането и декриптирането се извършва с един и същ секретен ключ.

Криптиране със Публичен Ключ



Конфиденциалност на данните – **ДА**

Цялост на данните - **НЕ**

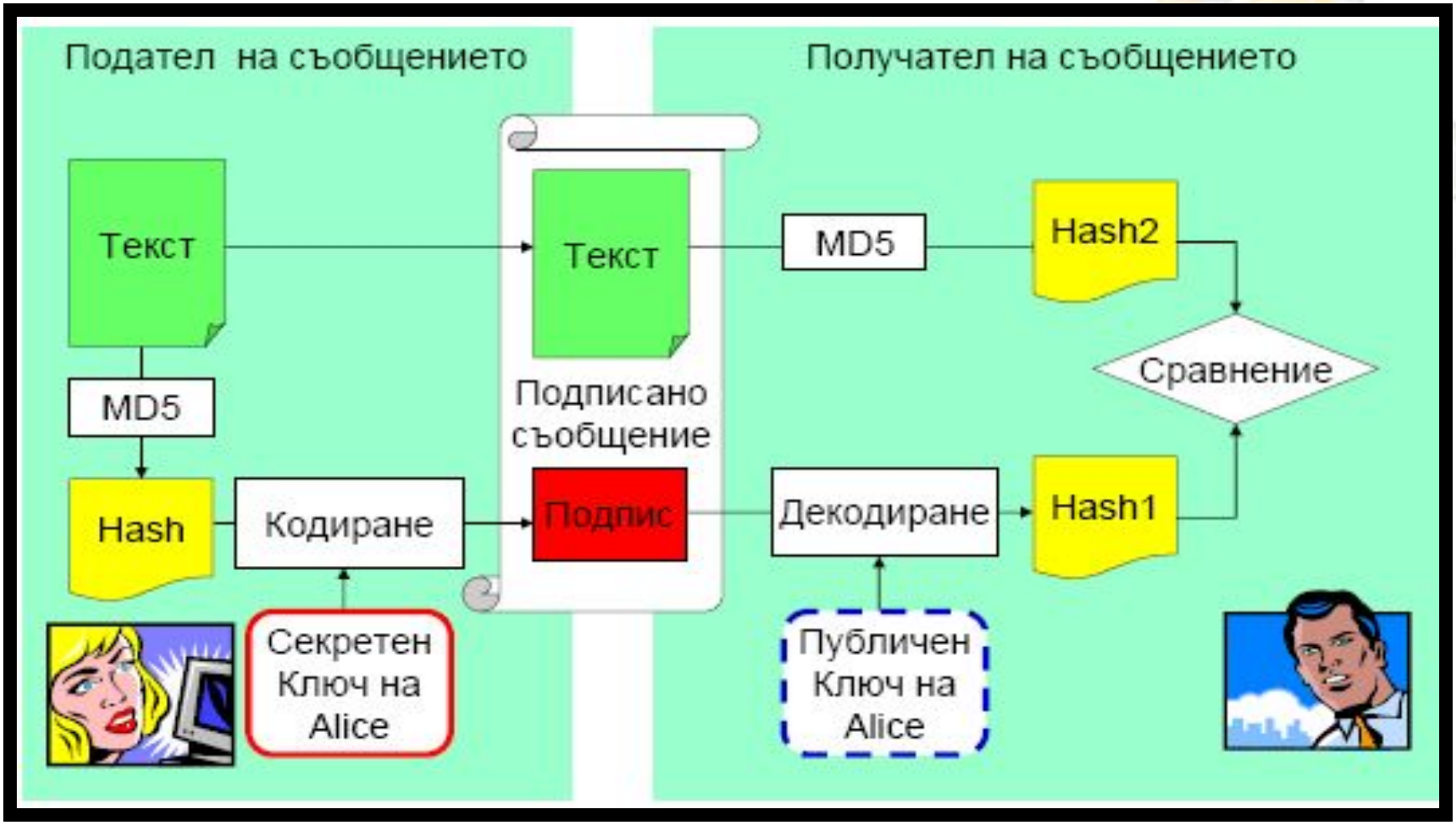
Идентификация на изпращача - **НЕ**

Доказване на авторството – **НЕ**

Предимство е лесното и безопасно разпространение на публичните ключове!

Криптираната информация със секретния ключ се декриптира само с публичния ключ, и криптираната информация с публичния ключ се декриптира само със секретния ключ.

Цифров Подпис



*Конфиденциалност на данните – **НЕ*** *Цялост на данните – **ДА***

*Идентификация на изпращача – **ДА*** *Доказване на авторството - **ДА***