

MỤC LỤC

LỜI CẢM ƠN	2
1.1 MỘT SỐ KHÁI NIỆM TOÁN HỌC	3
1.1.1 Số nguyên tố và nguyên tố cùng nhau	3
1.2 CÁC KHÁI NIỆM VỀ MÃ HOÁ	9
1.2.1 Khái niệm mã hóa.	9
1.2.2 Các phương pháp mã hóa.	11
1.2.3 Một số hệ mã hoá cụ thể.	13
1.3 KHÁI NIỆM VỀ KÝ ĐIỆN TỬ.	17
1.3.1 Định nghĩa.	17
1.3.2 Phân loại sơ đồ chữ ký điện tử.	17
1.3.3 Một số sơ đồ ký số cơ bản.	18
1.4 VẤN ĐỀ XÁC THỰC.	21
1.4.1 Khái niệm xác thực	21
1.4.2 Khái niệm xác thực số (điện tử).	22
1.4.3 Công cụ xác thực: Chứng chỉ số.	24
CHƯƠNG 2. GIAO DỊCH ĐIỆN TỬ	29
2.1 THƯƠNG MẠI ĐIỆN TỬ	29
2.1.1 Khái niệm	29
2.1.2 Các đặc trưng của Thương mại điện tử	30
2.1.3 Các cơ sở để phát triển Thương mại điện tử	32
2.1.4 Các loại hình giao dịch Thương mại điện tử	32
2.1.5 Các hình thức hoạt động chủ yếu của Thương mại điện tử	34
2.2 THANH TOÁN ĐIỆN TỬ	41
2.2.1 Tổng quan về thanh toán điện tử	41
2.3 GIAO DỊCH ĐIỆN TỬ SỬ DỤNG TIỀN ĐIỆN TỬ	49
2.3.1 Tổng quan về giao dịch điện tử dùng tiền điện tử	49
2.3.2 Tiền điện tử	50
2.4 GIAO DỊCH ĐIỆN TỬ KHÔNG SỬ DỤNG TIỀN ĐIỆN TỬ	57
2.4.1 Dịch vụ ngân hàng điện tử	57
2.4.2 Tổng quan về sự phát triển ngân hàng điện tử tại Việt Nam	58
2.4.3 Giới thiệu một số dịch vụ ngân hàng điện tử tại Việt Nam	59
2.4.4 Ưu nhược điểm, hướng phát triển.	63
CHƯƠNG 3. MÔ HÌNH GIẢI PHÁP THANH TOÁN TRỰC TUYẾN	66
CHƯƠNG 4. CHƯƠNG TRÌNH MÔ PHỎNG	71
4.1 Yêu cầu phần cứng & phần mềm thử nghiệm	71
4.2 Chương trình mô phỏng	72
KẾT LUẬN	77
TÀI LIỆU THAM KHẢO	78

LỜI CẢM ƠN

Em xin chân thành gửi lời cảm ơn tới các thầy cô của trường, các thầy cô trong Ban giám hiệu và thầy cô trong Bộ môn Tin học của trường Đại học Dân lập Hải Phòng đã tận tình giảng dạy, giúp đỡ và tạo mọi điều kiện cho chúng em trong suốt thời gian học tập tại trường.

Và em cũng xin gửi lời cảm ơn tới thầy Trần Ngọc Thái – Giáo viên hướng dẫn - đã tận tình, hết lòng hướng dẫn em trong suốt quá trình nghiên cứu đề hoàn thành đồ án tốt nghiệp này. Em mong thầy luôn luôn mạnh khỏe để nghiên cứu và giảng dạy, đào tạo nguồn nhân lực cho đất nước.

Một lần nữa em xin chân thành cảm ơn.

Hải Phòng, ngày tháng năm 2009

Sinh viên thực hiện

Vũ Hoàng Nam

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN

1.1 MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.1.1 Số nguyên tố và nguyên tố cùng nhau

Số nguyên tố là số nguyên dương chỉ chia hết cho 1 và chính nó.

Ví dụ: 2, 3, 5, 7, 17, ... là những số nguyên tố.

Hệ mật mã thường sử dụng các số nguyên tố ít nhất là lớn hơn 10^{150} .

Hai số m và n được gọi là **nguyên tố cùng nhau** nếu ước số chung lớn nhất của chúng bằng 1. Ký hiệu: $\gcd(m, n) = 1$.

Ví dụ: 9 và 14 là nguyên tố cùng nhau.

1.1.2 Đồng dư thức

Cho a và b là các số nguyên tố, n là số nguyên dương thì a được gọi là đồng dư với b theo modulo n nếu $n|a-b$ (tức $a - b$ chia hết cho n , hay khi chia a và b cho n được cùng một số dư như nhau). Số nguyên n được gọi là modulo của đồng dư.

Kí hiệu: $a \equiv b \pmod{n}$

Ví dụ: $67 \equiv 11 \pmod{7}$, bởi vì $67 \pmod{7} = 4$ và $11 \pmod{7} = 4$.

Tính chất của đồng dư:

Cho $a, a_1, b, b_1, c \in \mathbb{Z}$. Ta có các tính chất:

- $a \equiv b \pmod{n}$ nếu và chỉ nếu a và b có cùng số dư khi chia cho n .
- Tính phản xạ: $a \equiv a \pmod{n}$.
- Tính đối xứng: Nếu $a \equiv b \pmod{n}$ thì $b \equiv a \pmod{n}$.
- Tính giao hoán: Nếu $a \equiv b \pmod{n}$ và $b \equiv c \pmod{n}$ thì $a \equiv c \pmod{n}$.
- Nếu $a \equiv a_1 \pmod{n}$, $b \equiv b_1 \pmod{n}$
thì $a + b \equiv (a_1 + b_1) \pmod{n}$ và $ab \equiv a_1b_1 \pmod{n}$.

1.1.3 Không gian Z_n và Z_n^*

Không gian Z_n (các số nguyên theo modulo n)

Là tập hợp các số nguyên $\{0, 1, 2, \dots, n-1\}$. Các phép toán trong Z_n như cộng, trừ, nhân, chia đều được thực hiện theo module n .

Ví dụ: $Z_{11} = \{0, 1, 2, 3, \dots, 10\}$

Trong Z_{11} : $6 + 7 = 2$, bởi vì $6 + 7 = 13 \equiv 2 \pmod{11}$.

Không gian Z_n^*

Là tập hợp các số nguyên $p \in Z_n$, nguyên tố cùng n .

Tức là: $Z_n^* = \{p \in Z_n \mid \gcd(n, p) = 1\}$, $\Phi(n)$ là số phần tử của Z_n^*

Nếu n là một số nguyên tố thì: $Z_n^* = \{p \in Z_n \mid 1 \leq p \leq n-1\}$

Ví dụ: $Z_2 = \{0, 1\}$ thì $Z_2^* = \{1\}$ vì $\gcd(1, 2) = 1$.

1.1.4 Phần tử nghịch đảo

Định nghĩa:

Cho $a \in Z_n$. Nghịch đảo của a theo modulo n là số nguyên $x \in Z_n$ sao cho $ax \equiv 1 \pmod{n}$. Nếu x tồn tại thì đó là giá trị duy nhất, và a được gọi là khả nghịch, nghịch đảo của a ký hiệu là a^{-1} .

Tính chất:

- Cho $a, b \in Z_n$. Phép chia của a cho b theo modulo n là tích của a và b^{-1} theo modulo n , và chỉ được xác định khi b có nghịch đảo theo modulo n .
- Cho $a \in Z_n$, a là khả nghịch khi và chỉ khi $\gcd(a, n) = 1$.
- Giả sử $d = \gcd(a, n)$. Phương trình đồng dư $ax \equiv b \pmod{n}$ có nghiệm x nếu và chỉ nếu d chia hết cho b , trong trường hợp các nghiệm d nằm trong khoảng 0 đến $n - 1$ thì các nghiệm đồng dư theo modulo n/d .

Ví dụ: $4^{-1} = 7 \pmod{9}$ vì $4 \cdot 7 \equiv 1 \pmod{9}$

1.1.5 Khái niệm nhóm, nhóm con, nhóm Cyclic

Nhóm là bộ các phần tử $(G, *)$ thỏa mãn các tính chất:

- Kết hợp: $(x * y) * z = x * (y * z)$
- Tồn tại phần tử trung lập $e \in G: e * x = x * e = x, \forall x \in G$
- Tồn tại phần tử nghịch đảo $x' \in G: x' * x = x * x' = e$

Nhóm con của nhóm $(G, *)$ là bộ các phần tử $(S, *)$ thỏa mãn các tính chất:

- $S \subset G$, phần tử trung lập $e \in S$.
- $x, y \in S \Rightarrow x * y \in S$.

Nhóm Cyclic: Là nhóm mà mọi phần tử của nó được sinh ra từ một phần tử đặc biệt $g \in G$.

Phần tử này được gọi là **phần tử sinh (nguyên thủy)**, tức là:

Với $\forall x \in G: \exists n \in \mathbb{N}$ mà $g^n = x$.

Ví dụ: $(\mathbb{Z}^+, *)$ là nhóm cyclic có phần tử sinh là 1.

Định nghĩa:

Ta gọi **Cấp** của nhóm là số các phần tử trong nhóm đó.

Như vậy, nhóm $\mathbb{Z}_n^*$ có cấp $\Phi(n)$.

Nếu p là số nguyên tố thì nhóm $\mathbb{Z}_p^*$ có cấp là $p-1$

Định nghĩa:

Cho $a \in \mathbb{Z}_n^*$, cấp của a ký hiệu là **ord(a)**

được định nghĩa là số nguyên dương nhỏ nhất t thỏa mãn: $a^t \equiv 1 \pmod{n}$.

Ví dụ: $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, $\Phi(21) = 12 = |\mathbb{Z}_{21}^*|$

và cấp của từng thành phần trong $\mathbb{Z}_{21}^*$ là:

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
Cấp của a	1	6	3	6	2	6	6	2	3	6	6	2

1.1.6 Bộ phần tử sinh (Generator-tuple)

$\{g_1, \dots, g_k\}$ được gọi là bộ phần tử sinh nếu mỗi g_i là một phần tử sinh và những phần tử này khác nhau ($g_i \neq g_j$ nếu $i \neq j$).

Ví dụ: $\{3, 5\}$ là bộ phần tử sinh của Z_7^* , bởi vì:

$$1 = 3^6 \bmod 7 = 5^6 \bmod 7$$

$$2 = 3^2 \bmod 7 = 5^4 \bmod 7$$

$$3 = 3^1 \bmod 7 = 5^5 \bmod 7$$

$$4 = 3^4 \bmod 7 = 5^2 \bmod 7$$

$$5 = 3^5 \bmod 7 = 5^1 \bmod 7$$

$$6 = 3^3 \bmod 7 = 5^3 \bmod 7.$$

2 không phải là phần tử sinh của Z_7^* , bởi vì:

$$\{2, 2^2, 2^3, 2^4, 2^5, 2^6\} = \{2, 4, 1, 2, 4, 1\} \Leftrightarrow \{1, 2, 4\}$$

Tuy nhiên $\{1, 2, 4\}$ là tập con của $\{1, 2, 3, 4, 5, 6\} = Z_7^*$,

do đó số 2 được gọi là “phần tử sinh của nhóm $G(3)$ ”,

$G(3)$ là nhóm có 3 thành phần $\{1, 2, 4\}$.

1.1.7 Bài toán đại diện (Presentation problem).

Gọi g là phần tử sinh của nhóm con $G(q)$ thuộc Z_n^* . Bài toán logarit rời rạc liên quan đến việc tìm số mũ a , sao cho:

$$a = \log_g h \bmod n \quad (\text{với } h \in G(q)).$$

Cho $k \geq 2$, $1 \leq a_i \leq q$, $i = 1 \dots k$.

Bài toán đại diện là: cho h thuộc $G(q)$, tìm $\{a_1, \dots, a_k\}$, của bộ phần tử sinh $\{g_1, \dots, g_k\}$,

sao cho:

$$h = g_1^{a_1} * g_2^{a_2} * \dots * g_k^{a_k} \bmod n$$

$\{a_1, \dots, a_k\}$ được gọi là đại diện (*representation*).

Ví dụ:

Cho tập Z_{23}^* , thì ta có thể tìm được:

nhóm con $G(11)=\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ với những phần tử sinh g_i là: **2, 3**, 4, 6, 8, 9, 12, 13, 16, 18.

$\{2, 3\}$ là 2 phần tử sinh của nhóm con $G(11)$ trong Z_{23}^* .

Bài toán đại diện là với $h = 13 \in G(11)$, tìm $\{a_1, a_2\}$ sao cho:

$$13 = 2^{a_1} * 3^{a_2} \bmod 23$$

Logarit hai vế, có $a_1 * \log(2) + a_2 * \log(3) = \log(13) \bmod 23$.

Kết quả là: $a_1 = 2$ và $a_2 = 2$, vì $2^2 * 3^2 = 4 * 9 = 36 = 13 \bmod 23$.

Hay $a_1 = 7$ và $a_2 = 11$, vì $2^7 * 3^{11} = 128 * 177147 = 13 \bmod 23$.

1.1.8 Hàm băm.

Hàm băm ***h*** là hàm một chiều (one-way hash) với các đặc tính sau:

- Với thông điệp đầu vào ***x*** thu được bản băm ***z = h(x)*** là duy nhất.
- Nếu dữ liệu trong thông điệp ***x*** thay đổi hay bị xóa để thành thông điệp ***x'*** thì ***h(x') ≠ h(x)***. Cho dù chỉ là một sự thay đổi nhỏ hay chỉ là xóa đi 1 bit dữ liệu của thông điệp thì giá trị băm cũng vẫn thay đổi. Điều này có nghĩa là: hai thông điệp hoàn toàn khác nhau thì giá trị hàm băm cũng khác nhau.
- Nội dung của thông điệp gốc “khó” suy ra từ giá trị hàm băm. Nghĩa là: với thông điệp ***x*** thì dễ dàng tính được ***z = h(x)***, nhưng lại “khó” suy ngược lại ***x*** nếu chỉ biết giá trị hàm băm ***h(x)***.

Tính chất:

Hàm băm ***h*** là không va chạm yếu:

Nếu cho trước một bức điện ***x***, thì không thể tiến hành về mặt tính toán để tìm ra một bức điện ***x' ≠ x*** mà ***h(x') = h(x)***.

Hàm băm ***h*** là không va chạm mạnh:

Nếu không có khả năng tính toán để tìm ra hai bức thông điệp ***x*** và ***x'*** mà ***x ≠ x'*** và ***h(x) = h(x')***.

1.2 CÁC KHÁI NIỆM VỀ MÃ HOÁ.

1.2.1 Khái niệm mã hóa.

Ta biết rằng tin truyền trên mạng rất dễ bị lấy cắp. Để đảm bảo việc truyền tin an toàn người ta thường mã hoá thông tin trước khi truyền đi. Việc mã hoá thường theo quy tắc nhất định gọi là hệ mật mã. Hiện nay có hai loại hệ mật mã mật mã cổ điển và mật mã khoá công khai. Mật mã cổ điển dễ hiểu, dễ thực thi nhưng độ an toàn không cao. Vì giới hạn tính toán chỉ thực hiện trong phạm vi bảng chữ cái sử dụng văn bản cần mã hoá (ví dụ Z_{26} nếu dùng các chữ cái tiếng anh, Z_{256} nếu dùng bảng chữ cái ASCII...). Với các hệ mã cổ điển, nếu biết khoá lập mã hay thuật toán thuật toán lập mã, người ta có thể "dễ" tìm ra được bản rõ. Ngược lại các hệ mật mã khoá công khai cho biết khoá lập mã K và hàm lập mã C_k thì cũng rất "khó" tìm được cách giải mã.

1.2.1.1. Hệ mã hóa.

Hệ mã hóa là hệ bao gồm 5 thành phần (P , C , K , E , D) thỏa mãn các tính chất sau:

P (Plaintext): là tập hợp hữu hạn các bản rõ có thể.

C (Ciphertext): Là tập hữu hạn các bản mã có thể

K (Key): Là tập hợp các bản khoá có thể

E (Encryption): Là tập hợp các quy tắc mã hoá có thể

D (Decryption): Là tập hợp các quy tắc giải mã có thể.

Chúng ta đã biết một thông báo thường được xem là bản rõ. Người gửi sẽ làm nhiệm vụ mã hoá bản rõ, kết quả thu được gọi là bản mã. Bản mã được gửi đi trên đường truyền tới người nhận. Người nhận giải mã để tìm hiểu nội dung bản rõ. Dễ dàng thấy được công việc trên khi định nghĩa hàm lập mã và hàm giải mã:

$$E_k(P) = C \quad \text{và} \quad D_k(C) = P$$

1.2.1.2 Những khả năng của hệ mật mã.

- Cung cấp một mức cao về tính bảo mật, tính toàn vẹn, chống chối bỏ và tính xác thực.
- Tính bảo mật: Bảo đảm bí mật cho các thông báo và dữ liệu bằng việc che dấu thông tin nhờ các kỹ thuật mã hoá.
- Tính toàn vẹn: Bảo đảm với các bên rằng bản tin không bị thay đổi trên đường truyền tin.
- Chống chối bỏ: Có thể xác nhận rằng tài liệu đã đến từ ai đó, ngay cả khi họ cố gắng từ chối nó.
- Tính xác thực: Cung cấp hai dịch vụ:
 - Nhận dạng nguồn gốc của một thông báo và cung cấp một vài bảo đảm rằng nó là đúng sự thực.
 - Kiểm tra định danh của người đang đăng nhập một hệ thống, tiếp tục kiểm tra đặc điểm của họ trong trường hợp ai đó cố gắng kết nối và giả danh là người sử dụng hợp pháp.

1.2.2 Các phương pháp mã hóa.

1.2.2.1. Mã hóa đối xứng

Hệ mã hoá đối xứng: là hệ mã hoá tại đó khoá mã hoá có thể “dễ” tính toán ra được từ khoá giải mã và ngược lại. Trong rất nhiều trường hợp, khoá mã hoá và khoá giải mã là giống nhau.

Thuật toán này có nhiều tên gọi khác nhau như thuật toán khoá bí mật, thuật toán khoá đơn giản, thuật toán một khoá. Thuật toán này yêu cầu người gửi và người nhận phải thoả thuận một khoá trước khi thông báo được gửi đi và khoá này phải được cất giữ bí mật. Độ an toàn của thuật toán này phụ thuộc vào khoá, nếu để lộ ra khoá này nghĩa là bất kỳ người nào cũng có thể mã hoá và giải mã thông báo trong hệ thống mã hoá. Sự mã hoá và giải mã của hệ mã hoá đối xứng biểu thị bởi:

$$E_k: P \rightarrow C \text{ Và } D_k: C \rightarrow P$$

Nơi ứng dụng: Sử dụng trong môi trường mà khoá đơn dễ dàng được chuyển, như là trong cùng một văn phòng. Cũng dùng để mã hoá thông tin khi lưu trữ trên đĩa nhớ.

