ЕЛЕКТРОНЕН МАГАЗИН – ОСНОВНИ ПРИНЦИПИ ПРИ ОРГАНИЗАЦИЯТА. НАЧИНИ НА РАЗПЛАЩАНЕ. СИГУРНОСТ НА ТРАНЗАКЦИИТЕ

доц. д-р Иван Богомилов – НБУ

e-mail: bogomilov@bgmreja.com

E-SHOP - BASIC PRINCIPLES FOR THE ORGANIZATION. WAY OF PAYMENT. SECURITY OF TRANSACTIONS

Associated prof. d-r Ivan Bogomilov - NBU

e-mail: bogomilov@bgmreja.com

Key words: E-shop, SSL, ePay.bg.

Abstract - In the age of global communications based on Internet-based technologies to shape a new segment of the sale of goods and services between companies and between companies and end users - e-commerce. This report has discussed the difference between E-Business and E-commerce. Emphasis is on a major business models in electronic commerce - electronic shop (e-shop). In building such a structure must be taken into account the advertising of goods through the prism of "convenience of customers, methods of payment and security of transactions. Some principles have been considered in building the online shop. The following are specific examples. In the aspect of "security of transactions" briefly describes the payment system ePay.bg.

Резюме - Във века на глобалните комуникации, основани на Интернет базирани технологии се оформи нов сегмент на продажба на стоки и услуги между фирмите и между фирми и крайни потребители – електронна търговия. В този доклад е коментирана разликата между Е-бизнес и Е-търговия. Акцентирано е върху един от основните бизнес модели в електронната търговия - електронния магазин (Е-магазин). При изграждането на такава структура задължително се взема предвид начина на рекламиране на стоката през призмата „Удобство на клиента", начините на разплащане, както и сигурността на транзакциите. Разгледани са някои принципи при изграждането на Е-магазин. Дадени са конкретни примери. В аспект „Сигурност на транзакциите" накратко е описана платежната система ePay.bg.

1. УВОД

Интернет базираните технологии и развитието на глобалните мрежи стимулираха икономическа активност в Интернет, като ускориха обособяването и развитието на нов дял в икономиката - Интернет икономика. (Е – бизнес). Тя може да се опише като IP-базирани мрежи, софтуерни приложения и човешки ресурси, работещи за бизнеса в сферата на производство, купуване и предлагане на стоки и услуги в реално врене (on line).

Трябва да се прави разлика между Е- бизнес и Е-търговия.

Е- бизнесът покрива както вътрешни процеси, като организация и управление на производство, управление на човешки ресурси, контрол на заплащане, логистика, управление на складови ресурси, риск мениджмънт и други, така и Е-търговията. В основата е използването на ИКТ (информационни и комуникационни технологии), на базата на които се оптимизират бизнес процесите и се свежда до минимум влиянието на субективния фактор.

Така съвременните компании използват така наречените ERP (Enterprise resource planning) системи. ERP в общия случай е наименование на интегрирана корпоративна системи за управление на фирмените ресурси. Характерно за нея е това, че обхваща действително всички процеси в едно предприятие – производството (ако има такова), дистрибуцията на продуктите, служителите, сервиза, връзките с клиентите, връзките с доставчиците, счетоводството, склада, активите. Една ERP система обикновено е изградена в хардуерен и софтуерен план на модулен принцип. Модулният дизайн позволява да се добавят или реконфигурират модули, като се запази целостта на системата. ERP задължително поддържа релационна база данни. Всяка ERP система се изгражда съобразно конкретните нужди и спецификата на съответните бизнес процеси на даденото предприятие. Класическата ERP система е ориентирана предимно към вътрешните процеси, но вече се използват системи, интегриращи вътрешните процеси и тези от предния фронт (електронната търговия), това са така наречените CRM (customer relationship management) – управление на връзките с клиента, където например

клиентът може да бъде персонализиран, съобразно неговите приоритетни интереси или други параметри.