Các vấn đề đối với Hệ mã hoá đối xứng:

- Phương pháp mã hoá đối xứng đòi hỏi người mã hoá và người giải mã phải cùng chung một khoá. Khoá phải được giữ bí mật tuyệt đối. "Dễ dàng" xác định một khoá nếu biết khoá kia và ngược lại.
- Hệ mã hoá đối xứng không an toàn nếu khoá bị lộ với xác suất cao. Hệ này khoá phải được gửi đi trên kênh an toàn.
- Vấn đề quản lý và phân phối khoá là khó khăn, phức tạp khi sử dụng hệ mã hoá đối xứng. Người gửi và người nhận phải luôn thống nhất với nhau về khoá. Việc thay đổi khoá là rất khó và dễ bị lộ.
- Khuynh hướng cung cấp khoá dài mà nó phải được thay đổi thường xuyên cho mọi người, trong khi vẫn duy trì cả tính an toàn lẫn hiệu quả chi phí, sẽ cản trở rất nhiều tới việc phát triển hệ mật mã.

1.2.2.2 Mã hóa phi đối xứng (Mã hóa công khai).

Hệ mã hoá khoá công khai: là Hệ mã hoá trong đó khoá mã hoá là khác với khoá giải mã. Khoá giải mã “khó” tính toán được từ khoá mã hoá và ngược lại. Khoá mã hoá gọi là khoá công khai (Public key). Khoá giải mã được gọi là khoá bí mật (Private key).

Nơi ứng dụng: Sử dụng chủ yếu trong việc trao đổi dữ liệu công khai.

Các điều kiện của một hệ mã hoá công khai:

Việc tính toán ra cặp khoá công khai K_B và bí mật k_B dựa trên cơ sở các điều kiện ban đầu, phải được thực hiện một cách dễ dàng, nghĩa là thực hiện trong thời gian đa thức.

Người gửi A có được khoá công khai của người nhận B và có bản tin P cần gửi B, thì có thể dễ dàng tạo ra được bản mã C.

$$C = E_{K_B}(P) = E_B(P)$$

Người nhận B khi nhận được bản mã C với khoá bí mật k_B , thì có thể giải mã bản tin trong thời gian đa thức.

$$P = D_{K_B}(C) = D_B[E_B(P)]$$

Nếu kẻ địch biết khoá công khai K_B cố gắng tính toán khoá bí mật thì chúng phải đương đầu với trường hợp nan giải, đó là gặp bài toán "khó".

1.2.3 Một số hệ mã hoá cụ thể.

1.2.3.1 Hệ mã hoá RSA.

Cho $n=p*q$ với p, q là số nguyên tố lớn. Đặt $P = C = Z_n$

Chọn b nguyên tố với $\phi(n)$, $\phi(n) = (p-1)(q-1)$

Ta định nghĩa: $K=\{(n,a,b): a*b \equiv 1(\text{mod } \phi(n))\}$

Giá trị n và b là công khai và a là bí mật

Với mỗi $K=(n, a, b)$, mỗi $x \in P, y \in C$ định nghĩa

Hàm mã hóa: $y = e_k(x) = x^b \text{ mod } n$

Hàm giải mã: $d_k(x) = y^a \text{ mod } n$

1.2.3.2 Hệ mã hoá ElGamal.

Hệ mã hóa với khoá công khai ElGamal có thể được dựa trên tùy ý các nhóm mà với họ đó bài toán lôgarit rời rạc được xem là “khó” giải được.

Thông thường người ta dùng nhóm con G_q (cấp q) của Z_p ; ở đó p, q là các số nguyên tố lớn thoả mãn $q|(p-1)$. Ở đây giới thiệu cách xây dựng nhóm Z_p , với p là một số nguyên tố lớn.

Sơ đồ:

Chọn số nguyên tố lớn p sao cho bài toán lôgarit rời rạc trong Z_p là “khó” (ít nhất $p = 10^{150}$). Chọn g là phần tử sinh trong Z_p^* .

Lấy ngẫu nhiên một số nguyên α thoả mãn $1 \leq \alpha \leq p-2$ và tính toán $h = g^\alpha \text{ mod } p$.

Khoá công khai chính là (p, g, h) , và khoá bí mật là α .

Mã hoá: khoá công khai là (p, g, h) muốn mã hoá thư tín m ($0 \leq m < p$)

Lấy ngẫu nhiên một số nguyên k , $0 \leq k \leq p-2$.

Tính toán $x = g^k \text{ mod } p$, $y = m * h^k \text{ mod } p$.

Giải mã. Để phục hồi được bản gốc m từ $c = (x, y)$, ta làm như sau:

Sử dụng khoá riêng α , tính toán $r = x^{p-1-\alpha}$.

(Chú ý rằng $r = x^{p-1-\alpha} = x^{-\alpha} = (gk)^{-\alpha} = g^{-k\alpha}$).

Phục hồi m bằng cách tính toán $m = y * r \bmod p$.

1.2.3.3. Mã hoá đồng cấu.

Xét một sơ đồ mã hoá xác suất. Giả sử P là không gian các văn bản chưa mã hoá và C là không gian các văn bản mật mã. Có nghĩa là P là một nhóm với phép toán 2 ngôi $\oplus$ và C là một nhóm với phép toán $\otimes$. Ví dụ E của sơ đồ mã hoá xác suất được hình thành bởi sự tạo ra khoá riêng và khoá công khai của nó. Giả sử $E_r(m)$ là sự mã hoá thư tín m sử dụng tham số (s) r ta nói rằng sơ đồ mã hoá xác suất là $(\oplus, \otimes)$ đồng cấu. Nếu với bất kỳ ví dụ E của sơ đồ này, ta cho $c_1 = E_{r1}(m_1)$ và $c_2 = E_{r2}(m_2)$ thì tồn tại r sao cho:

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

Chẳng hạn, sơ đồ mã hoá ElGamal là đồng cấu. Ở đây, P là tập tất cả các số nguyên modulo p ($P = Z_p$), còn $C = \{(a, b) \mid a, b \in Z_p\}$. Phép toán $\oplus$ là phép nhân modulo p . Đối với phép toán 2 ngôi $\otimes$ được định nghĩa trên các văn bản mật mã, ta dùng phép nhân modulo p trên mỗi thành phần.

Hai văn bản gốc m_0, m_1 được mã hoá:

$$E_{k0}(m_0) = (g^{k_0}, h^{k_0} m_0)$$

$$E_{k1}(m_1) = (g^{k_1}, h^{k_1} m_1)$$

Ở đó k_0, k_1 là ngẫu nhiên.

$$\text{Từ đó: } E_{k0}(m_0) E_{k1}(m_1) = (g^{k_0}, h^{k_0} m_0) (g^{k_1}, h^{k_1} m_1) = E_k(m_0 m_1)$$

$$\text{với } k = k_0 + k_1$$

Bởi vậy, trong hệ thống bí mật ElGamal từ phép nhân các văn bản mật mã chúng ta sẽ có được phép nhân đã được mã hoá của các văn bản gốc tương ứng.

1.2.3.4 Mã nhị phân.

Giả sử rằng Alice muốn gửi cho Bob 1 chữ số nhị phân b . Cô ta không muốn tiết lộ b cho Bob ngay. Bob yêu cầu Alice không được đổi ý, tức là chữ số mà sau đó Alice tiết lộ phải giống với chữ số mà cô ta nghĩ bây giờ.

Alice mã hoá chữ số b bằng một cách nào đó rồi gửi sự mã hoá cho Bob. Bob không thể phục hồi được b tới tận khi Alice gửi chìa khoá cho anh ta. Sự mã hoá của b được gọi là một blob.

Một cách tổng quát, sơ đồ mã nhị phân là một hàm $\xi: \{0, 1\} \times X \rightarrow Y$, trong đó X, Y là những tập hữu hạn. Mỗi mã hoá của b là giá trị $\xi(b, k)$, $k \in X$. Sơ đồ mã nhị phân phải thoả mãn những tính chất sau:

- Tính che đậy (Bob không thể tìm ra giá trị b từ $\xi(b, k)$)
- Tính mù (Alice sau đó có thể mở $\xi(b, k)$ bằng cách tiết lộ b, k thì được dùng trong cách xây dựng nó. Cô ta không thể mở blob bởi 0 hay 1).

Nếu Alice muốn mã hoá một xâu những chữ số nhị phân, cô ta mã hoá từng chữ số một cách độc lập.

Sơ đồ mã hoá số nhị phân mà trong đó Alice có thể mở blob bằng 0 hay 1 được gọi là mã hoá nhị phân cửa lật.

Mã hoá số nhị phân có thể được thực hiện như sau:

Giả sử một số nguyên tố lớn p , một phần tử sinh $g \in \mathbb{Z}_p$ và $G \in \mathbb{Z}_p$ đã biết logarit rời rạc cơ sở g của G thì cả Alice và Bob đều không biết (G có thể chọn ngẫu nhiên). Sự mã hoá nhị phân $\xi: \{0,1\} \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ là:

$$\xi(b, k) = g^k G^b$$

Đặt $\log_g G = a$. Blob có thể được mở bởi b bằng cách tiết lộ k và mở bởi $-b$ bằng cách tiết lộ $k-a$ nếu $b=0$ hoặc $k+a$ nếu $b=1$. Nếu Alice không biết a , cô ta không thể mở blob bằng $-b$.

Tương tự, nếu Bob không biết k , anh ta không thể xác định b với chỉ một dữ kiện $\xi(b, k) = g^k G^b$.

Sơ đồ mã hoá chữ số nhị phân của lậ đạt được trong trường hợp Alice biết a .

Nếu Bob biết a và Alice mở blob cho Bob thông qua kênh chống đột nhập đường truyền (untappable channel) Bob có thể sẽ nói dối với người thứ ba về sự mã hoá chữ số nhị phân b . Rất đơn giản, anh ta nói rằng anh ta nhận được $k+a$ hoặc $k+a$ (mà thực tế là k). Sơ đồ mã hoá số nhị phân mà cho phép người xác minh (Bob) nói dối về việc mở blob, được gọi là sự mã hoá nhị phân chameleon.

Thay vì mã hoá từng chữ số nhị phân trong sâu s một cách độc lập, Alice có thể mã hoá một cách đơn giản $0 \leq s \leq p$ bằng $\xi(b, k) = G^s g^k$.

Hơn nữa, những thông tin về số a sẽ cho Alice khả năng mở $\xi(s, k)$ bởi bất kì s', k' thoả mãn $as + k = as' + k'$.

1.3 KHÁI NIỆM VỀ KÝ ĐIỆN TỬ.

1.3.1 Định nghĩa.

Một sơ đồ chữ ký gồm bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

P là tập hữu hạn các bức điện (thông điệp) có thể

A là tập hữu hạn các chữ kí có thể

K không gian khoá là tập hữu hạn các khoá có thể

Sig_k là thuật toán ký $P \rightarrow A$

$x \in P \rightarrow y = Sig_k(x)$

Ver_k là thuật toán kiểm thử: $(P, A) \rightarrow (\text{Đúng}, \text{sai})$

$$Ver_k(x, y) = \begin{cases} \text{Đúng} & \text{Nếu } y = Sig_k(x) \\ \text{Sai} & \text{Nếu } y \neq Sig_k(x) \end{cases}$$

1.3.2 Phân loại sơ đồ chữ ký điện tử.

Chữ ký “điện tử” được chia làm 2 lớp, lớp chữ ký kèm thông điệp (message appendix) và lớp chữ ký khôi phục thông điệp (message recovery).

Chữ ký kèm thông điệp: Đòi hỏi thông điệp ban đầu là đầu vào của giải thuật kiểm tra. Ví dụ: chữ ký Elgamal.

Chữ ký khôi phục thông điệp: Thông điệp ban đầu sinh ra từ bản thân chữ ký. Ví dụ: chữ ký RSA.

1.3.3 Một số sơ đồ ký số cơ bản.

1.3.3.1 Sơ đồ chữ ký Elgamal.

Chọn p là số nguyên tố sao cho bài toán log rời rạc trong Z_p là khó.

Chọn g là phần tử sinh $\in Z_p^*$; $a \in Z_p^*$.

Tính $\beta \equiv g^a \pmod{p}$.

Chọn r ngẫu nhiên $\in Z_{p-1}^*$

Ký trên x : $\text{Sig}(x) = (\gamma, \delta)$,

Trong đó $\gamma = g^k \pmod{p}$, $\delta = (x - a\gamma) r^{-1} \pmod{(p-1)}$.

Kiểm tra chữ ký:

$\text{Ver}(x, \gamma, \delta) = \text{True} \Leftrightarrow \beta^\gamma \gamma^\delta \equiv g^x \pmod{p}$

Ví dụ:

Chọn $p=463$; $g=2$; $a=211$;

$\beta \equiv 2^{211} \pmod{463} = 249$;

chọn $r=235$; $r^{-1}=289$

Ký trên $x = 112$

$\text{Sig}(x, r) = \text{Sig}(112, 235) = (\gamma, \delta) = (16, 108)$

$\gamma = 2^{235} \pmod{463} = 16$

$\delta = (112 - 211 \cdot 16) \cdot 289 \pmod{(463-1)} = 108$

Kiểm tra chữ ký:

$\text{Ver}(x, \gamma, \delta) = \text{True} \Leftrightarrow \beta^\gamma \gamma^\delta \equiv g^x \pmod{p}$

$\beta^\gamma \gamma^\delta = 249^{16} \cdot 16^{108} \pmod{463} = 132$

$g^x \pmod{p} = 2^{112} \pmod{463} = 132$

1.3.3.2 Sơ đồ chữ ký RSA.

Chọn p, q nguyên tố lớn .

Tính $n=p.q; \phi(n)=(p-1)(q-1)$.

Chọn b nguyên tố cùng $\phi(n)$.

Chọn a nghịch đảo với $b; a=b^{-1} \bmod \phi(n)$.

Ký trên x :

$$\text{Sig}(x) = x^a \bmod n$$

Kiểm tra chữ ký:

$$\text{Ver}(x,y) = \text{True} \Leftrightarrow x \equiv y^b \bmod n$$

Ví dụ:

$$p=3; q=5;$$

$$n=15; \phi(n)= 8;$$

$$\text{chọn } b=3; a=3$$

Ký $x=2$:

Chữ ký :

$$y = x^a \bmod n = 2^3 \bmod 15=8$$

Kiểm tra:

$$x = y^b \bmod n = 8^3 \bmod 15 =2 \text{ (chữ ký đúng)}$$

1.3.3.3 Sơ đồ chữ ký Schnorr.**Chuẩn bị:**

Lấy G là nhóm con cấp q của Z_n^* , với q là số nguyên tố.

Chọn phần tử sinh $g \in G$ sao cho bài toán logarit trên G là khó giải.

Chọn $x \neq 0$ làm khóa bí mật, $x \in Z_q$. Tính $y = g^x$ làm khóa công khai.

Lấy H là hàm băm không va chạm.

Ký trên thông điệp m :

Chọn r ngẫu nhiên thuộc Z_q

Tính $c = H(m, g^r)$

Tính $s = (r - c x) \bmod q$

Chữ ký Schnorr là cặp (c, s)

Kiểm tra chữ ký:

Với một văn bản m cho trước, một cặp (c, s) được gọi là một chữ ký Schnorr hợp lệ nếu thỏa mãn phương trình:

$$c = H(m, g^{s*y^c})$$

Đề ý rằng ở đây, c xuất hiện ở cả 2 vế của phương trình

1.4 VẤN ĐỀ XÁC THỰC.

1.4.1 Khái niệm xác thực

Xác thực là việc xác minh, kiểm tra một thông tin để công nhận hoặc bác bỏ tính hợp lệ của thông tin đó. Xác thực luôn là yêu cầu quan trọng trong các giao tiếp cần có sự tin cậy. Để đơn giản xét mô hình giao tiếp gồm hai thực thể trao đổi thông tin A và B, họ cùng mục đích trao đổi thông tin M nào đó.

Khi đó việc xác thực bao gồm:

- A cần xác minh B đúng là B và ngược lại.
- Cả A và B cần xác minh tính an toàn của thông tin M mà họ trao đổi.

Như vậy, xác thực bao gồm hai việc chính:

- Xác thực tính hợp lệ của các thực thể tham gia giao tiếp.
- Xác thực tính bảo mật và toàn vẹn của thông tin trao đổi.

Theo phương pháp truyền thống, việc thực hiện xác thực thực thể được thực thi bằng các giấy tờ như: chứng minh thư, giấy phép lái xe, hoặc các giấy tờ cá nhân khác. Việc xác thực tính an toàn của thông tin thường dựa trên chữ ký, con dấu.

1.4.2 Khái niệm xác thực số (điện tử).

Xác thực điện tử là việc chứng minh từ xa bằng phương tiện điện tử, sự tồn tại chính xác và hợp lệ danh tính của một chủ thể khi tham gia trao đổi thông tin điện tử như: các nhân, tổ chức, dịch vụ,... hoặc một lớp thông tin nào đó mà không cần biết các thông tin đó cụ thể như thế nào, thông qua thông tin đặc trưng đại diện cho chủ thể đó mà vẫn đảm bảo được bí mật của chủ thể, hoặc lớp thông tin cần chứng minh.

Xác thực điện tử là việc cần thực hiện trước khi thực sự diễn ra các cuộc trao đổi thông tin điện tử chính thức.

Việc xác thực điện tử trong hệ thống trao đổi thông tin điện tử được uỷ quyền cho một bên thứ ba tin cậy. Bên thứ ba ấy chính là CA (Certification Authority), một cơ quan có tư cách pháp nhân thường xuyên tiếp nhận đăng ký các thông tin đặc trưng đại diện cho chủ thể: khoá công khai và lưu trữ khoá công khai cùng lý lịch của chủ thể trong một cơ sở dữ liệu được bảo vệ chặt chẽ. CA chuyên nghiệp không nhất thiết là cơ quan nhà nước. Điều quan trọng nhất của một CA là uy tín để khẳng định sự thật, bảo đảm không thể có chuyện "đổi trắng thay đen".

Mục đích của việc xác thực điện tử: chống giả mạo, chống chối bỏ, đảm bảo tính toàn vẹn, tính bí mật, tính xác thực của thông tin và mục đích cuối cùng là hoàn thiện các giải pháp an toàn thông tin.

Cơ sở ứng dụng đề xây dựng các giải pháp an toàn cho xác thực điện tử là các hệ mật mã.

Ứng dụng trong: thương mại điện tử, trong các hệ thống thanh toán trực tuyến, là nền tảng của chính phủ điện tử.

Hiện nay, xác thực điện tử được sử dụng trong khá nhiều ứng dụng, theo số liệu điều tra công bố vào tháng 8/2003 của tổ chức OASIS (Organization for the Advancement of Structured Information Standard):

- 24,1% sử dụng trong việc ký vào các dữ liệu điện tử;
- 16,3% sử dụng để đảm bảo cho e-mail;
- 13,2% dùng trong thương mại điện tử;
- 9,1% sử dụng để bảo vệ WLAN;
- 8% sử dụng đảm bảo an toàn cho các dịch vụ web;
- 6% sử dụng bảo đảm an toàn cho Web Server;
- 6% sử dụng trong các mạng riêng ảo...