Електронната търговия (E-commerce) е продажба на стоки и услуги в средата на публичната мрежа. Предимствата на Е-търговията, спрямо традиционната са очевидни:

- **Неограничени възможности от страна на клиента за проучване на пазара** – Е-търговията позволява на клиента да открива, разглежда и поръчва стоките, които се предлагат двадесет и четири часа в денонощието, 365 дни в годината. Разнообразието на стоките, предлагани в различните търговски сайтове е огромно.
- **Глобален достъп** – На практика всички интернет потребители (потенциални клиенти) от целия свят имат достъп до съответния сайт. Това значително облекчава съответната компания в аспект развитие на офисна инфраструктура и разкриване на магазини, спестяват се и човешки ресурси.
- **Складова база** - наемането и поддръжката на складови пространства не е необходимо, особено когато продажбата не е на едро.
- **Удобство за клиента** - Доставката на закупената от клиента стока е „до вашата врата"
- **Разплащането е облекчено** – става по мрежата.
- **Значително по-низки цени на стоки и услуги** – на базата на горе споменатите предимства, които са в непосредствена връзка с повишената online конкуренция, чувствително по- низките режийни разходи и създадените удобства за клиента.
- **Рекламата** – в мрежата тя е по-евтина от средата на конвенционалните медии - радио, телевизия и преса.

В Е–търговията се дефинират различни бизнес модели в зависимост от спецификата на участващите играчи и съответните търговски отношения. Един от основните модели е Е-магазин (E-shop). При Е-магазина механизмите в отношенията търговец-клиент не се различават съществено от тези при традиционния магазин (разбира се трябва да се има предвид, че става въпрос за предлагане на стоки и услуги, в този смисъл например един хотел може също да се разглежда като

магазин). Разликата е, че тези отношения се развиват във виртуална среда, като са в сила всички изброени предимства на Е-търговията.

2. Е-МАГАЗИН. ЕЛЕМЕНТИ И ОРГАНИЗАЦИЯ

Задължителни елементи в организацията на Е-магазина са:

- Продукти
- WEB сайт (или присъствие в такъв)
- Начин на разплащане – обикновено е дефинирана електронната платежна система, която се използва (ако се използва такава)
- Дефиниране на доставката (цена и срок).
- Допълнителни елементи

Продуктите са основния елемент, който трябва да присъства в един сайт на Е-магазин. Стоки или услуги трябва да бъдат групирани по определени признаци, да бъдат подробно описвани, а също така да имат цени за продажба. Добрата организация осигурява както по-лесното управление на електронния магазин, така и по-голяма гъвкавост на клиентите при работата им с продуктовите каталози.

WEB сайт. Този елемент също е задължителен за Е-магазина по понятни причини. Трябва да се има предвид, че не винаги за дадена фирма е рентабилно да поддържа собствен сайт**.** В повечето случаи, особено при малкия и средния бизнес се използва форма на обединение на отделни Е-магазини, известно като бизнес модели „Електронни хали" или „Пазар при трето лице". В първия случай това е обединение на Е-магазини в WEB сайт, във втория – обединение под шапката на известна компания. Двата модела са много близки като същност и фактически са производни на Е-магазина. И в двата случая има единно администриране на сайта и в общия случай, използване на единна система за разплащане.

Независимо от това дали сайтът е за отделен Е-магазин, или група такива, той трябва да удовлетворява определени изисквания [1]:

- Сайтът се състои от публична и административна част. Публичната част е тази, която се вижда, т.е. върху нея са разположени всички продукти и се осъществяват процесите на покупко-продажба.

Административната част е мястото, в което се въвежда и редактира информацията за всички продукти, клиенти и техните поръчки. Тук могат да влизат само за служители с определено ниво на достъп.

- Публичната част на сайта трябва да бъде „friendly" ориентирана към клиента, т.е. същият да не среща трудности при разглеждането и подбора на стоките и услугите. Това се получава при вертикално и хоризонтално структуриране на продуктовата информация. Използват се категории и подкатегории – по вертикалата и атрибути – по хоризонталата. Така например ако клиентът търси лаптоп с производител HP и конкретни параметри отива в категория „компютри", от там в категория „лаптоп", след което въвежда атрибутите (производител, тип и скорост на процесора, обем на RAM-а и др.). В резултат на филтрирането се появява желания продукт [2]. В крайна сметка търсачката на сайта трябва да бъде така организирана, че клиентът да може да прави нужните му разрези на предлаганите стоки – например по цени, по година на производство, по производител и т.н.

Начин на разплащане. В сайта на търговеца всеки продукт трябва да бъде представен задължително с цената си. Трябва да бъдат описани начините на разплащане. Модерните компании използват електронни платежни системи (не е задължително). В такъв случай сайтът осигурява достъп до съответния платежен инструмент.

Доставка. Описанието на продукта трябва да бъде съпроводено с условията на доставянето му до клиента – цена и срок на доставката [3].

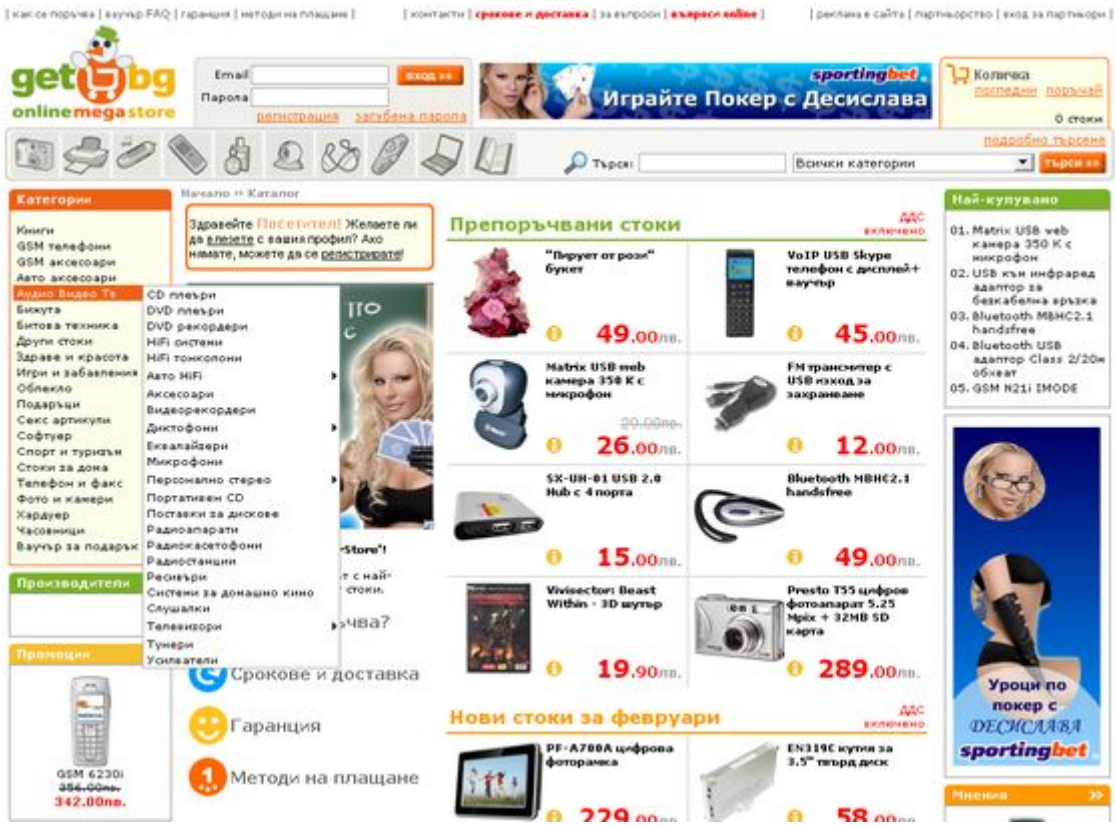
Допълнителни елементи. Това са модулите, които са свързани с помощ при използване на електронния магазин, често задавани въпроси, контакти и др. В последно време с цел изграждане на доверие в клиента, към някои търговски сайтове се организират форуми, в които клиентите изказват мнение за обслужването и дават препоръки.

3. КОНКРЕТНИ РЕШЕНИЯ.

Един добре структуриран магазини изглежда, както следва:

Още с отварянето на сайта всичко, което е необходимо, стои на преден план – фиг. 1. В лявата част на страницата се намират основните менюта – "Категории", "Производители", "Промоции" и "Какво ново" [4].