Có nhiều phương pháp xác thực điện tử đã được phát triển. Tuy nhiên có 3 phương pháp xác thực chính sau đây:

a. Phương pháp thứ nhất: Xác thực dựa vào những gì mà ta “*biết*”

Phương pháp này thường sử dụng mật khẩu, mã PIN để xác thực chủ thể. Khi cần xác thực, hệ thống yêu cầu chủ thể cung cấp những thông tin mà chủ thể biết (mật khẩu, mã PIN, ...).

b. Phương pháp thứ hai: Xác thực dựa vào những gì mà ta “*có*”.

Phương pháp này đòi hỏi người dùng phải sở hữu một thứ gì đó để có thể xác nhận, chẳng hạn như chứng chỉ số, thẻ ATM, thẻ SIM.

c. Phương pháp thứ ba: Xác thực những gì mà ta “*đại diện*”.

Phương pháp này thường sử dụng việc nhận dạng sinh học như dấu vân tay, mẫu võng mạc, mẫu giọng nói, ... để xác thực.

Xác thực bằng mật khẩu, mã PIN có ưu điểm là tạo lập và sử dụng đơn giản, nhưng có nhược điểm lớn là người dùng thường chọn mật khẩu dễ nhớ, do vậy dễ đoán nên dễ bị tấn công. Kẻ tấn công cũng có nhiều phương pháp tấn công để đạt được mật khẩu.

1.4.3 Công cụ xác thực: Chứng chỉ số.

1.4.3.1 Khái niệm chứng chỉ số (*Digital Certificate*).

Chứng chỉ số là một trong số các công cụ để thực hiện bảo toàn và bảo mật trong hệ thống thông tin.

Như đã trình bày, việc sử dụng hệ mã hoá khoá công khai trong bảo mật thông tin là rất quan trọng. Tuy nhiên, có vấn đề nảy sinh là nếu hai người không biết nhau, nhưng muốn tiến hành giao dịch, thì làm sao họ có thể có khoá công khai của nhau. Giả sử ông A muốn giao tiếp với ông B, ông ta sẽ vào website của ông B để lấy khoá công khai. Ông A gõ địa chỉ URL của ông B trên trình duyệt, tìm DNS của trang Web và gửi yêu cầu của ông A. Nhưng không may, kẻ giả mạo **B'** lại nhận yêu cầu của A và trả về trang Web của **B'** là bản sao của B, hoàn toàn giống trang web của B, khiến cho A không thể phát hiện được. Lúc này A có khoá công khai của **B'**, chứ không phải là của B. Ông A mã hoá thông điệp bằng khoá công khai của **B'**. Kẻ gian **B'** giải mã thông điệp, đọc thông tin, mã hóa lại bằng khoá công khai của B, và gửi thông điệp cho B. Như vậy cả A và B hoàn toàn không biết có kẻ thứ 3 là **B'** đã đọc được nội dung của thông điệp. Trường hợp xấu hơn, **B'** sẽ thay đổi nội dung thông điệp của A trước khi gửi cho B.

Bài toán đặt ra là phải có một giải pháp để đảm bảo rằng khoá công khai được trao đổi an toàn, không có giả mạo.

Để giải quyết vấn đề này cần có một tổ chức cung cấp chứng nhận, nó xác nhận: khoá công khai này thuộc về một người, công ty hay tổ chức nào đó. Tổ chức cung cấp các chứng nhận khoá công khai được gọi là **CA** (Certification Authority), và chứng nhận này gọi là chứng chỉ số.

Với bài toán trên, ông B muốn cho phép A và những người khác giao tiếp với mình, ông ta phải đến một tổ chức **CA** để xin giấy chứng nhận khoá công khai của ông ta. Nhà cung cấp sẽ phát hành chứng nhận và chữ ký số của nhà cung cấp. Nhiệm vụ chính của nhà cung cấp CA là gắn kết khoá công khai với tên của người đăng ký (cá nhân, công ty hay tổ chức) sở hữu khoá đó.

Chứng chỉ số là một văn bản điện tử theo định dạng chuẩn nhất định, dùng để xác minh danh tính một cá nhân, một công ty, ... hay thực thể nào đó trên mạng truyền thông công cộng, cùng với khoá công khai của họ trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có chứng minh thư, ta phải được cơ quan Công An sở tại cấp. Chứng chỉ số cũng vậy, phải do một tổ chức đứng ra chứng nhận những thông tin của ta là chính xác, được gọi là Nhà cung cấp chứng chỉ số (Certification Authority, viết tắt là CA). CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà họ cấp.

Trong chứng chỉ số có ba thành phần chính:

Thông tin cá nhân:

Đây là các thông tin của đối tượng được cấp chứng chỉ số, gồm tên, quốc tịch, địa chỉ, điện thoại, email, tên tổ chức .v.v. Phần này giống như các thông tin trên chứng minh thư của mỗi người.

Khoá công khai:

Trong mật mã, khoá công khai là một giá trị được CA chứng thực, đó là khoá mã hoá, kết hợp với khoá bí mật duy nhất được tạo ra từ khoá công khai, để tạo thành cặp khoá mật mã bất đối xứng.

Chữ ký số của CA cấp chứng chỉ:

Đây chính là sự xác nhận của CA, bảo đảm tính chính xác và hợp lệ của chứng chỉ. Muốn kiểm tra một chứng chỉ số, trước tiên phải kiểm tra chữ ký số của CA có hợp lệ hay không.

Trong cơ sở hạ tầng mật mã khoá công khai (Public Key Infrastructure - PKI), CA sẽ kiểm soát cùng với nhà quản lý đăng ký (Registration Authority - RA), để xác minh thông tin về chứng chỉ số mà người ta yêu cầu xác thực. RA xác nhận thông tin của người cần xác thực, CA sau đó sẽ cấp chứng chỉ.

1.4.3.2 Định dạng X.509 của chứng chỉ số.

Cơ sở hạ tầng của mật mã khóa công khai (PKI) được xây dựng để bảo đảm an toàn thông tin. Trong hệ thống này, người ta sử dụng một thành phần dữ liệu được gọi là chứng chỉ số, nó gắn thông tin về người sở hữu khóa riêng với khóa công khai tương ứng.

Hình 1.1 mô tả chứng chỉ số phiên bản 3, được định nghĩa theo chuẩn X.509, chuẩn được sử dụng phổ biến trên thế giới hiện nay.

Các thành viên tham gia hệ thống, sử dụng hệ mật mã khóa công khai hoàn toàn có thể tin rằng: Khóa công khai chứa trong chứng chỉ số là thuộc về đối tượng có thông tin trong trường đối tượng được cấp. CA sử dụng chữ ký điện tử để đảm bảo tính toàn vẹn và xác thực các thông tin có trong chứng chỉ số.

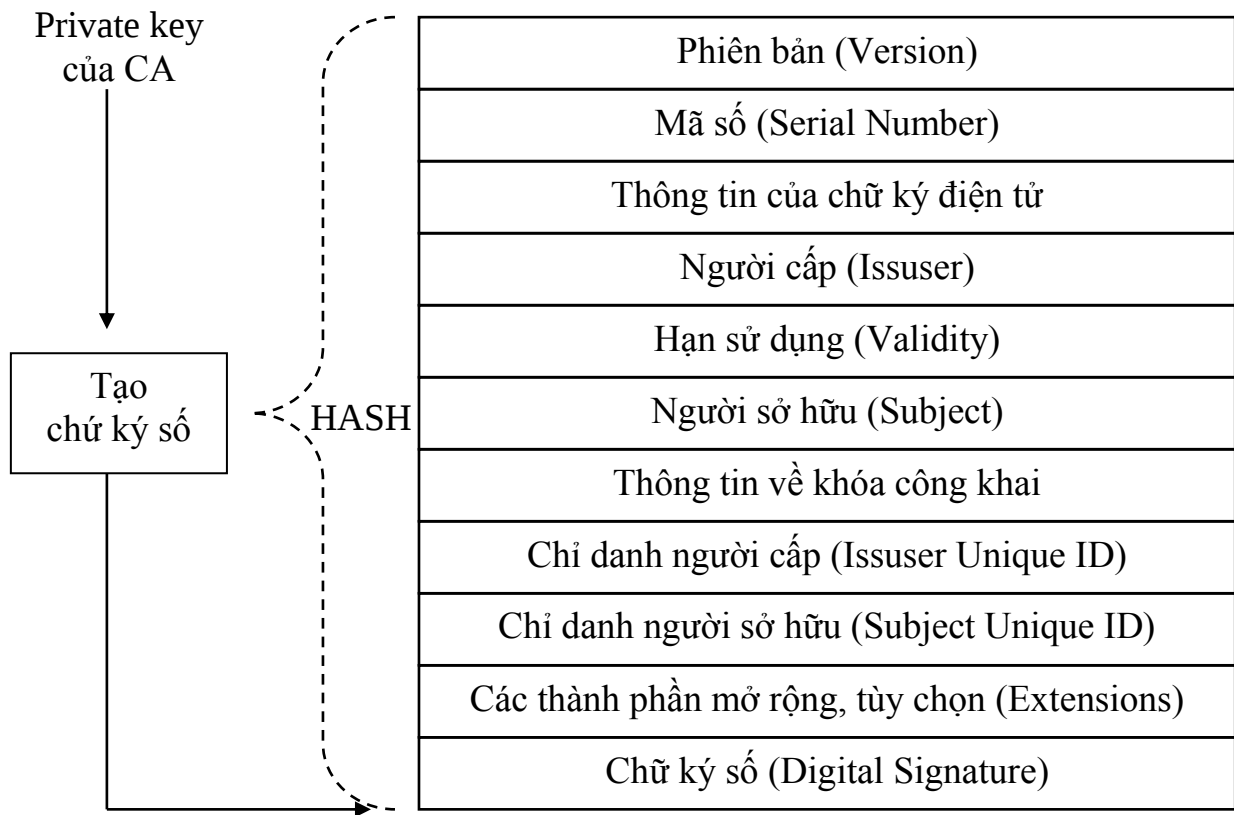
Chữ ký được tạo ra như sau:

Thiết lập đại diện của toàn bộ thông tin trong chứng chỉ số (gồm các thông tin cơ bản và phần mở rộng).

CA sử dụng khóa riêng (private key) của mình ký trên đại diện vừa có được, để tạo ra chữ ký số.

Đóng gói các thông tin cùng với chữ ký trên, đó là chứng chỉ

Sự tin tưởng của các thành viên chỉ có thể được đảm bảo khi họ tin tưởng vào CA đã tạo ra chứng chỉ đó. Mỗi chứng chỉ số đều có hạn sử dụng. Việc kiểm tra chứng chỉ số được thực hiện độc lập với hệ thống cấp chứng chỉ, nó được thực hiện tại đầu cuối, hoặc thông qua các dịch vụ kiểm tra trạng thái của chứng chỉ số. Chứng chỉ số có thể công khai.

Các trường cơ bản của một chứng chỉ số**Hình 1.1: Chứng chỉ số theo chuẩn X.509**

CHƯƠNG 2. GIAO DỊCH ĐIỆN TỬ

2.1 THƯƠNG MẠI ĐIỆN TỬ

2.1.1 Khái niệm

Thương mại điện tử là hình thức mua bán hàng hóa và dịch vụ thông qua mạng máy tính toàn cầu. Thương mại điện tử theo nghĩa rộng được định nghĩa trong luật mẫu về Thương mại điện tử của Ủy ban Liên Hợp quốc về Luật Thương mại Quốc tế (UNCITRAL):

“Thuật ngữ Thương mại cần được diễn giải theo nghĩa rộng để bao quát các vấn đề phát sinh từ mọi quan hệ mang tính chất thương mại dù có hay không có hợp đồng. Các quan hệ mang tính thương mại bao gồm các giao dịch sau đây: bất cứ giao dịch thương mại nào về cung cấp hoặc trao đổi hàng hóa hoặc dịch vụ; thỏa thuận phân phối; đại diện hoặc đại lý thương mại, ủy thác hoa hồng; cho thuê dài hạn; xây dựng các công trình; tư vấn; kỹ thuật công trình; đầu tư; cấp vốn; ngân hàng; bảo hiểm; thỏa thuận khai thác; liên doanh các hình thức khác về hợp tác công nghiệp hoặc kinh doanh; chuyên chở hàng hóa hay hành khách bằng đường biển, đường không, đường sắt hoặc đường bộ.”

Như vậy có thể thấy rằng phạm vi của Thương mại điện tử rất rộng, bao quát hầu hết các lĩnh vực hoạt động kinh tế, việc mua bán hàng hóa và dịch vụ chỉ là một trong hàng ngàn lĩnh vực áp dụng của Thương mại điện tử. Theo nghĩa hẹp Thương mại điện tử chỉ gồm các hoạt động thương mại được tiến hành trên mạng máy tính mở như Internet. Trên thực tế, chính các hoạt động thương mại thông qua mạng Internet đã làm phát sinh thuật ngữ Thương mại điện tử.

Thương mại điện tử bao gồm các hoạt động mua bán hàng hóa và dịch vụ qua phương tiện điện tử, giao nhận các nội dung kỹ thuật số trên mạng, chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn điện tử, đấu giá thương mại, hợp tác thiết kế, tài nguyên mạng, mua sắm công cộng, tiếp thị trực tuyến tới người

tiêu dùng và các dịch vụ sau bán hàng. Thương mại điện tử được thực hiện đối với cả thương mại hàng hóa và thương mại dịch vụ; các hoạt động truyền thống và các hoạt động mới. Thương mại điện tử đang trở thành một cuộc cách mạng làm thay đổi cách thức mua sắm của con người.

2.1.2 Các đặc trưng của Thương mại điện tử

So với các hoạt động Thương mại truyền thống, Thương mại điện tử có một số điểm khác biệt cơ bản sau:

- Các bên tiến hành giao dịch trong thương mại điện tử không tiếp xúc trực tiếp với nhau và không đòi hỏi phải biết nhau từ trước.

Trong Thương mại truyền thống, các bên thường gặp gỡ nhau trực tiếp để tiến hành giao dịch. Các giao dịch được thực hiện chủ yếu theo nguyên tắc vật lý như chuyển tiền, séc, hóa đơn, vận đơn, gửi báo cáo. Các phương tiện viễn thông như fax, telex... chỉ được dùng để trao đổi số liệu kinh doanh. Tuy nhiên, việc sử dụng phương tiện điện tử trong thương mại truyền thông chỉ để chuyển tải thông tin một cách trực tiếp giữa hai đối tác của cùng một giao dịch.

Thương mại điện tử cho phép mọi người cùng tham gia từ các vùng xa xôi hẻo lánh đến các khu vực đô thị lớn, tạo điều kiện cho tất cả mọi người ở khắp mọi nơi đều có cơ hội ngang nhau tham gia vào thị trường giao dịch toàn cầu và không đòi hỏi nhất thiết phải có mối quen biết với nhau.

- Các giao dịch thương mại truyền thống được thực hiện với sự tồn tại của khái niệm biên giới quốc gia, còn Thương mại điện tử được thực hiện trong một thị trường không có biên giới (thị trường thống nhất toàn cầu). Thương mại điện tử trực tiếp tác động tới môi trường cạnh tranh toàn cầu.

Thương mại điện tử ngày càng phát triển, thì máy tính cá nhân trở thành cửa sổ cho doanh nghiệp hướng ra thị trường khắp thế giới. Với Thương mại điện tử, một doanh nhân dù mới thành lập đã có thể kinh doanh ở các nước khác nhau mà không hề phải bước ra khỏi nhà, một công việc trước kia phải mất nhiều năm.

- Trong hoạt động giao dịch Thương mại điện tử đều có sự tham gia của ít nhất ba chủ thể, trong đó có một bên không thể thiếu là người cung cấp dịch vụ mạng, các cơ quan chứng thực.

Trong Thương mại điện tử, ngoài các chủ thể tham gia quan hệ giao dịch giống như giao dịch thương mại truyền thống đã xuất hiện một bên thứ ba đó là nhà cung cấp dịch vụ mạng, các cơ quan chứng thực... là những người tạo môi trường cho các giao dịch Thương mại điện tử. Nhà cung cấp dịch vụ mạng và cơ quan chứng thực có nhiệm vụ chuyển đi, lưu giữ các thông tin giữa các bên tham gia giao dịch, đồng thời họ cũng xác nhận độ tin cậy của các thông tin trong giao dịch.

- Đối với thương mại truyền thống thì mạng lưới thông tin chỉ là phương tiện để trao đổi dữ liệu, còn với Thương mại điện tử thì mạng lưới thông tin chính là thị trường.

Thông qua Thương mại điện tử, nhiều loại hình kinh doanh mới được hình thành. Ví dụ: các dịch vụ gia tăng giá trị trên mạng máy tính hình thành nên các nhà trung gian ảo là các dịch vụ môi giới cho giới kinh doanh và tiêu dùng; các siêu thị ảo được hình thành để cung cấp hàng hóa và dịch vụ trên mạng máy tính.

Các trang Web khá nổi tiếng như Yahoo! America Online hay Google đóng vai trò quan trọng cung cấp thông tin trên mạng. Với mỗi lần nhấn chuột, khách hàng có khả năng truy cập vào hàng ngàn cửa hàng ảo khác nhau và tỷ lệ khách hàng vào hàng ngàn các cửa hàng ảo khác. Người tiêu dùng đã bắt đầu mua trên mạng một số các loại hàng trước đây được coi là khó bán trên mạng. Nhiều người sẵn sàng trả thêm một chút tiền còn hơn là phải đi tới tận cửa hàng. Một số công ty đã mời khách may đo quần áo trên mạng, tức là khách hàng chọn kiểu, gửi số đo theo hướng dẫn tới cửa hàng (qua Internet) rồi sau một thời gian nhất định nhận được bộ quần áo theo đúng yêu cầu của mình. Điều tưởng như không thể thực hiện được này cũng có rất nhiều người hưởng ứng.

Các chủ cửa hàng thông thường ngày nay cũng đang đua nhau đưa thông tin lên Web để tiến tới khai thác mảng thị trường rộng lớn trên Web bằng cách mở cửa hàng ảo.

2.1.3 Các cơ sở để phát triển Thương mại điện tử

Để phát triển TMĐT cần phải có hội đủ một số cơ sở:

- Hạ tầng kỹ thuật internet phải đủ nhanh, mạnh đảm bảo truyền tải các nội dung thông tin bao gồm âm thanh, hình ảnh trung thực và sống động. Một hạ tầng internet mạnh cho phép cung cấp các dịch vụ như xem phim, xem TV, nghe nhạc v.v. trực tiếp. Chi phí kết nối internet phải rẻ để đảm bảo số người dùng internet phải lớn.
- Hạ tầng pháp lý: phải có luật về TMĐT công nhận tính pháp lý của các chứng từ điện tử, các hợp đồng điện tử ký qua mạng; phải có luật bảo vệ quyền sở hữu trí tuệ, bảo vệ sự riêng tư, bảo vệ người tiêu dùng v.v. để điều chỉnh các giao dịch qua mạng.
- Phải có cơ sở thanh toán điện tử an toàn bảo mật. Thanh toán điện tử qua thẻ, qua tiền điện tử, thanh toán qua EDI. Các ngân hàng phải triển khai hệ thống thanh toán điện tử rộng khắp.
- Phải có hệ thống cơ sở chuyển phát hàng nhanh chóng, kịp thời và tin cậy.
- Phải có hệ thống an toàn bảo mật cho các giao dịch, chống xâm nhập trái phép, chống virus, chống thoái thác.
- Phải có nhân lực am hiểu kinh doanh, công nghệ thông tin, thương mại điện tử để triển khai tiếp thị, quảng cáo, xúc tiến, bán hàng và thanh toán qua mạng.