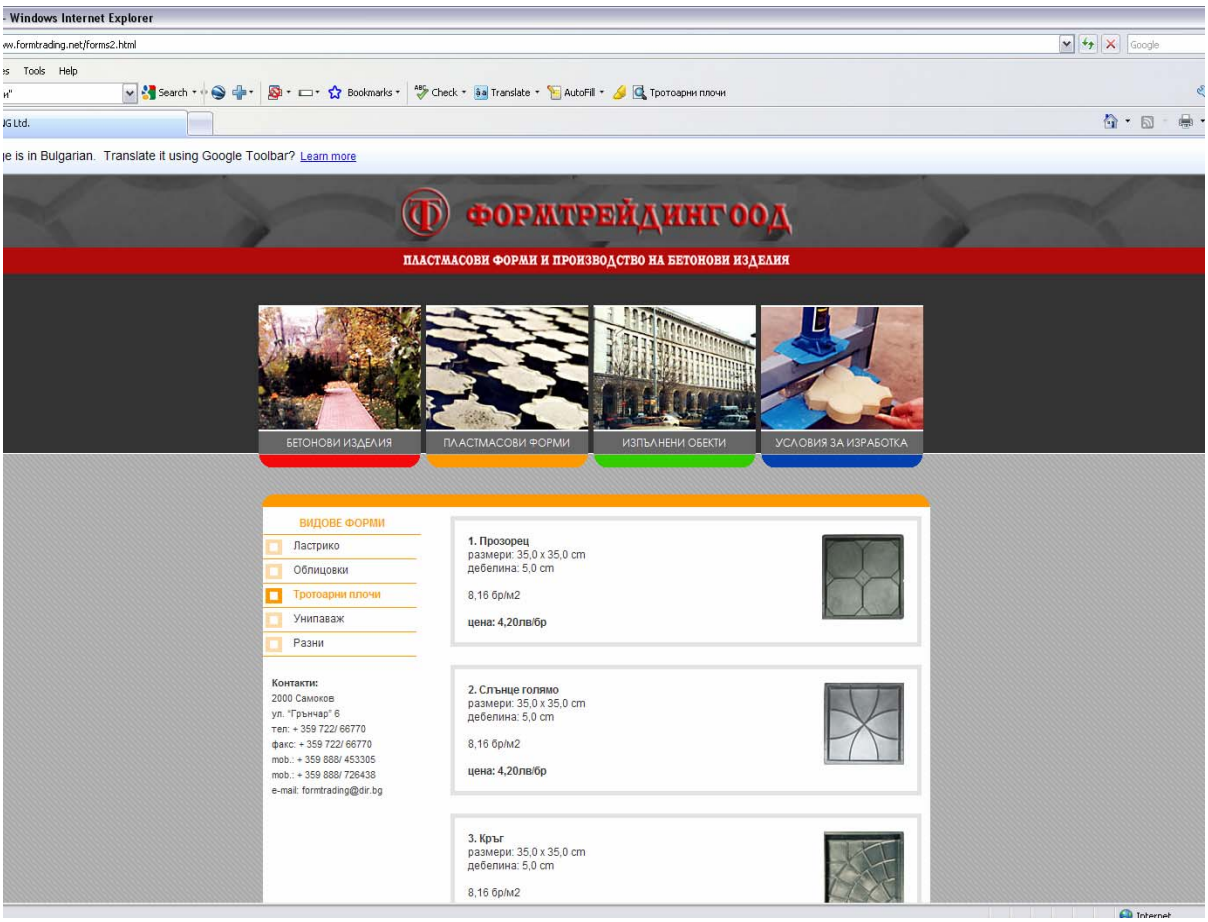
В "Категории" се намират всички основни групи стоки, които се предлагат. При избиране на категорията, в централната част на екрана се зареждат съответните подкатегории, илюстрирани със снимки. От наличния падащ списък "Покажи" могат да се изведат на страницата само стоките от даден производител или търговска марка. Маркирайки снимката или описанието на продукта, се влиза в индивидуалната страница на продукта. Там може да се види подробно описание на всички негови функции, както и по-голяма снимка и разбира се цената му.



Фиг. 1

На началната страница се намират и четири връзки, които ще улеснят всеки, който има проблеми с ориентацията в самия сайт. Те отговарят на въпросите "Как се поръчва?", "Срокове и доставка", "Гаранция" и "Методи на плащане".

Много често, по-голямата част от изискванията към организацията на Е-магазина не са изпълнени и тогава се стига до примера от фиг. 2.



Фиг. 2

В случая производител на облицовъчни плочи представя своето производство [5]. Описани са продуктите със съответните цени и са дадени телефони и E-mail за контакти. Начина на плащане, отстъпки, условия за доставка се договарят допълнително (по телефон или факс). Независимо от това, примерът (често срещан в България) притежава елементи на Е-магазин – глобалния достъп за всички клиенти, лесен WEB маркетинг за производителя, по-низки режии и от там по-низки цени (в последното авторът се е убедил лично).

4. РАЗПЛАЩАНЕ, СИГУРНОСТ ПРИ ТРАНЗАКЦИИТЕ

Както вече бе споменато, модерният търговски сайт използва електронни инструменти за плащане. Това обикновено е електронна платежна система – в България най често се използва e-Pay.bg. Също така се предлагат алтернативни начини на плащане, базирани на конвенционални инструменти. Процедурите при електронното разплащане се реализират в публичната мрежа. Това е свързано с

определени рискове по отношение сигурността на транзакциите. Всяка електронна платежна система взема мерки в това отношение. Мерките са свързани с изграждане на защитени канали за комуникация в публичната мрежа между клиента и сървъра на платежната система.

Сървърът и клиентът трябва да се аутентикират един спрямо друг, т.е клиентът да е убеден, че комуникира точно с избрания сървър и сървърът - точно с определения клиент.

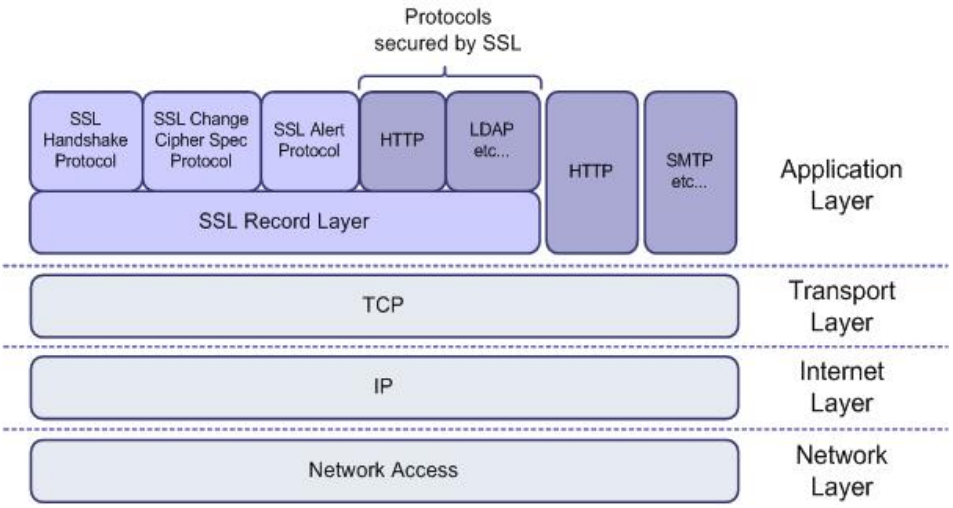
Участниците в тази комуникация трябва да са убедени, че данните, които обменят не са променени по пътя, т.е. да е гарантиран техният интегритет.

Аутентикацията се постига с използването на публични ключове (публичен и частен), които съдържат в себе си информация за притежателя им (т.н. е-сертификат). Интегритета на данните се гарантира с използването на Хеш функция (хеширане) – SHA-1 или MD5. Конфиденциалността е резултат от криптиране на данните. Същите могат да бъдат криптирани с публичен и частен ключ (асиметрично криптиране и декриптиране), но това ангажира прекалено голям изчислителен ресурс. За това двете страни договарят сесиен ключ на симетричен криптографски алгоритъм, обменят го криптиран с публични ключове и след това го използват само за дадената сесия.

Тези операции се реализират, чрез протокола SSL (Secure Socket Layer и неговия наследник TLS (Transport Layer Security) [6]. След 2 последователни итерации се стига до версията SSL v3.0, след което се стига до TLS (RFC 2246), известен още като SSL v.3.1.