2.1.4 Các loại hình giao dịch Thương mại điện tử

Trong TMĐT có ba chủ thể tham gia: Doanh nghiệp (B) giữ vai trò động lực phát triển TMĐT, người tiêu dùng (C) giữ vai trò quyết định sự thành công của TMĐT và chính phủ (G) giữ vai trò định hướng, điều tiết và quản lý. Từ các mối quan hệ giữa các chủ thể trên ta có các loại giao dịch TMĐT: B2B, B2C,

B2G, C2G, C2C ... trong đó B2B và B2C là hai loại hình giao dịch TMĐT quan trọng nhất.

2.1.4.1 Business-to-business (B2B) : Mô hình TMĐT giữa các doanh nghiệp với doanh nghiệp.

TMĐT B2B (Business-to-business) là việc thực hiện các giao dịch giữa các doanh nghiệp với nhau trên mạng. Thường gọi là giao dịch B2B. Các bên tham gia giao dịch B2B gồm: người trung gian trực tuyến (ảo hoặc click-and-mortar) người mua và người bán. Các loại giao dịch B2B gồm: mua ngay theo yêu cầu khi giá cả thích hợp và mua theo hợp đồng dài hạn, dựa trên đàm phán cá nhân giữa người mua và người bán.

Các loại giao dịch B2B cơ bản:

- Bên Bán — (một bên bán nhiều bên mua) là mô hình dựa trên công nghệ web trong đó một công ty bán cho nhiều công ty mua. Có 3 phương pháp bán trực tiếp trong mô hình này: Bán từ catalog điện tử, Bán qua quá trình đấu giá, Bán theo hợp đồng cung ứng dài hạn đã thoả thuận trước. Công ty bán có thể là nhà sản xuất loại click-and-mortar hoặc nhà trung gian thông thường là nhà phân phối hay đại lý.
- Bên Mua — một bên mua nhiều bên bán.
- Sàn Giao Dịch — nhiều bên bán - nhiều bên mua .
- TMĐT phối hợp — Các đối tác phối hợp nhau ngay trong quá trình thiết kế chế tạo sản phẩm.

2.1.4.2 Business-to-consumer (B2C): Mô hình TMĐT giữa doanh nghiệp và người tiêu dùng.

Đây là mô hình bán lẻ trực tiếp đến người tiêu dùng. Trong TMĐT, bán lẻ điện tử có thể từ nhà sản xuất, hoặc từ một cửa hàng thông qua kênh phân phối. Hàng hoá bán lẻ trên mạng thường là hàng hoá, máy tính, đồ điện tử, dụng cụ thể thao, đồ dùng văn phòng, sách và âm nhạc, đồ chơi, sức khỏe và mỹ phẩm, giải trí v.v...

Mô hình kinh doanh bán lẻ có thể phân loại theo quy mô các loại hàng hoá bán (Tổng hợp, chuyên ngành), theo phạm vi địa lý (toàn cầu , khu vực), theo kênh bán (bán trực tiếp, bán qua kênh phân phối).

Một số hình thức các cửa hàng bán lẻ trên mạng: Brick-and-mortar là loại cửa hàng bán lẻ kiểu truyền thống, không sử dụng Internet, Click-and-mortar là loại cửa hàng bán lẻ truyền thống nhưng có kênh bán hàng qua mạng và cửa hàng ảo là cửa hàng bán lẻ hoàn toàn trên mạng mà không sử dụng kênh bán truyền thống.

Hai loại giao dịch trên là giao dịch cơ bản của TMĐT. Ngoài ra trong TMĐT người ta còn sử dụng các loại giao dịch: Govement-to-Business (G2B) là mô hình TMĐT giữa doanh nghiệp với cơ quan chính phủ, Government-to-citizens (G2C) là mô hình TMĐT giữa các cơ quan chính phủ và công dân còn gọi là chính phủ điện tử, consumer-to-consumer (C2C) là mô hình TMĐT giữa các người tiêu dùng và mobile commerce (m-commerce) là TMĐT thực hiện qua điện thoại di động.

2.1.5 Các hình thức hoạt động chủ yếu của Thương mại điện tử

2.1.5.1 Thư điện tử

Các doanh nghiệp, các cơ quan Nhà nước,.. sử dụng thư điện tử để gửi thư cho nhau một cách “trực tuyến” thông qua mạng, gọi là thư điện tử (electronic mail, viết tắt là e-mail). Thông tin trong thư điện tử không phải tuân theo một cấu trúc định trước nào.

2.1.5.2 Thanh toán điện tử

Thanh toán điện tử (electronic payment) là việc thanh toán tiền thông qua bức thư điện tử (electronic message) ví dụ, trả lương bằng cách chuyển tiền trực tiếp vào tài khoản, trả tiền mua hàng bằng thẻ mua hàng, thẻ tín dụng v.v.. thực chất đều là dạng thanh toán điện tử. Ngày nay, với sự phát triển của TMĐT, thanh toán điện tử đã mở rộng sang các lĩnh vực mới đó là:

a. Trao đổi dữ liệu điện tử tài chính (Financial Electronic Data Interchange, gọi tắt là FEDI) chuyên phục vụ cho việc thanh toán điện tử giữa các công ty giao dịch với nhau bằng điện tử.

b. Tiền lẻ điện tử (Internet Cash) là tiền mặt được mua từ một nơi phát hành (ngân hàng hoặc một tổ chức tín dụng nào đó), sau đó được chuyển đổi tự do sang các đồng tiền khác thông qua Internet, áp dụng trong cả phạm vi một nước cũng như giữa các quốc gia; tất cả đều được thực hiện bằng kỹ thuật số hóa, vì thế tiền mặt này còn có tên gọi là “tiền mặt số hóa” (digital cash). Tiền lẻ điện tử đang trên đà phát triển nhanh, nó có ưu điểm nổi bật sau:

- + Dùng để thanh toán những món hàng giá trị nhỏ, thậm chí ngay cả tiền mua báo (vì phí giao dịch mua hàng và chuyển tiền rất thấp);
- + Có thể tiến hành giữa hai người hoặc hai công ty bất kỳ, các thanh toán là vô danh;
- + Tiền mặt nhận được đảm bảo là tiền thật, tránh được tiền giả.

c. Ví điện tử (electronic purse); là nơi để tiền mặt Internet, chủ yếu là thẻ thông minh (smart card), còn gọi là thẻ giữ tiền (stored value card), tiền được trả cho bất kỳ ai đọc được thẻ đó; kỹ thuật của túi tiền điện tử tương tự như kỹ thuật áp dụng cho “tiền lẻ điện tử”. Thẻ thông minh, nhìn bề ngoài như thẻ tín dụng, nhưng ở mặt sau của thẻ, có một chip máy tính điện tử có một bộ nhớ để lưu trữ tiền số hóa, tiền ấy chỉ được “chi trả” khi sử dụng hoặc thư yêu cầu (như xác nhận thanh toán hóa đơn) được xác thực là “đúng”.

d. Giao dịch điện tử của ngân hàng (digital banking). Hệ thống thanh toán điện tử của ngân hàng là một hệ thống lớn gồm nhiều hệ thống nhỏ:

- (1) Thanh toán giữa ngân hàng với khách hàng qua điện thoại, tại các điểm bán lẻ, các kiốt, giao dịch cá nhân tại các gia đình, giao dịch tại trụ sở khách hàng, giao dịch qua Internet, chuyển tiền điện tử, thẻ tín dụng, thông tin hỏi đáp...
- (2) Thanh toán giữa ngân hàng với các đại lý thanh toán (nhà hàng, siêu

thị...,)

(3) Thanh toán nội bộ một hệ thống ngân hàng.

(4) Thanh toán liên ngân hàng .

2.1.5.3 Trao đổi dữ liệu điện tử

Trao đổi dữ liệu điện tử (electronic data interchange, viết tắt là EDI) là việc trao đổi các dữ liệu dưới dạng “có cấu trúc” (structured form), từ máy tính điện tử này sang máy tính điện tử khác, giữa các công ty hoặc đơn vị đã thỏa thuận buôn bán với nhau.

Theo Ủy ban liên hợp quốc về luật thương mại quốc tế (UNCITRAL), “Trao đổi dữ liệu điện tử (EDI) là việc chuyển giao thông tin từ máy tính điện tử này sang máy tính điện tử khác bằng phương tiện điện tử, có sử dụng một tiêu chuẩn đã được thỏa thuận để cấu trúc thông tin”.

EDI ngày càng được sử dụng rộng rãi trên toàn cầu, chủ yếu phục vụ cho việc mua và phân phối hàng (gửi đơn hàng, các xác nhận, các tài liệu gửi hàng, hóa đơn v.v...), người ta cũng dùng cho các mục đích khác, như thanh toán tiền khám bệnh, trao đổi các kết quả xét nghiệm v.v.

Trước khi có Internet đã có EDI, khi đó người ta dùng “mạng giá trị gia tăng” (Value Added Network, viết tắt là VAN) để liên kết các đối tác EDI với nhau; cốt lõi của VAN là một hệ thống thư điện tử cho phép các máy tính điện tử liên lạc được với nhau, và hoạt động như một phương tiện lưu trữ và tìm kiếm; khi nối vào VAN, một doanh nghiệp có thể liên lạc với nhiều máy tính điện tử nằm ở nhiều thành phố trên khắp thế giới.

Ngày nay EDI chủ yếu được thực hiện thông qua mạng Internet. Để phục vụ cho buôn bán giữa các doanh nghiệp thuận lợi hơn với chi phí truyền thông không quá tốn kém, người ta đã xây dựng một kiểu mạng mới gọi là “mạng riêng ảo” (virtual private network), là mạng riêng dạng Intranet của một doanh

ngành nhưng được thiết lập dựa trên chuẩn trang Web và truyền thông qua mạng Internet.

Công việc trao đổi EDI trong TMĐT thường gồm các nội dung sau: 1/ Giao dịch kết nối. 2/ Đặt hàng. 3/ Giao dịch gửi hàng. 4/ Thanh toán .

Vấn đề này đang được tiếp tục nghiên cứu và xử lý, đặc biệt là buôn bán giữa các nước có quan điểm chính sách, và luật pháp thương mại khác nhau, đòi hỏi phải có một pháp lý chung trên nền tảng thống nhất quan điểm về tự do hóa thương mại và tự do hóa việc sử dụng mạng Internet, chỉ như vậy mới bảo đảm được tính khả thi, tính an toàn, và tính có hiệu quả của việc trao đổi dữ liệu điện tử (EDI).

2.1.5.4 Truyền dung liệu

Dung liệu (content) là nội dung của hàng hóa số, giá trị của nó không phải trong vật mang tin mà nằm trong bản thân nội dung của nó. Hàng hoá số có thể được giao qua mạng. Ví dụ hàng hoá số là: Tin tức, nhạc phim, các chương trình phát thanh, truyền hình, các chương trình phần mềm, các ý kiến tư vấn, vé máy bay, vé xem phim, xem hát, hợp đồng bảo hiểm, v.v..

Trước đây, dung liệu được trao đổi dưới dạng hiện vật (physical form) bằng cách đưa vào đĩa, vào băng, in thành sách báo, thành văn bản, đóng gói bao bì chuyển đến tay người sử dụng, hoặc đến điểm phân phối (như cửa hàng, quầy báo v.v.) để người sử dụng mua và nhận trực tiếp. Ngày nay, dung liệu được số hóa và truyền gửi theo mạng, gọi là “giao gửi số hóa” (digital delivery).

Các tờ báo, các tư liệu công ty, các ca-ta-lô sản phẩm lần lượt đưa lên Web, người ta gọi là “xuất bản điện tử” (electronic publishing hoặc Web publishing), khoảng 2700 tờ báo đã được đưa lên Web gọi là “sách điện tử”; các chương trình phát thanh, truyền hình, giáo dục, ca nhạc, kể chuyện v.v..cũng được số hóa, truyền qua Internet, người sử dụng tải xuống (download); và sử dụng thông qua màn hình và thiết bị âm thanh của máy tính điện tử.

2.1.5.5 Mua bán hàng hóa hữu hình

Đến nay, danh sách các hàng hóa bán lẻ qua mạng đã mở rộng, từ hoa tới quần áo, ô tô và xuất hiện một loại hoạt động gọi là “mua hàng điện tử” (electronic shopping), hay “mua hàng trên mạng”; ở một số nước, Internet bắt đầu trở thành công cụ để cạnh tranh bán lẻ hàng hữu hình (Retail of tangible goods). Tận dụng tính năng đa phương tiện (multimedia) của môi trường Web và Java, người bán xây dựng trên mạng các “cửa hàng ảo” (virtual shop), gọi là ảo bởi vì, cửa hàng có thật nhưng ta chỉ xem toàn bộ quang cảnh cửa hàng và các hàng hóa chứa trong đó trên từng trang màn hình một.

2.1.6 Lợi ích của Thương mại điện tử

2.1.6.1 Thu thập được nhiều thông tin

TMĐT giúp người ta tham gia thu được nhiều thông tin về thị trường, đối tác, giảm chi phí tiếp thị và giao dịch, rút ngắn thời gian sản xuất, tạo dựng và củng cố quan hệ bạn hàng. Các doanh nghiệp nắm được thông tin phong phú về kinh tế thị trường, nhờ đó có thể xây dựng được chiến lược sản xuất và kinh doanh thích hợp với xu thế phát triển của thị trường trong nước, khu vực và quốc tế. Điều này đặc biệt có ý nghĩa đối với các doanh nghiệp vừa và nhỏ, hiện nay đang được nhiều nước quan tâm, coi là một trong những động lực phát triển kinh tế.

2.1.6.2 Giảm chi phí sản xuất

TMĐT giúp giảm chi phí sản xuất, trước hết là chi phí văn phòng. Các văn phòng không giấy tờ (paperless office) chiếm diện tích nhỏ hơn rất nhiều, chi phí tìm kiếm chuyển giao tài liệu giảm nhiều lần (trong đó khâu in ấn hầu như được bỏ hẳn); theo số liệu của hãng General Electricity của Mỹ, tiết kiệm trên hướng này đạt tới 30%. Điều quan trọng hơn, với góc độ chiến lược, là các nhân viên có năng lực được giải phóng khỏi nhiều công đoạn sự vụ có thể tập trung vào nghiên cứu phát triển, sẽ đưa đến những lợi ích to lớn lâu dài.

2.1.6.3 Giảm chi phí bán hàng, tiếp thị và giao dịch

TMĐT giúp giảm thấp chi bán hàng và chi phí tiếp thị. Bằng phương tiện Internet/Web, một nhân viên bán hàng có thể giao dịch được với rất nhiều khách hàng, catalogue điện tử (electronic catalogue) trên Web phong phú hơn nhiều và thường xuyên cập nhật so với catalogue in ấn chỉ có khuôn khổ giới hạn và luôn luôn lỗi thời. Theo số liệu của hãng máy bay Boeing của Mỹ, đã có tới 50% khách hàng đặt mua 9% phụ tùng qua Internet, và mỗi ngày giảm bán được 600 cuộc gọi điện thoại.

TMĐT qua Internet/Web giúp người tiêu thụ và các doanh nghiệp giảm đáng kể thời gian và chi phí giao dịch (giao dịch được hiểu là từ quá trình quảng cáo, tiếp xúc ban đầu, giao dịch đặt hàng, giao dịch thanh toán). Thời gian giao dịch qua Internet chỉ bằng 7% thời gian giao dịch qua Fax, và bằng khoảng 0.5 phần nghìn thời gian giao dịch qua bưu điện chuyển phát nhanh, chi phí thanh toán điện tử qua Internet chỉ bằng từ 10% đến 20% chi phí thanh toán theo lối thông thường.

Tổng hợp tất cả các lợi ích trên, chu trình sản xuất (cycle time) được rút ngắn, nhờ đó sản phẩm mới xuất hiện nhanh và hoàn thiện hơn.

2.1.6.4 Xây dựng quan hệ với đối tác

TMĐT tạo điều kiện cho việc thiết lập và củng cố mối quan hệ giữa các thành viên tham gia vào quá trình thương mại: thông qua mạng (Internet/ Web) các thành viên tham gia (người tiêu thụ, doanh nghiệp, các cơ quan Chính phủ...) có thể giao tiếp trực tiếp (liên lạc “trực tuyến”) và liên tục với nhau, có cảm giác như không có khoảng cách về địa lý và thời gian nữa; nhờ đó sự hợp tác và sự quản lý đều được tiến hành nhanh chóng một cách liên tục: các bạn hàng mới, các cơ hội kinh doanh mới được phát hiện nhanh chóng trên phạm vi toàn quốc, toàn khu vực, toàn thế giới, và có nhiều cơ hội để lựa chọn hơn.

2.1.6.5 Tạo điều kiện sớm tiếp cận nền kinh tế tri thức

Trước hết, TMĐT sẽ kích thích sự phát triển của ngành công nghệ thông tin tạo cơ sở cho phát triển kinh tế tri thức. Lợi ích này có một ý nghĩa lớn đối với các nước đang phát triển: nếu không nhanh chóng tiếp cận nền kinh tế tri thức thì sau khoảng một thập kỷ nữa, nước đang phát triển có thể bị bỏ rơi hoàn toàn. Khía cạnh lợi ích này mang tính chiến lược công nghệ và tính chính sách phát triển cần cho các nước công nghiệp hóa.

2.2 THANH TOÁN ĐIỆN TỬ

2.2.1 Tổng quan về thanh toán điện tử

2.2.1.1 Định nghĩa thanh toán điện tử

- Theo nghĩa rộng: Thanh toán điện tử là việc thanh toán tiền thông qua các thông điệp điện tử thay cho việc trao tay tiền mặt (Theo báo cáo quốc gia về kỹ thuật Thương mại điện tử của Bộ thương mại)

- Theo nghĩa hẹp: Thanh toán trong thương mại điện tử có thể hiểu là việc trả tiền và nhận tiền hàng cho các hàng hóa và dịch vụ được mua bán thông qua Internet.

2.2.1.2 Lợi ích của thanh toán điện tử

2.2.1.2.1 Một số lợi ích chung của Thương mại điện tử

- Hoàn thiện và phát triển thương mại điện tử

Xét trên nhiều phương diện, thanh toán trực tuyến là nền tảng của các hệ thống thương mại điện tử. Sự khác biệt cơ bản giữa thương mại điện tử với các ứng dụng khác cung cấp trên Internet chính là nhờ khả năng thanh toán trực tuyến này. Do vậy, việc phát triển thanh toán trực tuyến sẽ hoàn thiện hóa thương mại điện tử, để Thương mại điện tử được theo đúng nghĩa của nó – các giao dịch hoàn toàn qua mạng, người mua chỉ cần thao tác qua máy tính cá nhân của mình để mua hàng, các doanh nghiệp có những hệ thống xử lý tiền số tự động. Một khi thanh toán trong thương mại điện tử an toàn, tiện lợi, việc phát triển thương mại điện tử trên toàn cầu là một điều tất yếu với số đông đảo và không ngừng tăng của mạng Internet.

- Tăng quá trình lưu thông tiền tệ và hàng hóa

Thanh toán trong thương mại điện tử với ưu điểm đẩy mạnh quá trình lưu thông tiền tệ và hàng hóa. Người bán hàng có thể nhận tiền thanh toán qua mạng tức thì, do đó có thể yên tâm tiến hành giao hàng một cách sớm nhất, sớm thu hồi vốn để tiếp tục đầu tư sản xuất. Thanh toán điện tử giúp thực hiện thanh toán nhanh, an toàn, đảm bảo quyền lợi cho các bên tham gia thanh toán, hạn chế rủi

ro so với thanh toán bằng tiền mặt, mở rộng thanh toán không dùng tiền mặt, tạo lập thói quen mới trong dân chúng về thanh toán hiện đại.

- Hiện đại hóa hệ thống thanh toán

Tiến cao hơn một bước, thanh toán điện tử tạo ra một loại tiền mới, tiền số hóa, không chỉ thỏa mãn các tài khoản tại ngân hàng mà hoàn toàn có thể dùng để mua hàng hóa thông thường. Quá trình giao dịch được đơn giản và nhanh chóng, chi phí giao dịch giảm bớt đáng kể và an toàn hơn. Tiền số hóa không chiếm một không gian hữu hình nào, có thể di chuyển nửa vòng trái đất trong chớp mắt. Đây sẽ là một cơ cấu tiền tệ mới, một mạng tài chính hiện đại gắn liền với mạng Internet.

2.2.1.2.2 Một số lợi ích đối với ngân hàng

- Giảm chi phí tăng hiệu quả kinh doanh

- + Giảm chi phí văn phòng: giao dịch qua mạng giúp rút ngắn thời gian tác nghiệp, chuẩn hóa các thủ tục, quy trình, nâng cao hiệu quả tìm kiếm và xử lý chứng từ.
- + Giảm chi phí nhân viên: một máy rút tiền tự động có thể làm việc 24/24 giờ và tương đương một chi nhánh ngân hàng truyền thống.
- + Cung cấp dịch vụ thuận tiện cho khách hàng: thông qua web/internet, ngân hàng có khả năng cung cấp dịch vụ mới (internet banking) và thu hút thêm nhiều khách hàng giao dịch thường xuyên hơn, giảm chi phí bán hàng và tiếp thị.
- + Mở rộng thị trường thông qua Internet, ngân hàng thay vì mở nhiều chi nhánh ở các nước khác nhau có thể cung cấp dịch vụ Internet banking để mở rộng phạm vi cung cấp dịch vụ.

- Đa dạng hóa dịch vụ và sản phẩm

Ngày nay, dịch vụ ngân hàng đang vươn tới từng người dân. Đó là dịch vụ ngân hàng tiêu dùng và bán lẻ. “Ngân hàng điện tử”, với sự trợ giúp của công nghệ thông tin cho phép tiến hành các giao dịch bán lẻ với tốc độ cao và liên tục.

Các ngân hàng có thể cung cấp thêm các dịch vụ mới cho khách hàng như “phone banking”, “home banking”, “Internet banking”, chuyển tiền, rút tiền, thanh toán tự động...

- Nâng cao năng lực cạnh tranh và tạo nét riêng trong kinh doanh

“Ngân hàng điện tử” giúp các ngân hàng tạo và duy trì một hệ thống khách hàng rộng rãi và bền vững. Thay vì phải xếp hàng rất lâu chờ rút tiền tại một chi nhánh ngân hàng, khách hàng có thể đi tới một máy rút tiền tự động của một ngân hàng khác và thực hiện giao dịch trong vài phút. Thế mạnh về dịch vụ ngân hàng điện tử cũng là một đặc điểm để các ngân hàng hiện đại tạo dựng nét riêng của mình.

- Thực hiện chiến lược toàn cầu hóa

Một lợi ích quan trọng khác mà ngân hàng điện tử đem lại cho ngân hàng, đó là việc ngân hàng có thể thực hiện chiến lược “toàn cầu hóa”, chiến lược “bành trướng” mà không cần phải mở thêm chi nhánh. Ngân hàng có thể vừa tiết kiệm chi phí do không phải thiết lập quá nhiều các trụ sở hoặc văn phòng, nhân sự gọn nhẹ mà lại có thể phục vụ một lượng lớn khách hàng tại cùng một thời điểm.

- Xúc tiến thương mại, quảng bá thương hiệu toàn cầu

Thông qua Internet, ngân hàng có thể đăng tải tất cả những thông tin tài chính, tổng giá trị tài sản, các dịch vụ của ngân hàng mình, để phục vụ cho mục đích quảng cáo. Có thể ngân hàng chưa thể tiến hành các giao dịch tài chính trực tuyến, song bằng cách thiết lập các website của riêng mình với chức năng ban đầu là cung cấp thông tin và giải đáp ý kiến thắc mắc của khách hàng qua mạng, ngân hàng cũng được coi là đã bước đầu tham gia áp dụng dịch vụ ngân hàng điện tử và hòa mình vào xu thế chung.

2.2.1.2.3 Một số lợi ích đối với khách hàng

- Khách hàng tiết kiệm được chi phí

Phí giao dịch ngân hàng điện tử hiển nhiên được đánh giá ở mức thấp nhất so với các phương tiện giao dịch khác. Điều này hoàn toàn có thể lý giải được bởi một khi các ngân hàng có thể tiết kiệm được chi phí triển khai ngân hàng, các chi phí khác vì thế sẽ cũng theo đó mà giảm đi rất nhiều

- Khách hàng tiết kiệm thời gian

Đối với các giao dịch ngân hàng từ Internet được thực hiện và xử lý một cách nhanh chóng và hết sức chính xác. Khách hàng cũng không cần phải tới tận văn phòng giao dịch của ngân hàng, không phải mất thời gian đi lại hoặc nhiều khi phải xếp hàng chờ tới lượt. Giờ đây với ngân hàng điện tử, họ có thể tiếp cận với bất cứ giao dịch nào vào bất cứ lúc nào hay bất cứ nơi đâu họ muốn.

- Thông tin liên lạc với ngân hàng nhanh hơn và hiệu quả hơn

Khi khách hàng sử dụng ngân hàng điện tử, họ sẽ nắm được nhanh chóng, kịp thời những thông tin về tài khoản, tỷ giá, lãi suất. Chỉ trong chốc lát, qua máy tính, khách hàng đã có thể kiểm tra số dư tài khoản, chuyển tiền, thanh toán hóa đơn dịch vụ công cộng, thanh toán thẻ tín dụng, kinh doanh ngoại hối, vay nợ...

2.2.1.3 Hạn chế của thanh toán điện tử

- Gian lận thẻ tín dụng

+ Rủi ro đối với chủ thẻ

Do tính chất của thẻ tín dụng là không biết được người rút tiền có phải là chủ thẻ hay không mà chủ yếu dựa vào kiểm tra số pin trên thẻ nên các chủ thẻ dễ bị lừa ăn cắp thẻ cùng mã số. Bên cạnh đó chủ thẻ còn có thể gặp tình trạng làm thẻ giả ngày càng tinh vi.

+ Rủi ro đối với ngân hàng phát hành

Rủi ro thứ nhất là việc chủ thẻ lừa dối sử dụng tại nhiều điểm thanh toán thẻ khác nhau với mức thanh toán thấp hơn hạn mức thanh toán nhưng tổng số tiền thanh toán lại cao hơn hạn mức thanh toán trong thẻ.

Một hình thức lừa dối khác từ phía chủ thẻ là do việc lợi dụng tính chất thanh toán quốc tế của thẻ để thông đồng với người khác chuyển thẻ ra nước khác nhằm thanh toán ngoài quốc gia chủ thẻ cư trú.

+ Rủi ro đối với ngân hàng thanh toán

Tuy chỉ là đơn vị trung gian trong hoạt động thanh toán song các ngân hàng thanh toán cũng có thể gặp rủi ro nếu họ có sai sót trong việc cấp phép cho các khoản thanh toán có giá trị lớn hơn hạn mức quy định. Bên cạnh đó, nếu không kịp thời cung cấp cho các đơn vị chấp nhận thẻ danh sách các thẻ bị mất hoặc bị vô hiệu mà chúng vẫn được sử dụng thì ngân hàng phát hành sẽ từ chối thanh toán những khoản này.

+ Rủi ro cho đơn vị chấp nhận thẻ

Rủi ro cho các đơn vị chấp nhận thẻ chủ yếu là bị từ chối thanh toán cho số hàng hóa cung ứng ra vì các lý do liên quan đến thẻ. Đó là việc thẻ bị hết hiệu lực những các đơn vị chấp nhận thẻ không phát hiện ra. Tự ý sửa đổi các hóa đơn và bị các ngân hàng phát hiện ra thì cũng sẽ không được thanh toán.

- Vấn đề bảo mật thông tin

Việc đảm bảo an toàn thông tin tiền gửi và tài sản gửi của khách hàng là nghĩa vụ của các ngân hàng thương mại. Tuy nhiên, trong điều kiện hiện nay, với trình độ khoa học rất phát triển, số lượng các vụ xâm nhập trái phép vào hệ thống ngân hàng qua mạng internet ngày càng nhiều thì việc lưu chuyển thông tin khách hàng qua mạng internet không còn được an toàn:

- + Thông tin bị truy cập trái phép trên đường truyền.
- + Bất cẩn của các nhân viên ngân hàng khi thực hiện các quy tắc bảo mật.
- + Bất cẩn từ chính khách hàng để lộ thông tin giao dịch.
- + Hệ thống máy tính và mạng làm việc kém hiệu quả hoặc lỗi.

2.2.1.4 Yêu cầu đối với thanh toán điện tử

- Khả năng có thể chấp nhận được

Để được thành công thì cơ sở hạ tầng của việc thanh toán phải được công nhận rộng hơn, môi trường pháp lý đầy đủ, bảo đảm quyền lợi cho cả khách hàng và doanh nghiệp, công nghệ áp dụng đồng bộ ở các ngân hàng cũng như tại tổ chức thanh toán.

- An toàn và bảo mật

Cho các giao dịch tài chính qua các mạng mở như Internet vì đây sẽ là mục tiêu cho tội phạm, hacker.... Do các dịch vụ trên Internet ngày nay được cung cấp toàn cầu với mọi tiện ích phục vụ khách hàng, mọi thành phần trong xã hội. Chính vì vậy phải đảm bảo khả dụng nhưng chống lại được sự tấn công, khai thác, điều chỉnh thông tin.

- Giấu tên (nặc danh)

Nếu như khách hàng yêu cầu thì đặc điểm nhận dạng của họ phải được giữ kín dù khách hàng đã cung cấp đầy đủ các thông tin để người bán được thanh toán. Phải đảm bảo không làm lộ các thông tin cá nhân của khách hàng.

- Khả năng có thể hoán đổi

Tiền số có thể chuyển thành các loại quỹ khác. Có thể dễ dàng chuyển sang tiền mặt hay từ quỹ tiền điện tử về tài khoản của cá nhân. Có thể chuyển sang ngoại tệ khác với tỉ giá tốt nhất.

- Hiệu quả

Chi phí cho mỗi giao dịch nên chỉ là một con số tượng trưng rất nhỏ, đặc biệt với những giao dịch giá trị thấp.

- Tính linh hoạt

Nên cung cấp nhiều phương thức thanh toán, giao dịch tiện lợi cho mọi đối tượng.

- Tính hợp nhất

Để hỗ trợ cho sự tồn tại của các ứng dụng này thì giao diện nên tạo ra theo sự thống nhất của từng ứng dụng. Khi mua hàng trên bất cứ trang web nào cũng cần có những giao diện với trình tự thao tác giống nhau.

- Tính tin cậy

Hệ thống thanh toán phải luôn thích ứng, tránh những sai sót không đáng có, tránh cho nó không phải là mục tiêu của sự phá hoại.

- Có tính co giãn

Cho phép khách hàng và những nhà kinh doanh có thể tham gia vào hệ thống mà không làm hỏng cơ cấu hạ tầng, đảm bảo xử lý tốt dù khi nhu cầu thanh toán trong thương mại điện tử tăng.

- Tiện lợi dễ sử dụng

Thanh toán tiện lợi như và hơn trong thực tế.

2.2.1.5 Rủi ro trong thanh toán điện tử

- Những rủi ro liên quan đến quá trình thanh toán

- + Sao chụp thiết bị
- + Sửa đổi hoặc sao chép dữ liệu hoặc phần mềm
- + Lầy trộm thiết bị.
- + Không ghi lại giao dịch
- + Sự cố hoạt động

- Rủi ro với người tiêu dùng tham gia thanh toán

Ngoài những rủi ro mất an toàn như trên, người tiêu dùng có thể gặp những rủi ro khác như: chi tiết giao dịch ghi lại không đầy đủ để có thể giải quyết tranh chấp. Rủi ro nếu nhà phát hành lâm vào phá sản hoặc mất khả năng chi trả.

- Rủi ro đối với các tổ chức cung ứng phương tiện thanh toán điện tử

Nhà phát hành cũng có thể phải chịu các rủi ro lừa đảo, vận hành sai, bồi thường cho khách hàng...

- Rủi ro do các hoạt động gian lận và phi pháp

Lợi dụng sự chưa hoàn thiện của các hệ thống bảo mật, các dữ liệu về thẻ có thể bị đánh cắp và khai thác bất hợp pháp.

- Thẻ mất cắp, thất lạc

Chủ thẻ bị mất cắp, thất lạc thẻ và bị người khác sử dụng trước khi chủ thẻ kịp thông báo cho ngân hàng phát hành để có các biện pháp hạn chế hoặc thu hồi thẻ. Thẻ này có thể bị các tổ chức tội phạm lợi dụng để thực hiện các giao dịch giả mạo. Rủi ro này thường chiếm tỉ lệ lớn.

- Thẻ giả

Thẻ do tổ chức tội phạm làm giả dựa trên các thông tin được khai thác bất hợp pháp. Đây là loại rủi ro nguy hiểm và khó lường vì có liên quan tới nhiều nguồn thông tin và nằm ngoài khả năng kiểm soát của ngân hàng phát hành.

- Đơn xin phát hành thẻ với thông tin giả mạo

Do không thẩm định kỹ hồ sơ, ngân hàng phát hành thẻ cho khách hàng giả mạo thông tin. Trường hợp này sẽ dẫn đến rủi ro cho Ngân hàng phát hành khi chủ thẻ không có hoặc không có khả năng thanh toán.

- Tài khoản của chủ thẻ bị lợi dụng

Đến kỳ phát hành lại thẻ, Ngân hàng phát hành nhận được thông báo thay đổi địa chỉ của chủ thẻ, do không thẩm định kỹ mà thẻ được gửi về địa chỉ không chính xác dẫn tới tài khoản của chủ thẻ bị lợi dụng.

- Thẻ bị giả mạo để thanh toán qua thư, điện thoại

Cơ sở chấp nhận thẻ cung cấp dịch vụ theo yêu cầu của chủ thẻ qua thư hoặc điện thoại dựa vào thông tin của chủ thẻ, mà không biết rằng thông tin này đang bị giả mạo, dẫn tới bị ngân hàng phát hành thẻ từ chối thanh toán cho đơn vị chấp nhận thẻ.

- Nhân viên Cơ sở chấp nhận thẻ giả mạo hóa đơn thanh toán thẻ

Khi thực hiện giao dịch, nhân viên cơ sở chấp nhận thẻ cố tình làm sai lệch thông tin hoặc in nhiều hóa đơn, rồi dùng vào việc đòi tiền không từ ngân hàng thanh toán.

- Tạo băng từ giả

Tội phạm sao chép thông tin từ băng từ của thẻ thật rồi sao chép và thực hiện các giao dịch giả mạo. Gây thiệt hại cho chủ thẻ, ngân hàng phát hành, ngân hàng thanh toán.

2.2.1.6 Cơ sở vật chất kỹ thuật cho thanh toán điện tử

- Hệ thống mạng giữa các ngân hàng và cơ sở chấp nhận thanh toán
- Hệ thống mạng viễn thông
- Cơ sở vật chất của ngân hàng phục vụ thanh toán điện tử
- Cơ sở vật chất của các cơ sở chấp nhận thẻ.

2.3 GIAO DỊCH ĐIỆN TỬ SỬ DỤNG TIỀN ĐIỆN TỬ

2.3.1 Tổng quan về giao dịch điện tử dùng tiền điện tử

Ngày nay thương mại điện tử đã được áp dụng rộng rãi, phương thức thanh toán điện tử là yếu tố rất quan trọng ảnh hưởng đến sự thành công của thương mại điện tử. Tuy nhiên, hiện tại hầu hết các dịch vụ mua bán hàng hóa trên mạng đều sử dụng hình thức thanh toán bằng thẻ tín dụng (credit card). Người sử dụng cần nhập vào các thông tin: tên người sử dụng, mã số thẻ, ngày hết hạn của thẻ. Nhưng vì thẻ tín dụng được dùng phổ biến cho các thanh toán khác nhau, nên những thông tin trên có nhiều người biết. Thực tế hiện nay, các gian lận về thẻ trên Internet chiếm 6-7% tổng số các giao dịch thẻ ở các nước châu Âu, tỷ lệ này ở châu Á là 10%. Tại Việt Nam, dịch vụ thẻ tín dụng mới sử dụng cuối năm 1996, nhưng đến nay, tỷ lệ các giao dịch gian lận trên tổng số các giao dịch là hơn 10%. Trong 5 giao dịch gian lận, thì có 4 giao dịch gian lận mua hàng trên Internet, trong 4 giao dịch đó, thì có 1 giao dịch là mua hàng hóa, 3 giao dịch là các dịch vụ khác. Với những giao dịch giá trị nhỏ (khoảng vài cent), việc sử dụng thẻ tín dụng không mang lại hiệu quả. Có thể kết luận rằng, trên thế giới hiện nay, nhu cầu về thương mại điện tử rất phổ biến, nhưng các vấn đề hạ tầng trong thanh toán điện tử vẫn chưa được giải quyết tương xứng và đáp ứng được các đòi hỏi đặt ra. Việc nghiên cứu xây dựng các hệ thống thanh

toán điện tử để đảm bảo an toàn thông tin trong các dịch vụ thương mại điện tử là một hướng nghiên cứu rất cần thiết hiện nay. Việc xây dựng các hệ thống thanh toán điện tử về mặt kỹ thuật chính là ứng dụng các thành tựu của lý thuyết mật mã. Các mô hình thanh toán sử dụng các giao thức mật mã được xây dựng để đảm bảo an toàn cho việc giao dịch giữa các bên tham gia. Vào thập niên 90, sự mở rộng và phổ biến của Internet đã tạo ra phương thức mua hàng và bán hàng qua mạng (thương mại điện tử). Và đặc biệt khi Internet thực sự bùng nổ vào năm 2000, một số chuyên gia tin rằng đây là mốc quan trọng đánh dấu bước khởi đầu của tiền điện tử. Sự thành công của một số hệ thống tiền điện tử đã và đang được tiếp tục triển khai tại một số quốc gia.