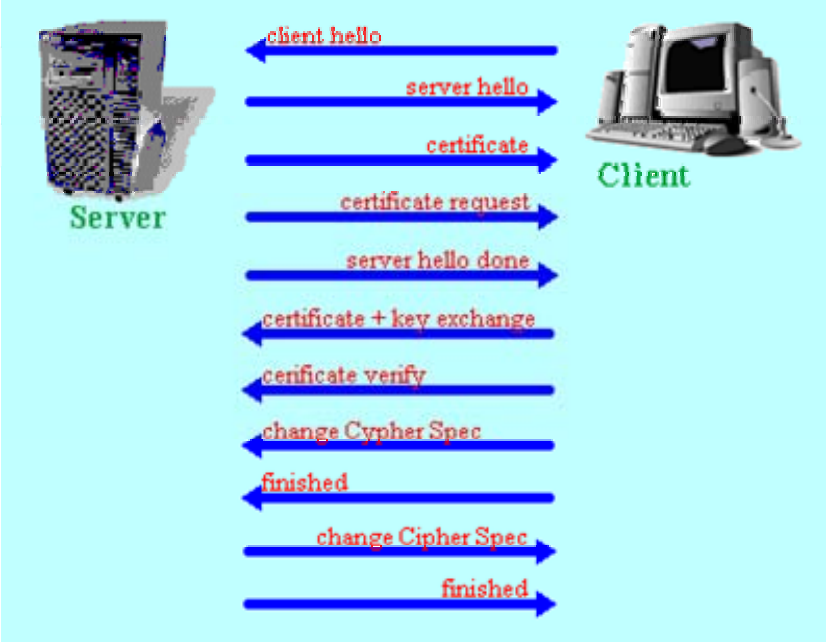
По-надолу е дадено описанието на TSL (SSL) и неговото действие:

В същност трябва да се говори за протоколен стек, състоящ се от Handshake Protocol, Change Cipher Spec и Alert protocol. От фигура 3. се вижда, че този стек гарантира сигурността на HTTP, а също може да се използва за SMTP.



Фиг.3

Handshake се реализира, както следва (фиг.4):



Фиг.4

- Клиентът изпраща **ClientHello** съобщение, което указва версията на TLS, която поддържа, едно случайно число, лист на предложените комплекти за кодиране и методи за компресия.

- Сървърът отговаря със **ServerHello**, което съдържа избраната версия на протокола, едно случайно число, кодирането и методът за компресия от посочените от клиента методи
- Сървърът изпраща своя **Сертификат** (обикновено X.509).
- Сървърът може да поиска сертификат от клиента, така че връзката да бъде взимно автентифицирана, чрез използванен на CertificateRequest (това е опционално).
- Сървърът изпраща съобщение **ServerHelloDone**, след като приключи с договарянето на handshake.
- Клиентът отговаря с **ClientKeyExchange**, което може да съдържа *PreMasterSecret*, публичен ключ или нищо (Това отново зависи от избраното кодиране)
- Клиентът и сървъра след това използват случайните числа и PreMasterSecret за да изчислят една обща парола, наричана „главна парола" ("master secret"). Всички други данни за ключове се изчисляват от тази главна парола (както и от генерираните от клиента и от сървъра случайни числа), които се предават през внимателно планирана „псевдослучайна функция".
- След това Клиентът изпраща на съобщение **ChangeCipherSpec**, с което казва на сървъра, „всичко, което ти изпратя отсега нататък ще бъде криптирано."
- Накрая Клиентът изпраща криптирано съобщение **Finished**, което съдържа хеш и MAC (Message authentication code) върху предишните handshake съобщения.
- Сървърът дешифрира Клиентското съобщение *Finished*, и проверява хеш и MAC. Ако дешифрирането или проверката са неуспешни, handshake се счита за неуспешен и връзката би трябвало да бъде прекъсната.
- Накрая сървърът изпраща **ChangeCipherSpec** и неговото криптирано съобщение **Finished**, а клиентът изпълнява същото дешифриране и проверка.
- На този етап **handshake** е приключен.