2.3.2 Tiền điện tử

2.3.2.1 Tổng quan về tiền điện tử

Tiền điện tử (e-money, digital money, digital cash, electronic money, electronic currency, digital currency hay internet money) là thuật ngữ vẫn còn mơ hồ và chưa định nghĩa đầy đủ. Tuy nhiên có thể hiểu Tiền điện tử là loại tiền trao đổi theo phương pháp “điện tử”, liên quan đến mạng máy tính và những hệ thống chứa giá trị ở dạng số (digital stored value systems). Hệ thống Tiền điện tử cho phép người dùng có thể thanh toán khi mua hàng, hoặc sử dụng các dịch vụ nhờ truyền đi các “dãy số” từ máy tính (hay thiết bị lưu trữ như smart card) này tới máy tính khác (hay smart card). Giống như dãy số (serial) trên tiền giấy, dãy số của tiền điện tử là duy nhất. Mỗi “đồng” tiền điện tử được phát hành bởi một tổ chức (ngân hàng) và biểu diễn một lượng tiền thật nào đó.

Tiền điện tử có loại ẩn danh và định danh. Hệ thống tiền ẩn danh không tiết lộ thông tin định danh của người sử dụng, và hệ thống này dựa vào Sơ đồ chữ ký “mù”. Hệ thống tiền định danh tiết lộ thông tin định danh của người sử dụng, hệ thống dựa vào Sơ đồ chữ ký thông thường. *Tính ẩn danh của tiền điện tử tương tự như tiền mặt thông thường, hệ thống tiền định danh tương tự như hệ thống thẻ tín dụng.*

2.3.2.2 Thực trạng ứng dụng tiền điện tử

Tiền điện tử được bắt đầu sử dụng từ những năm cuối của thập kỉ 90, nhưng loại tiền này vẫn còn quá ít so với việc sử dụng thẻ tín dụng. Được sử dụng với mục đích chính là giao dịch trực tuyến, các loại tiền này được phát hành bởi các công ty như Beenz.com, Flooz.com và một số các công ty khác.

Tuy nhiên, vào thời kì suy thoái năm 2000, rất nhiều công ty "dot-com" được thành lập, nhưng đã nhanh chóng bị đổ vỡ và trở thành công ty "dot- bom". Do đó, tiền điện tử còn là vấn đề cần phải cân nhắc và xem xét lại một cách kĩ lưỡng, cẩn thận hơn.

Tiền điện tử bắt đầu được sử dụng tại Nhật cách đây 4 năm dưới hình thức trả tiền vé tháng khi đi tàu xe. Ngày nay, chúng được tích hợp trong thẻ thông minh và ĐTDD để mua sắm từ những gian hàng nhỏ, những cửa hàng lớn, những nhà hàng, cho tới siêu thị, những cửa hàng bán lẻ... Năm 2005, NTT DoCoMo - hãng truyền thông lớn nhất Nhật Bản đã bán ra 3,34 triệu thiết bị cầm tay được trang bị công nghệ FeliCa kể từ tháng 4/2005. Trong năm 2005, số tiền thu được từ giao dịch điện tử tăng lên gấp đôi. Một số siêu thị lớn của Nhật đã thông báo rằng 40% những cuộc mua bán của họ sử dụng tiền điện tử.

Tuy nhiên, nâng cấp hệ thống thanh toán sẽ tiêu tốn chi phí đầu tư của những hãng kinh doanh. Những nhà kinh doanh thường "bất đắc dĩ " mới đầu tư vào công nghệ nhằm đem lại sự tiện lợi cho khách hàng. Còn khách hàng thì lại luôn dè dặt khi sử dụng những công nghệ mới. Chính điều này đã làm cho sự thành công và sự ủng hộ cho tiền điện tử còn chưa cao. Cũng giống như trường hợp tiền giấy vẫn sẽ tồn tại sau khi séc được đưa ra. Vì vậy, khả năng tiền giấy sẽ cùng song song tồn tại với tiền điện tử. Đặc biệt, tiền điện tử cũng không thể loại bỏ hoàn toàn thẻ tín dụng (credit-card) và thẻ nợ (debit-card).

Tiền điện tử cũng sẽ cần thêm thời gian để thực sự trưởng thành. Khi những công ty cung cấp viễn thông chuyển sang công nghệ 3G, chúng sẽ là cơ sở hạ tầng cần thiết và vững chắc để hỗ trợ những phiên giao dịch, thanh toán

trực tuyến bằng ĐTDĐ. Lúc đó, tiền điện tử sẽ thực sự "cất cánh", là điểm tựa vững chắc cho thương mại điện tử.

Hiện tại, khái niệm tiền điện tử vẫn là một khái niệm khá mới mẻ tại Việt Nam. Một số doanh nghiệp đã nghiên cứu và đưa ra thị trường loại thẻ thanh toán đa mục đích để chơi game, sử dụng Internet hay mua hàng hóa trên website của doanh nghiệp. Một vài ngân hàng cũng đã bắt đầu đẩy mạnh cung ứng các sản phẩm, dịch vụ ngân hàng qua kênh điện tử như Internet banking, Mobile banking.

2.3.2.3 Một số vấn đề về tiền điện tử

Tiền điện tử được kỳ vọng mang lại nhiều ích lợi không chỉ cho phía người sử dụng, mà còn cho cả phía ngân hàng cũng như phía các nhà cung cấp, là một phương thức thanh toán hiệu quả. Tuy nhiên, để đưa tiền điện tử thực sự trở thành phương thức thanh toán hữu hiệu, được người sử dụng chấp nhận, thì các nhà công nghệ, các nhà phát triển và các chuyên gia an toàn thông tin còn phải đứng trước nhiều thách thức. Hai vấn đề lớn nhất hiện nay đặt ra đối với tiền điện tử bao gồm: vấn đề ẩn danh người sử dụng và vấn đề ngăn chặn người sử dụng tiêu một đồng tiền điện tử nhiều lần (double-spending). Tùy theo từng loại tiền điện tử, sẽ có những giải pháp khác nhau để giải quyết những vấn đề này.

- *Vấn đề ẩn danh.*

Tính ẩn danh là một đặc tính rất quan trọng của phương thức thanh toán bằng tiền điện tử, đây là ưu điểm của phương thức này so với những phương thức khác. Tính ẩn danh là quá trình thanh toán của người trả tiền phải được ẩn danh và không để lại dấu vết, nghĩa là ngân hàng sẽ không nói được: tiền giao dịch là của ai. Trong hệ thống tiền điện tử, để giải quyết vấn đề trên người ta đã sử dụng kỹ thuật “chữ ký số mù”. Chữ ký số mù là một dạng đặc biệt của chữ ký điện tử, nó đòi hỏi người ký thực hiện ký vào một thông điệp mà không biết nội dung của nó. Thêm vào đó, người ký sau này có thể nhìn thấy cặp chữ ký/thông điệp, nhưng không thể biết được là mình đã ký thông điệp đó khi nào và ở đâu (mặc dù anh ta có thể kiểm tra được chữ ký đó là đúng đắn). Nó cũng giống như ký khi đang nhắm mắt vậy. Chữ ký số mù đảm bảo ngân hàng không thể có được bất cứ mối liên hệ nào giữa đồng tiền điện tử và chủ sở hữu của nó.

Tùy theo từng hệ thống tiền điện tử cụ thể mà sẽ áp dụng những sơ đồ chữ ký số mù khác nhau. Chẳng hạn trong lược đồ của CHAUM-FIATNAOR thì sử dụng sơ đồ chữ ký mù RSA, trong khi đó trong lược đồ BRAND thì dựa trên sơ đồ chữ ký Schnorr. Mỗi lược đồ có những ưu và nhược điểm khác nhau, điều

này sẽ được trình bày cụ thể trong những phần sau. Tuy nhiên giải pháp sử dụng chữ ký mù làm nảy sinh một vấn đề, đó là: Điều gì xảy ra nếu như ông A cố tình gian lận, gửi tới ngân hàng một đồng tiền điện tử ghi giá trị 50\$ để ký, nhưng báo với ngân hàng là 1\$. Vì ngân hàng ký mù lên đồng tiền, nên rõ ràng là không thể biết được nội dung của nó. Để giải quyết trường hợp gian lận này, có hai giải pháp được đề ra: Cách rõ ràng nhất là ngân hàng sử dụng một khoá công khai khác nhau cho mỗi loại tiền. Nghĩa là nếu có k đồng tiền khác biệt thì ngân hàng phải công khai k khoá công khai. Giả sử với đơn vị tiền có giá trị là 1\$ thì ngân hàng sử dụng khoá k_1 và 50\$ thì sử dụng khoá k_{50} . Như vậy trường hợp gian lận của ông A sẽ tạo ra đồng tiền có giá trị 50\$ với k_1 , đây là đồng tiền không hợp lệ. Phương pháp thứ hai là dùng giao thức “cắt và chọn” (Cut and choose). Ý tưởng của giao thức này là: để có một đồng tiền có giá trị thì ông A phải tạo k đồng tiền, ký hiệu là $C_1, C_2, \dots, C_k$. Mỗi đồng tiền đều được gán định danh, sự khác nhau duy nhất giữa chúng là số sê-ri. Ông A làm mù những đồng tiền này và gửi chúng đến ngân hàng. Ngân hàng yêu cầu ông A cung cấp các thông tin tương ứng để có thể khử mù $k-1$ đồng tiền bất kỳ. Ngân hàng khử mù và kiểm tra chúng. Nếu tất cả đều hợp lệ, ngân hàng ký mù lên đồng tiền còn lại C_i (là đồng tiền mà ngân hàng không khử mù) và gửi lại cho ông A. Ngân hàng có sự đảm bảo cao rằng đồng tiền còn lại cũng là hợp lệ vì nếu ông A gửi kèm đồng tiền không hợp pháp trong số k đồng tiền, thì xác suất bị phát hiện ít nhất là $k-1/k$. Xác suất này càng cao nếu k càng lớn. Tuy nhiên nếu k quá lớn thì hệ thống xử lý phải trao đổi nhiều dữ liệu.

- Vấn đề tiêu xài hai lần.

Với tính chất dạng số hoá, nên với Tiền điện tử, dễ dàng tạo bản sao từ bản gốc. Không thể phân biệt được đây là bản sao từ một bản gốc nào đấy, chính vì thế việc giả mạo là không thể phát hiện được. Một hệ thống tiền điện tử tầm thường sẽ cho phép tạo bản sao của tiền điện tử và kẻ gian có thể tiêu xài bản sao này bình thường mà không bị phát hiện. Hệ thống tiền điện tử khi được áp

dụng vào thực tế thì thật sự phải có khả năng ngăn ngừa hay phát hiện được trường hợp “tiêu xài hai lần” (double spending). Để giải quyết vấn đề này, tùy theo từng loại hệ thống tiền điện tử mà có giải pháp khác nhau.

+*Đối với hệ thống Tiền điện tử trực tuyến*: Hệ thống yêu cầu người bán hàng liên lạc tới ngân hàng với mỗi lần bán. Ngân hàng lưu giữ thông tin tất cả những đồng tiền điện tử đã tiêu xài trước đây và có thể dễ dàng cho người bán hàng biết đồng tiền nào còn khả năng tiêu xài được. Nếu ngân hàng báo rằng đồng tiền nào đó đã thực sự được tiêu xài rồi, thì người bán hàng lập tức từ chối bán hàng. Điều này giống như cách mà những nhà bán hàng hiện tại kiểm tra thẻ tín dụng tại những điểm bán hàng.

+*Đối với hệ thống Tiền điện tử ngoại tuyến*: Việc phát hiện trường hợp “tiêu xài hai lần” sẽ được thực hiện bằng hai cách khác nhau. Cách thứ nhất là tạo thẻ thông minh đặc biệt (special smart card) chứa con chip chống trộm cắp. Trong những hệ thống khác, chip này còn được gọi là “người theo dõi”. Chip theo dõi sẽ lưu một lượng nhỏ dữ liệu của tất cả những tiền điện tử đã được tiêu xài qua smart card. Nếu người sở hữu smart card đó cố gắng sao chép tiền điện tử này và tiêu xài nó lần hai, thì chip theo dõi (được gắn vào smart card) sẽ phát hiện được hành động này, và không cho phép giao dịch “tiêu xài”. Bởi vì chip theo dõi dùng để chống sự gian dối, người sở hữu smart card này không thể xóa được dữ liệu trừ khi họ phá hủy smart card. Cách thứ hai là dựa vào cấu trúc của tiền điện tử và những giao thức mật mã để có thể truy vết tìm ra kẻ gian lận (tiêu xài hai lần). Nếu như người sử dụng biết rằng họ sẽ bị bắt khi cố tính gian lận, về lý thuyết thì tỷ lệ hành động gian lận sẽ bị giảm đi. Điều thuận lợi của phương pháp là chúng không đòi hỏi những con chip đặc biệt. Hệ thống có thể được phát triển trên chương trình phần mềm (software) và có thể chạy trên máy tính cá nhân thông thường hay smartcard.

+*Tiền điện tử định danh-ngoại tuyến (Identified offline)*: Dựa vào thông tin định danh để truy vết tìm ra kẻ gian lận. Trong quá trình giao dịch, định danh

của người sử dụng được tích lũy đầy đủ trên đường đi của đồng tiền và thông tin định danh sẽ “trưởng thành” ở mỗi lần nó được tiêu xài. Những chi tiết thông tin mỗi lần giao dịch được gắn vào phần tiền điện tử, và đi với nó khi nó được chuyển từ người này sang người khác. Khi tiền điện tử chuyển tới ngân hàng, họ kiểm tra dữ liệu của nó, để xem tiền điện tử có bị tiêu xài hai lần không ?. Ngân hàng sử dụng những thông tin này để lần theo vết của những giao dịch, để phát hiện ra người nào tiêu xài hai lần.

+ *Tiền điện tử ẩn danh-ngoại tuyến (Anonymous Offline)*: Đây là dạng phức tạp nhất, bởi vì hệ thống phải làm sao vừa đảm bảo tính ẩn danh của người dùng, vừa đảm bảo có thể truy vết được định danh người dùng trong trong hợp xảy ra vi phạm (tiêu xài hai lần). Giải pháp cho hệ thống này là gắn thông tin lên đồng tiền ở mỗi lần giao dịch. Thông tin này sẽ ‘trưởng thành’ với mỗi giao dịch. Khi tiền điện tử đến ngân hàng, họ sẽ kiểm tra trong cơ sở dữ liệu xem tiền này đã được tiêu chưa. Nếu ngân hàng phát hiện tiền này đã được tiêu trước đây, thì họ sẽ sử dụng thông tin tích lũy để xác định định danh của kẻ gian lận (người tiêu xài hai lần). Tuy nhiên thông tin được tích lũy trong trường hợp này chỉ có thể dùng để lần theo vết giao dịch nếu như tiền điện tử được tiêu hai lần, nghĩa là chỉ khi có gian lận thì ngân hàng mới có thể truy lại thông tin của người sử dụng. Nếu tiền điện tử ẩn danh không bị tiêu hai lần, thì ngân hàng không thể phát hiện được định danh của người tiêu tiền, cũng như không thể xây dựng lại đường đi của tiền điện tử.

2.4 GIAO DỊCH ĐIỆN TỬ KHÔNG SỬ DỤNG TIỀN ĐIỆN TỬ

2.4.1 Dịch vụ ngân hàng điện tử

Mạng Internet, mạng viễn thông và các mạng thông tin khác giúp con người thực hiện toàn bộ hoặc một phần các giao dịch qua mạng một cách thuận tiện và nhanh chóng, vì nó khắc phục được trở ngại về khoảng cách địa lý giữa các bên tham gia giao dịch.

Theo khoản 6 và khoản 10 điều 4 Luật giao dịch điện tử được Quốc hội Việt Nam thông qua ngày 29/11/2005, giao dịch điện tử là giao dịch được thực hiện bằng phương tiện điện tử. Trong đó, phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự.

Căn cứ quy định nêu trên, giao dịch mua hàng tại quầy và thanh toán bằng thẻ tín dụng, tức quẹt thẻ vào máy bán hàng để tự động in ra sao kê thẻ và hóa đơn bán hàng thì được xem là giao dịch điện tử vì thẻ tín dụng là phương tiện điện tử.

Nhận thấy khái niệm giao dịch điện tử không chỉ giới hạn trong phạm vi mạng Internet và các mạng thông tin khác, mà còn mở rộng ra đối với tất cả các giao dịch được thực hiện bằng phương tiện điện tử. Do đó, giao dịch điện tử trong dịch vụ ngân hàng là giao dịch bằng phương tiện điện tử trong dịch vụ ngân hàng, nói cách khác là dịch vụ ngân hàng được giao dịch bằng phương tiện điện tử (gọi tắt là “dịch vụ ngân hàng điện tử”).

Trong thời gian vừa qua, hệ thống ngân hàng thương mại Việt Nam đã có những bước chuyển biến mạnh mẽ về quy mô cũng như chất lượng dịch vụ ngân hàng. Đặc biệt, đã có một số ngân hàng mạnh dạn thử nghiệm và cung cấp dịch vụ ngân hàng điện tử cho khách hàng, mang lại sự thuận tiện, hiệu quả rất lớn cho khách hàng, ngân hàng và xã hội.

Tuy nhiên, phần lớn khách hàng còn dè dặt, thăm dò và sử dụng còn hạn chế vì hình như những khái niệm như Home-banking, Phone-banking, Mobile-

banking, Internet-banking,... còn tương đối mới mẻ và lạ lẫm. Do nhiều nguyên nhân (tài chính, con người, công nghệ...) nên một số ngân hàng cũng chưa có website và dịch vụ ngân hàng điện tử vẫn còn bỏ ngỏ.

2.4.2 Tổng quan về sự phát triển ngân hàng điện tử tại Việt Nam

2.4.2.1 Dịch vụ ngân hàng điện tử (E-Banking)

Ngân hàng điện tử được hiểu là các nghiệp vụ, các sản phẩm dịch vụ ngân hàng truyền thống trước đây được phân phối trên các kênh mới như Internet, điện thoại, mạng không dây... Hiện nay, ngân hàng điện tử tồn tại dưới hai hình thức: hình thức ngân hàng trực tuyến, chỉ tồn tại dựa trên môi trường mạng Internet, cung cấp dịch vụ 100% thông qua môi trường mạng; và mô hình kết hợp giữa hệ thống ngân hàng thương mại truyền thống và điện tử hoá các dịch vụ truyền thống, tức là phân phối những sản phẩm dịch vụ cũ trên những kênh phân phối mới. Ngân hàng điện tử tại Việt Nam chủ yếu phát triển theo mô hình này.

2.4.2.2 Sự phát triển ngân hàng điện tử tại Việt Nam

Cùng với sự phát triển của thương mại điện tử, ngân hàng điện tử tại Việt Nam cũng đã có được những bước tiến quan trọng. Tuy nhiên, do tính chất còn quá mới mẻ và do khách hàng cũng chưa thực sự quan tâm lắm tới những dịch vụ này, các ngân hàng thương mại tại Việt Nam vẫn đang thận trọng và dè dặt khi tung ra những sản phẩm dịch vụ mới. Cụ thể, đối với dịch vụ PC-banking, trên thị trường mới chỉ có vài ngân hàng thương mại cung cấp dịch vụ ngân hàng tại nhà “home-banking” (Vietcombank, Incombank, ACB, Eximbank ...) và 2 ngân hàng nước ngoài là ANZ và Citibank cung cấp. Dịch vụ Phone-banking, có các ngân hàng cung cấp là VCB, ACB, Techcombank, HSBC, ANZ và Citibank... Dịch vụ Mobile-banking thì có ngân hàng Incombank, ACB và Techcombank..., ngoài ra, các ngân hàng khác chỉ mới dừng lại ở việc thiết lập các trang web chủ yếu để giới thiệu ngân hàng và cung cấp thông tin dịch vụ.

Riêng Ngân hàng Nông nghiệp và PTNTVN đang triển khai thử nghiệm dự án E-banking.

Bên cạnh đó, để phục vụ cho hệ thống thanh toán cho TMĐT, VASC đã xây dựng cổng thanh toán VASC Payment để làm cơ sở cho hệ thống thanh toán qua mạng Internet và hệ thống quản lý chứng chỉ số - VASC CA (Certificate Authority), để cung cấp chữ ký điện tử và chứng nhận điện tử để làm cơ sở pháp lý cho giao dịch điện tử, tạo niềm tin cho khách hàng cũng như nhà cung cấp dịch vụ, là xương sống cho sự phát triển thương mại điện tử trong thời gian tới.

2.4.3 Giới thiệu một số dịch vụ ngân hàng điện tử tại Việt Nam

Về nguyên tắc, thực chất của dịch vụ ngân hàng điện tử là việc thiết lập một kênh trao đổi thông tin tài chính giữa khách hàng và ngân hàng nhằm phục vụ nhu cầu sử dụng dịch vụ ngân hàng của khách hàng một cách nhanh chóng, an toàn và thuận tiện. Sau rất nhiều tìm tòi, thử nghiệm và ứng dụng, hiện nay dịch vụ ngân hàng điện tử được các ngân hàng thương mại Việt Nam cung cấp qua các kênh chính sau đây: ngân hàng tại nhà (home-banking, Internet-banking); ngân hàng tự động qua điện thoại (Phone-banking, mobile banking); ngân hàng qua mạng không dây (Wireless-banking)...

2.4.3.1 Dịch vụ ngân hàng tại nhà (home-banking):

Home-banking là kênh phân phối dịch vụ của ngân hàng điện tử, cho phép khách hàng thực hiện hầu hết các giao dịch chuyển khoản với ngân hàng (nơi khách hàng mở tài khoản) tại nhà, tại văn phòng công ty mà không cần đến ngân hàng.

Ứng dụng và phát triển Home-banking là một bước tiến mau mắn của các ngân hàng thương mại Việt Nam trước sức ép rất lớn của tiến trình hội nhập toàn cầu về dịch vụ ngân hàng. Đứng về phía khách hàng, Home-banking đã mang lại những lợi ích thiết thực: nhanh chóng- an toàn- thuận tiện. Và khẩu hiệu “Dịch vụ ngân hàng 24 giờ mỗi ngày, bảy ngày mỗi tuần” chính là ưu thế lớn nhất mà mô hình ngân hàng “hành chính” truyền thống không thể nào sánh

được. Hiện nay, dịch vụ Home-banking tại Việt Nam đã được nhiều ngân hàng tại Việt Nam ứng dụng và triển khai rộng rãi như: Ngân hàng Á Châu www.acb.com.vn; Ngân hàng công thương Việt Nam www.icb.com.vn; Ngân hàng ngoại Thương VN www.vcb.com.vn; Ngân hàng kỹ thương www.techcombank.com.vn, Ngân hàng xuất nhập khẩu Việt Nam www.eximbank.com.vn ...

Dịch vụ ngân hàng tại nhà được xây dựng trên một trong hai nền tảng: hệ thống các phần mềm ứng dụng (Software Base) và nền tảng công nghệ web (Web Base), thông qua hệ thống máy chủ, mạng Internet và máy tính con của khách hàng, thông tin tài chính sẽ được thiết lập, mã hoá, trao đổi và xác nhận giữa ngân hàng và khách hàng. Mặc dù có một số điểm khác biệt, nhưng nhìn chung, chu trình sử dụng dịch vụ ngân hàng tại nhà bao gồm các bước cơ bản sau đây:

+ Bước 1: Thiết lập kết nối.

Khách hàng kết nối máy tính của mình với hệ thống máy tính của ngân hàng qua mạng Internet, sau đó truy cập vào trang web của ngân hàng phục vụ mình (hoặc giao diện người sử dụng của phần mềm). Sau khi kiểm tra và xác nhận khách hàng (User ID, Password...), khách hàng sẽ được thiết lập một đường truyền bảo mật (https) và đăng nhập (login) vào mạng máy tính của ngân hàng.

+ Bước 2: Thực hiện yêu cầu dịch vụ.

Dịch vụ NHĐT rất phong phú và đa dạng, có thể là truy vấn thông tin tài khoản, thiết lập nghiệp vụ chuyển tiền, hủy bỏ việc chi trả séc, thanh toán điện tử ... và rất nhiều các dịch vụ trực tuyến khác.

Trên website (hoặc giao diện người sử dụng) có sẵn hệ thống Menu chọn lựa và hướng dẫn cụ thể các bước để thực hiện quá trình giao dịch. Tất cả mọi việc khách hàng phải làm chỉ là chọn dịch vụ, cung cấp thông tin theo yêu cầu của dịch vụ và của ngân hàng.

+ Bước 3:

Xác nhận giao dịch, kiểm tra thông tin và thoát khỏi mạng (thông qua chữ ký điện tử, xác nhận điện tử, chứng từ điện tử ...):

Khi giao dịch được thực hiện hoàn tất, khách hàng kiểm tra lại giao dịch và thoát khỏi mạng, những thông tin chứng từ cần thiết sẽ được quản lý, lưu trữ và gửi tới khách hàng khi có yêu cầu.

2.4.3.2 Dịch vụ ngân hàng tự động qua điện thoại (Phone-banking)

Phone-banking là hệ thống tự động trả lời hoạt động 24/24, khách hàng nhấn vào các phím trên bàn phím điện thoại theo mã do ngân hàng quy định trước, để yêu cầu hệ thống trả lời thông tin cần thiết.

Cũng như PC-banking, dịch vụ ngân hàng được cung cấp qua một hệ thống máy chủ và phần mềm quản lý đặt tại ngân hàng, liên kết với khách hàng thông qua tổng đài của dịch vụ. Thông qua các phím chức năng được định nghĩa trước, khách hàng sẽ được phục vụ một cách tự động hoặc thông qua nhân viên tổng đài.

Khi đăng ký sử dụng dịch vụ Phone-banking, khách hàng sẽ được cung cấp một mã khách hàng, hoặc mã tài khoản và tùy theo dịch vụ đăng ký, khách hàng có thể sử dụng nhiều dịch vụ khác nhau. Nhìn chung, quy trình sử dụng dịch vụ Phone-banking như sau:

- Đăng ký sử dụng dịch vụ: Khách hàng phải cung cấp các thông tin cần thiết và ký vào hợp đồng đồng ý sử dụng dịch vụ Phone-banking. Sau đó, khách hàng sẽ được cung cấp 2 số định danh duy nhất là mã khách hàng và mã khoá truy nhập hệ thống, ngoài ra khách hàng sẽ được cung cấp một mã tài khoản nhằm tạo sự thuận tiện trong giao dịch vãng như đảm bảo an toàn và bảo mật.

- Xử lý một giao dịch: Khi khách hàng quay số tới tổng đài, nhập mã khách hàng và khoá truy nhập dịch vụ, theo lời nhắc trên điện thoại, khách hàng chọn phím chức năng tương ứng với dịch vụ mình cần thực hiện giao dịch. Khách hàng có thể thay đổi, chỉnh sửa trước khi xác nhận giao dịch với ngân

hàng, chứng từ giao dịch sẽ được in ra và gửi tới khách hàng khi giao dịch được xử lý xong.

- Qua Phone-banking, khách hàng có thể sử dụng rất nhiều dịch vụ ngân hàng như : hướng dẫn sử dụng dịch vụ, giới thiệu thông tin về dịch vụ ngân hàng, cung cấp thông tin tài khoản và bảng kê các giao dịch, báo nợ, báo có, cung cấp thông tin ngân hàng như lãi suất, tỷ giá hối đoái, chuyển tiền, thanh toán hoá đơn và dịch vụ hỗ trợ khách hàng,..thực hiện mọi lúc mọi nơi kể cả ngoài giờ hành chính.

2.4.2.3 Dịch vụ ngân hàng qua ĐTDD (Mobile-banking):

Cùng với sự phát triển của mạng thông tin di động, dịch vụ ngân hàng tại Việt Nam cũng đã nhanh chóng ứng dụng những công nghệ mới này.

Mobile - banking là một kênh phân phối sản phẩm dịch vụ ngân hàng qua hệ thống mạng điện thoại di động. Về nguyên tắc, đây chính là quy trình thông tin được mã hoá, bảo mật và trao đổi giữa trung tâm xử lý của ngân hàng và thiết bị di động của khách hàng (ĐTDD, Pocket PC, Palm...).

Dịch vụ này đã được Ngân hàng Á Châu và Ngân hàng kỹ thương triển khai trong vài năm gần đây, và các ngân hàng khác cũng đã và đang bắt đầu xây dựng hệ thống và cung ứng dịch vụ Mobile-banking do tính chất thuận tiện, nhanh chóng đặc trưng của nó.

2.4.3.4 Internet banking:

Internet banking cũng là một trong những kênh phân phối các sản phẩm dịch vụ của ngân hàng, mang ngân hàng đến nhà, văn phòng, trường học, đến bất kỳ nơi đâu và bất cứ lúc nào. Với máy tính kết nối Internet, bạn sẽ được cung cấp và được hướng dẫn các sản phẩm, các dịch vụ của ngân hàng. Qua Internet banking các bạn có thể gửi đến ngân hàng những thắc mắc, góp ý với ngân hàng và được trả lời sau một thời gian nhất định. Tuy nhiên, với tính chất bảo mật không cao bằng dịch vụ ngân hàng tại nhà hoặc Kiosk-banking, dịch vụ

Internet-banking vẫn còn được cung cấp hạn chế và đòi hỏi quá trình xác nhận giao dịch phức tạp hơn.

2.4.3.5 Kiosk ngân hàng:

Là sự phát triển của dịch vụ ngân hàng hướng tới việc phục vụ khách hàng với chất lượng cao nhất và thuận tiện nhất. Trên đường phố sẽ đặt các trạm làm việc với đường kết nối Internet tốc độ cao. Khi khách hàng cần thực hiện giao dịch hoặc yêu cầu dịch vụ, họ chỉ cần truy cập, cung cấp số chứng nhận cá nhân và mật khẩu để sử dụng dịch vụ của hệ thống ngân hàng phục vụ mình. Đây cũng là một hướng phát triển đáng lưu tâm cho các nhà lãnh đạo các ngân hàng thương mại Việt Nam.

2.4.4 Ưu nhược điểm, hướng phát triển.

2.4.4.1 Ưu điểm :

- Về phía khách hàng: Ưu điểm lớn nhất của dịch vụ ngân hàng điện tử dành cho khách hàng chính là sự tiện nghi và luôn sẵn sàng của dịch vụ ngân hàng. Bây giờ, khách hàng chỉ cần gửi một tin nhắn lúc nửa đêm thay vì phải xin phép sếp ra ngoài trong giờ làm việc chỉ để đóng tiền điện thoại cho vợ là một ưu thế rõ rệt nhất của ngân hàng điện tử. Khách hàng có thể tiếp cận với ngân hàng điện tử mọi lúc mọi nơi. Bên cạnh đó, dịch vụ ngân hàng điện tử với công nghệ hiện đại đã tiết kiệm được thời gian và giảm chi phí dịch vụ cho khách hàng. Ngoài ra, khách hàng được ngân hàng phục vụ tận nơi với những thông tin nóng hổi nhất như biến động tỷ giá, tra cứu thông tin tài chính của đối tác ... Và hơn nữa, với những tiêu chuẩn chuẩn hoá, khách hàng được phục vụ tận tụy và chính xác thay vì phải tùy thuộc vào thái độ phục vụ khác nhau của các nhân viên ngân hàng.

- Về phía ngân hàng : Các giao dịch ngân hàng được tự động hoá không chỉ mang lại lợi ích cho khách hàng mà còn mang lại lợi ích thiết thực cho ngân hàng. Thông qua những dịch vụ mới, những kênh phân phối mới, ngân hàng có thể mở rộng đối tượng khách hàng, phát triển thị phần, giảm chi phí, thu hút

nguồn vốn huy động từ tiền gửi thanh toán của khách hàng, tăng thêm lợi nhuận ... bên cạnh đó, ứng dụng và phát triển những công nghệ ngân hàng hiện đại cũng giúp cho các ngân hàng luôn tự đổi mới, hoà nhập và phát triển không chỉ ở thị trường trong nước mà còn hướng tới thị trường nước ngoài.

2.4.4.1 Nhược điểm :

Tại Việt Nam, tiến trình phát triển ngân hàng điện tử đã đạt được những thành công nhất định, tuy nhiên bên cạnh đó còn có những hạn chế như:

- Chất lượng dịch vụ ngân hàng điện tử còn chưa thoả mãn khách hàng ở những cấp độ cao hơn như việc gửi tiền mặt vào tài khoản, việc đăng ký sử dụng dịch vụ... còn phải tới trực tiếp giao dịch tại chi nhánh ngân hàng, hoặc các dịch vụ ngân hàng điện tử chất lượng cao hơn còn chưa được phát triển như dịch vụ quản lý quỹ đầu tư, dịch vụ địa ốc, cho thuê tài chính...

- Cơ sở hạ tầng còn yếu kém như chất lượng mạng, tốc độ đường truyền, lỗi kỹ thuật hoặc thiết bị đầu cuối không đảm bảo chất lượng dẫn tới chất lượng dịch vụ chưa cao. Bên cạnh đó, các hệ thống ngân hàng điện tử của các ngân hàng còn phát triển tương đối độc lập, chưa có sự phối hợp, liên thông cần thiết nhằm phát huy cao nhất hiệu quả của dịch vụ mới này.

- Giao dịch ngân hàng điện tử còn phụ thuộc nhiều vào chứng từ lưu trữ truyền thống, chưa thể điện tử hoá mọi chứng từ giao dịch. Ngoài ra, việc sử dụng chữ ký điện tử, chứng nhận điện tử chưa được phổ biến rộng rãi và chưa thể hiện được ưu thế so với chữ ký thông thường.

- Bên cạnh đó, những rủi ro mới như hacker (tin tặc), virus máy tính có thể có những tác hại rất lớn không chỉ đối với ngân hàng mà còn đối với khách hàng, gây mất lòng tin của khách hàng đối với dịch vụ ngân hàng.

- Một lý do quan trọng nữa đó là quy mô và chất lượng của TMĐT còn rất thấp và phát triển chậm, cần có một hệ thống TMĐT đủ mạnh để cung cấp tất cả hàng hoá dịch vụ trên mạng, tạo tiền đề cho dịch vụ ngân hàng điện tử phát triển.

2.4.4.1 Hướng phát triển :

Trong tương lai, với trình độ và tốc độ hiện đại hoá công nghệ ngân hàng như hiện nay, các ngân hàng Việt Nam đang nỗ lực ứng dụng công nghệ mới, phát triển dịch vụ mới để tăng sức cạnh tranh, nhanh chóng hoà nhập với khu vực và thế giới. Từ những webpage giới thiệu dịch vụ ngân hàng (Giai đoạn Brochure-ware), tới website cung cấp dịch vụ ngân hàng (Giai đoạn E-commerce), các ngân hàng Việt Nam đang hướng tới việc cung cấp những dịch vụ ở cấp độ cao hơn, tăng sự chia sẻ thông tin giữa các ngân hàng, đối tác (Giai đoạn E-business) và tiến tới xây dựng mô hình ngân hàng điện tử (E-bank hay E-enterprise) thực sự , tận dụng được sức mạnh thực sự của mạng toàn cầu và cá nhân hoá dịch vụ ngân hàng cho từng đối tượng khách hàng chuyên biệt.

CHƯƠNG 3. MÔ HÌNH GIẢI PHÁP THANH TOÁN TRỰC TUYẾN

Trong mô hình này, đơn vị tiền sẽ được phát hành dưới dạng thẻ nạp, có nhiều loại thẻ mang mệnh giá khác nhau được người dùng nạp vào tài khoản. Để sử dụng hệ thống, người dùng sẽ phải *đăng ký* tạo tài khoản, hệ thống sau khi kiểm tra và xác minh các thông tin của người dùng sẽ cấp cho người dùng một *số tài khoản*. Người dùng sử dụng số tài khoản và mật khẩu để đăng nhập vào hệ thống. Khi người dùng có thể thực hiện giao dịch chuyển tiền từ tài khoản của mình sang tài khoản của người khác theo hai cách:

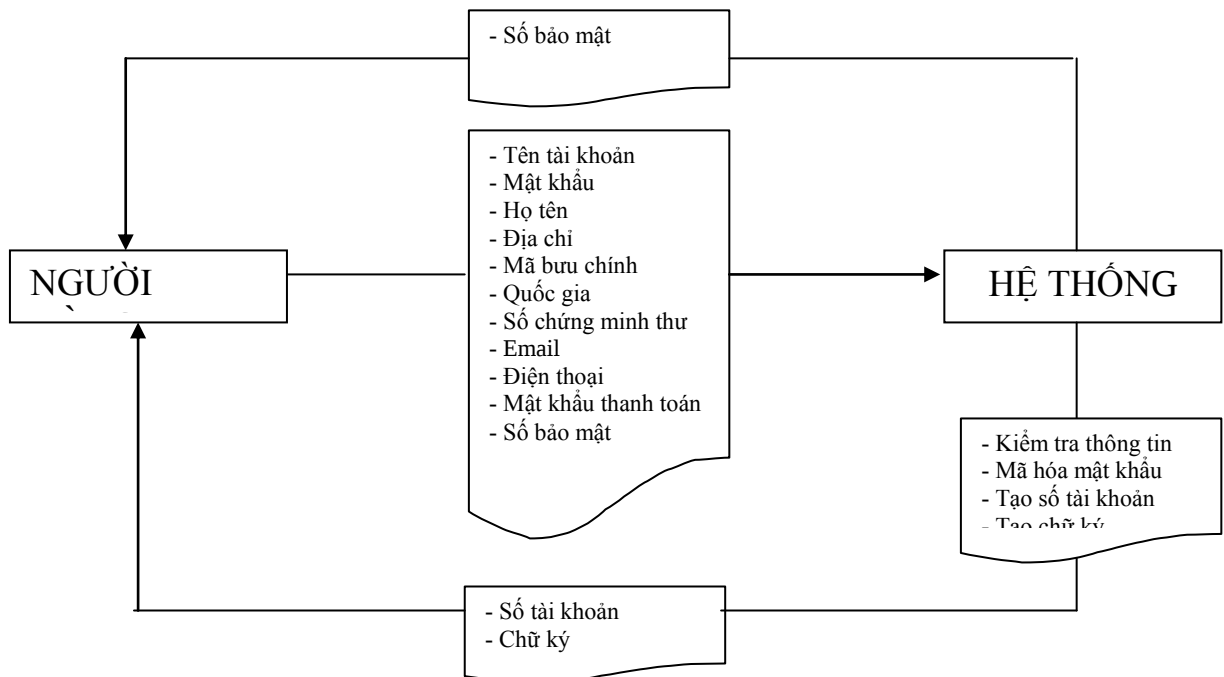
- Thực hiện trực tiếp sau khi *đăng nhập* vào hệ thống, trường hợp này được áp dụng đối với các hình thức chuyển tiền giữa những người dùng của hệ thống. Số dư trong tài khoản chuyển đi sẽ bị khấu trừ, số dư trong tài khoản chuyển đến sẽ được cộng thêm.