ChangeCipherSpec Protocol се използва в последната фаза на Handshake протокола за да се уверомят страните да првключат от статус на очакване към текущия статус. Това означава, че страните ще приключват използването на

алгоритма за обмен на ключове и пристъпват към криптиране и MAC алгоритмите, които са дефинирали през предишните фази на Handshake протокола.

Alert Protocol се грижи за предаване на информация за грешки, които се появяват по време на връзката. Има две нива на аларма: фатална аларма или предупреждение. В случай на фатална аларма, връзката се прекъсва.

За да стане ясно действието на SSL, по-долу е описана една конкретна имплементация в системата за защита на информацията в e-pay.bg.от 1999г [7].:

Системата има следните три цели:

- Аутентикация на сървъра пред клиента;
- Аутентикация на клиента пред сървъра;
- Осигуряване на секретен канал за предаване на данни между клиента и сървъра.

За осъществяване на тези цели се използва набор общодостъпни симетрични криптографски алгоритми, в частност DEA (DES), BLOWFISH и ELGAMAL. За електронен подпис се използва алгоритъма MD5 на RSA Data Security.

- Аутентикация на сървъра пред клиента

Аутентикацията на сървъра пред клиента се осъществява по следния механизъм:

1. Клиентът генерира случайна поредица с дължина 32 байта.
2. Клиентът кодира поредицата с публичния ключ на сървъра.
3. Клиентът изпраща кодираното съобщение на сървъра.
4. Сървърът декодира съобщението.
5. Сървърът съставя електронен подпис на поредицата байтове, използвайки MD5.
6. Сървърът изпраща електронния подпис на клиента в *явен (некодиран)* вид.
7. Клиентът сравнява получения подпис с подписа, генериран при него.

8. Съвпадението на двата подписа е основание за клиента да смята, че сървърът разполага със съответния секретен ключ, което идентифицира сървъра пред клиента.

Използването на електронен подпис в случая се налага, за да не се компрометира информацията, кодирана с публичния ключ, което потенциално би могло да доведе до извличане на секретния ключ.

- Аутентикация на клиента пред сървъра

За аутентикация на клиента пред сървъра се използва случайна поредица с дължина 32 байта, която е *секретна* , предоставя се от централата и е различна за всеки отделен клиент. По-долу ще наричаме тази поредица "пръстов отпечатък" (fingerprint, FP).

Описание на процедурата по аутентикация на клиента пред сървъра:

1. Сървърът генерира случайна поредица с дължина 32 байта.
2. Сървърът изпраща поредицата на клиента в явен вид.
3. Клиентът генерира случайна поредица с дължина 32 байта, която ще се използва и за ключ за предаване на данните (Data Encryption Key, DEK).
4. Клиентът съставя електронен подпис на DEK, поредицата на сървъра и своя FP, използвайки MD5.
5. Клиентът кодира DEK и електронния подпис с публичния ключ на сървъра.
6. Клиентът изпраща кодираното съобщение на сървъра
7. Сървърът декодира съобщението със своя секретен ключ.
8. Сървърът съставя електронен подпис на DEK, поредицата от т.1) и FP на клиента, с който предполага, че комуникира.
9. Сървърът сравнява електронния подпис от съобщението с подписа, генериран при него.
10. Съвпадението на двата подписа е основание за сървъра да смята, че клиентът наистина разполага със съответния FP, което идентифицира клиента пред сървъра.

FP на клиента не се използва в явен вид, за да не се компрометира секретният ключ на сървъра.

Използването на случайния пакет от т.1) се налага за защита от атаки, базирани на повторение на информация, прихванатата от трето лице.

- Осигуряване на секретен канал за предаване на данни между клиента и сървъра

  След успешна аутентикация на двете страни DEK се използва като ключ за симетричен криптографски алгоритъм, с който да се засекретяват данните – предмет на комуникацията между клиента и сървъра. Какъв точно алгоритъм ще се използва се определя от клиента.

  Възможни алгоритми за целта са DEA (DES), 3DES, IDEA, BLOWFISH.

DEK е валиден само за една комуникационна сесия между двете страни.

- Описание на конкретната имплементация

Поради изчислителната сложност на алгоритмите с публичен ключ и свързаните с това времезакъснения, описаните по-горе стъпки са обединени, така че да се налага само едно кодиране/разкодиране с алгоритъма с публичен ключ:

1. Клиентът установява връзка със сървъра, използвайки TCP/IP.
2. Сървърът генерира случайна поредица от 32 байта RS.
3. Сървърът изпраща RS на клиента в явен вид.
4. Клиентът приема RS.
5. Клиентът генерира случайни поредици от по 32 байта RC и DEK.
6. Клиентът съставя информационен пакет със следната структура

Поле	Дължина в байтове	Описание
RC	32	Случайна поредица за аутентикация на сървъра
A	1	Код на симетричния алгоритъм
DEK	32	Ключ за симетричния алгоритъм
MD5(DEK, RS, FP)	20	Електронен подпис за аутентикация на клиента

7. Клиентът кодира пакета с публичния ключ на сървъра.
8. Клиентът изпраща кодирания пакет на сървъра.
9. Сървърът приема кодирания пакет.
10. Сървърът декодира пакета.
11. Сървърът извършва процедурата по идентификация на клиента.
12. Ако аутентикацията на клиента пропадне, сървърът прекратява едностранно връзката.
13. Сървърът съставя електронен подпис MD5(RC).
14. Сървърът изпраща MD5(RC) на клиента в явен вид
15. Клиентът приема MD5(RC).
16. Клиентът извършва процедурата по аутентикация я на сървъра .
17. Ако аутентикацията на сървъра пропадне, клиентът прекратява едностранно връзката.
18. Клиентът и сървърът започват да обменят данни, използвайки алгоритъма A о с ключ DEK .

HTTPS:

HTTPS (HTTP през SSL или Secure HTTP) е използване на SSL/TLS под HTTP. HTTPS и SSL дава възможност на сървъра да използва на X.509 цифрови сертификати.

HTTPS използва порт 443, вместо порт 80 на http.

Всички описани по горе инструменти за сигурност се използват в системата ePay.bg [8]. Сигурността на съобщенията, свързани с плащането се основава на протокола SSL/TLS. Той осигурява идентификацията и авторизацията между браузъра на картодържателя и търговеца и Web сървъра на e-pay.bg, а също така и целостта и неприкосновеността на обменяните данни.

Системата работи на базата на персонална микросметка. Сигурността на транзакциите се поддържа посредством SSL/TLS на три нива: първото е едностранна аутентикация на сървъра пред клиента, като клиентът влиза в системата посредством потребителско име и парола. Второто ниво е когато клиентът изтегля и използва безплатен електронен сертификат от ePay.bg. Начинът на инсталиране на сертификата върху клиентския компютер в зависимост от клиентския браузер (Microsoft Internet Explorer или Mozilla Firefox) е описан в сайта на системата [7]. Третото ниво е когато клиентът притежава персонален сертификат, закупен от Доставчик на Удостоверителни Услуги (ДУУ). При второто и третото ниво аутентикацията е двустранна: сървър-клиент и клиент – сървър.

5. ЗАКЛЮЧЕНИЕ

Описаната по-горе форма на общуване на потребителя с търговеца става все по-популярна с развитието на информационното общество, включително и в България. Предимствата са очевидни – потребителят може да оптимизира намирането на желания продукт (цена и качество) "on line", с глобален достъп до информация, без да губи ценно време.

Като изключим атрактивността на съответния продукт, търговският сайт трябва да удовлетворява изискванията за

- Добра организация (много фирми са се специализирали в разработка на търговски сайтове).
- Изграждане на доверие
- Сигурност на транзакциите – използване на подходяща платежна система.

6. ЛИТЕРАТУРА:

[1] Fen Wang, "E-Shoppers' Perception of Web-Based Decision Aid ",Encyclopedia of e-commerce, e-government, and mobile commerce / Mehdi Khosrow-Pour, editor. Copyright © 2006 by Idea Group Inc.

[2] http://www.plesio.bg/

[3] http://www.ebay.com/

[4] http://www.get.bg

[5] http://www.formtrading.net

[6] http://docs.sun.com/source/816-6156-10/contents.htm

[7] Описание на системата за защита на търговската информация за системата ePay.bg, ДАТАМАКС ООД, 1999

[8] https://www.epay.bg/