- Thực hiện gián tiếp thông qua các hệ thống ủy quyền, trường hợp này được áp dụng khi người dùng thực hiện thanh toán cho người dùng khác thông qua các website bán hàng trên mạng (các website này đã đăng ký tài khoản tại hệ thống). Khi giao dịch gián tiếp người dùng sẽ phải nhập vào số tài khoản và mật khẩu thanh toán khi đăng ký tài khoản, hệ thống sẽ thực hiện kiểm tra và xác nhận giao dịch.

Toàn bộ thông tin giao dịch sẽ được mã hóa và ký xác nhận và lưu trữ trong hệ thống.

Giai đoạn 1: “ĐĂNG KÝ TÀI KHOẢN”

Sơ đồ:



Các bước thực hiện:

Bước 1: HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG

Bước 2: NGƯỜI DÙNG nhập các thông tin xác minh và số bảo mật nhận được rồi gửi lại cho HỆ THỐNG.

Bước 3: HỆ THỐNG kiểm tra và xác minh các thông tin của người dùng.

- Nếu đúng sẽ tạo một tài khoản mới và bộ chữ ký.
- Mã hóa mật khẩu và mật khẩu thanh toán của NGƯỜI DÙNG.
- Gửi số tài khoản và chữ ký cho người dùng.

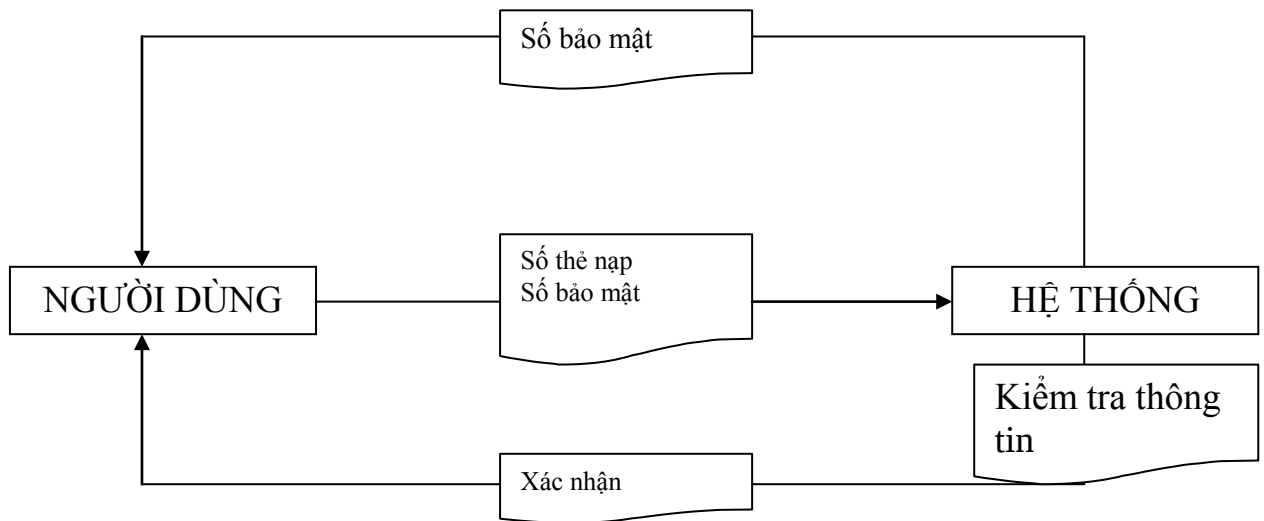
Ghi chú:

Số bảo mật: Được sử dụng để ngăn chặn hình thức tấn công tràn hệ thống của hacker.

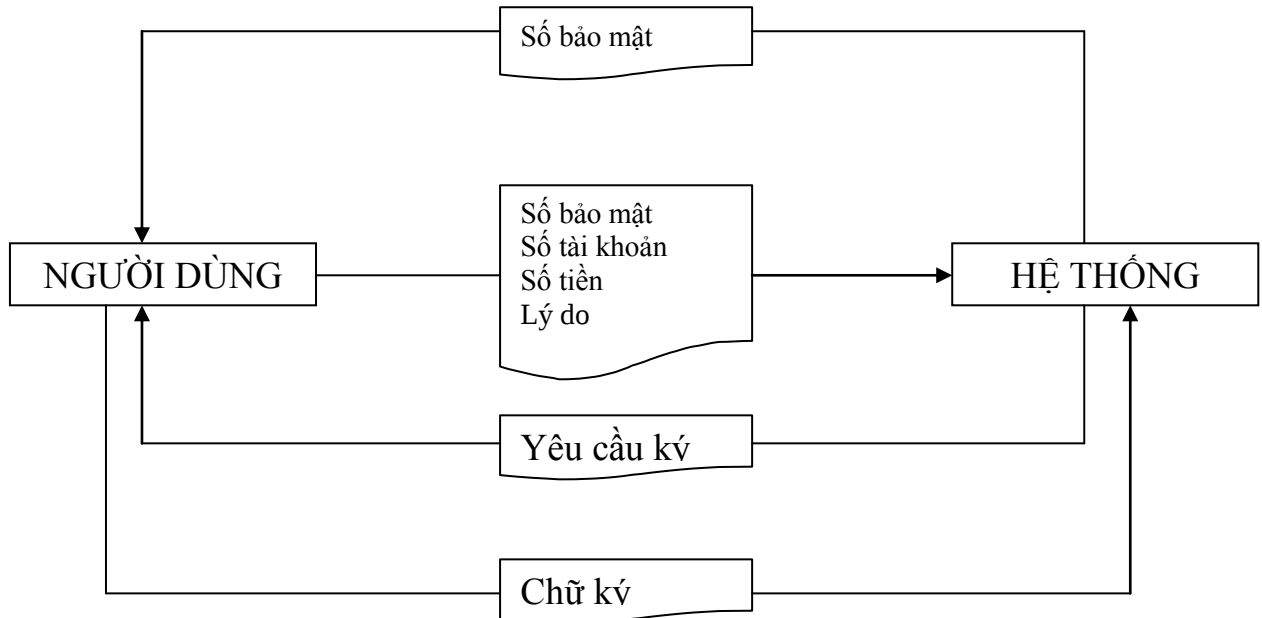
Chữ ký: Người dùng sẽ ký trên các giao dịch sau này để xác nhận.

Các kỹ thuật sử dụng:

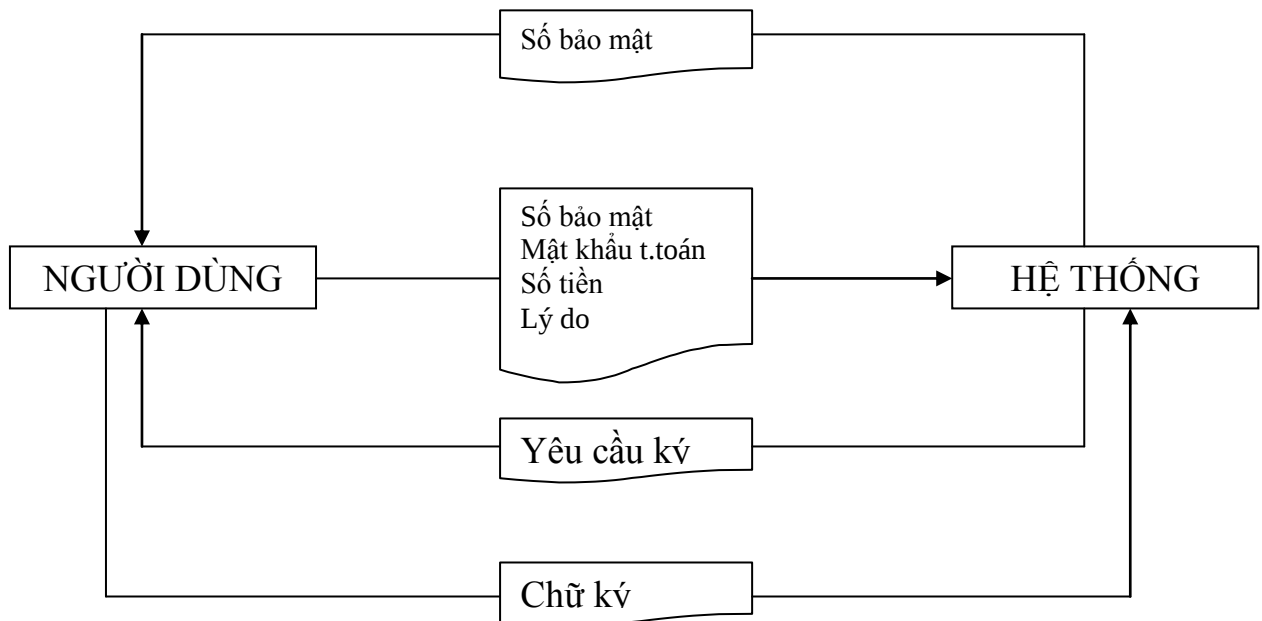
- Kỹ thuật sinh số ngẫu nhiên.
- Kỹ thuật tóm lược thông điệp MD5.
- Kỹ thuật chữ ký số RSA.

Giai đoạn: “NẠP TIỀN”**Sơ đồ:****Các bước thực hiện:****Bước 1:** HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG.**Bước 2:** NGƯỜI DÙNG nhập số tài khoản, mật khẩu và số bảo mật.**Bước 3:** HỆ THỐNG kiểm tra thông tin và xác nhận NGƯỜI DÙNG**Bước 4:** NGƯỜI DÙNG chọn chức năng “Nạp tiền”.**Bước 5:** HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG.**Bước 6:** NGƯỜI DÙNG nhập số thẻ nạp và số bảo mật rồi gửi cho HỆ THỐNG**Bước 7:** HỆ THỐNG kiểm tra các thông tin, nếu chính xác thực hiện cộng thêm tiền vào tài khoản của NGƯỜI DÙNG.**Các kỹ thuật sử dụng:**

- Kỹ thuật sinh số ngẫu nhiên.

Giai đoạn: “GIAO DỊCH TRỰC TIẾP”**Sơ đồ:****Các bước thực hiện:****Bước 1:** HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG.**Bước 2:** NGƯỜI DÙNG nhập số tài khoản, mật khẩu và số bảo mật.**Bước 3:** HỆ THỐNG kiểm tra thông tin và xác nhận NGƯỜI DÙNG.**Bước 4:** NGƯỜI DÙNG chọn chức năng “giao dịch”.**Bước 5:** HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG.**Bước 6:** NGƯỜI DÙNG nhập số tài khoản chuyển tiền đến, số lượng tiền chuyển, lý do chuyển tiền và số bảo mật**Bước 7:** HỆ THỐNG kiểm tra các thông tin, nếu chính xác yêu cầu NGƯỜI DÙNG ký lên các thông tin và thực hiện giao dịch.**Bước 8:** NGƯỜI DÙNG ký xác nhận lên thông tin giao dịch và gửi lại cho HỆ THỐNG**Các kỹ thuật sử dụng:**

- Kỹ thuật sinh số ngẫu nhiên.
- Kỹ thuật tóm lược thông điệp MD5.
- Kỹ thuật chữ ký số RSA.

Giai đoạn: “GIAO DỊCH GIÁN TIẾP”**Sơ đồ:****Các bước thực hiện:**

Bước 1: NGƯỜI DÙNG thực hiện chức năng thanh toán tại một website khác đã thực hiện đăng ký sử dụng chức năng giao dịch của HỆ THỐNG.

Bước 2: HỆ THỐNG sinh ngẫu nhiên số bảo mật gửi cho NGƯỜI DÙNG.

Bước 3: NGƯỜI DÙNG nhập số tài khoản của NGƯỜI DÙNG, mật khẩu thanh toán và số bảo mật.

Bước 4: HỆ THỐNG kiểm tra thông tin và xác nhận NGƯỜI DÙNG.

Bước 5: HỆ THỐNG kiểm tra các thông tin, nếu chính xác yêu cầu NGƯỜI DÙNG ký lên các thông tin và thực hiện giao dịch.

Bước 6: NGƯỜI DÙNG ký xác nhận lên thông tin giao dịch và gửi lại cho HỆ THỐNG

Các kỹ thuật sử dụng:

- Kỹ thuật sinh số ngẫu nhiên.
- Kỹ thuật tóm lược thông điệp MD5.
- Kỹ thuật chữ ký số RSA.

CHƯƠNG 4. CHƯƠNG TRÌNH MÔ PHỎNG

4.1 Yêu cầu phần cứng & phần mềm thử nghiệm

4.1.1 Server

Phần cứng:

- Server IBM, Xeon, 4GB RAM, Windows Server 2003

Phần mềm:

- Web server.
- Hệ quản trị cơ sở dữ liệu Microsoft SQL Server 2000.

4.2.1 Client

Phần cứng:

- E2200, 2GB RAM, Windows XP & Windows Vista.

Phần mềm:

- Hỗ trợ ASP.
- Bộ công cụ phát triển ứng dụng web Macromedia Dreamweaver 8.
- Trình duyệt Internet Explorer, Firefox.
- Đường truyền Internet ADSL.

4.2 Chương trình mô phỏng

Giao diện chương trình

4.2.1 Đăng ký tài khoản

ĐĂNG KÝ TÀI KHOẢN	
Thông tin tài khoản	
Các thông tin tài khoản người dùng	
Tên tài khoản (Account Name):	
Mật khẩu (Password):	
Lặp lại mật khẩu (Retype password):	
Thông tin cá nhân	
Các thông tin cá nhân của người đăng ký tài khoản	
Họ đệm (First name):	
Tên (Last name):	
Địa chỉ (Address):	
Thành phố (City):	
Mã bưu chính (Zip code):	
Quốc gia (Country):	Vietnam ▾
Số chứng minh thư (Id Card):	
Thư điện tử (Email):	
Số điện thoại (Phone):	

Hình 2.1. Đăng ký tài khoản

4.2.2 Đăng nhập

ĐĂNG NHẬP TÀI KHOẢN

Thông tin tài khoản

Nhập thông tin tài khoản và số bảo mật
Nếu chưa có tài khoản xin vui lòng [đăng ký](#).

Số tài khoản (ID Account):	
Mật khẩu (Password):	
Số bảo mật (Security Number):	9 1 0 9 3 2
Nhập dãy số trên (Enter security number):	

Hình 2.2. Đăng nhập

4.2.3 Thông tin tài khoản và nạp tiền

SỐ DƯ TÀI KHOẢN

Số tài khoản: 43

Tên tài khoản (Account name): **matrixcosmos**
Tên chủ tài khoản (Full Name): **Vu Nam**
Số dư tài khoản (Balance): **878790 VNĐ**

Nạp tiền vào tài khoản

Cào dãy số trên thẻ và nhập thông tin để nạp tiền

Dãy số trên thẻ cào (Card Number):	
Số bảo mật (Security Number):	1 3 3 8 5 1
Nhập dãy số trên (Enter security number):	

Hình 2.3. Thông tin tài khoản và nạp tiền

4.2.4 Thanh toán

THANH TOÁN

Số tài khoản: 43
Tên tài khoản (Account name): **matrixcosmos**
Tên chủ tài khoản (Full Name): **Vu Nam**
Số dư tài khoản (Balance): **878790 VNĐ**

Thanh toán cho tài khoản khác
Nhập thông tin thanh toán cho tài khoản khác và thực hiện thanh toán

Số tài khoản nhận (Pay):	(Nhập vào số tài khoản người nhận)
Số tiền chuyển (Amount):	
Lý do chuyển (Memo):	
Số bảo mật (Security Number):	4 1 0 6 7 2
Nhập dãy số trên (Enter security number):	

Hình 2.4. Thanh toán

4.2.5 Lịch sử giao dịch

Số tài khoản: 43

Tên tài khoản (Account name): matrixcosmos

Tên chủ tài khoản (Full Name): Vu Nam

Số dư tài khoản (Balance): 878790 VNĐ

Tiền chuyển đến

Thông tin giao dịch tiền chuyển đến

STT

Từ tài khoản

Số tiền

Lý do chuyển

Thời gian chuyển

Tiền chuyển đi

Thông tin giao dịch tiền chuyển đi

STT	Chuyển đến	Số tiền	Lý do chuyển	Thời gian chuyển
1	24	50000	2i3u4yiu	6/13/2009 6:44:28 AM
2	24	900	Thanh toán từ cửa hàng online của shonline	6/19/2009 7:41:33 AM
3	24	1400	Thanh toán từ cửa hàng online của shonline	6/19/2009 7:48:50 AM
4	24	1400	Thanh toán từ cửa hàng online của shonline	6/20/2009 9:29:10 AM
5	24	1400	Thanh toán từ cửa hàng online của shonline	6/20/2009 11:01:28 AM
6	40	654	56465	6/20/2009 11:26:52 AM
7	40	65456	656	6/20/2009 11:27:33 AM

Hình 2.5. Lịch sử giao dịch

4.2.6 Thông tin người dùng

Thông tin tài khoản	
Các thông tin tài khoản người dùng	
Tên tài khoản (Account Name):	matrixcosmos
Mật khẩu (Password):	•••••
Lặp lại mật khẩu (Retype password):	•••••

Thông tin cá nhân	
Các thông tin cá nhân của người đăng ký tài khoản	
Họ đệm (First name):	Vu
Tên (Last name):	Nam
Địa chỉ (Address):	Hai phong
Thành phố (City):	Hai pong
Mã bưu chính (Zip code):	2349878
Quốc gia (Country):	VN

Hình 2.6. Thông tin người dùng

KẾT LUẬN

Thông qua quá trình thực hiện Đồ án tốt nghiệp với đề tài “Giải pháp thanh toán trực tuyến.”, bản thân em tự thấy mình đã thu được các kết quả sau:

- Thêm hiểu biết về Thương mại điện tử nói chung và các giải pháp Thanh toán điện tử nói riêng.
- Có được các kinh nghiệm thực tế khi triển khai một hệ thống demo giải pháp thanh toán.
- Cài đặt một website thực hiện giải pháp dựa trên ngôn ngữ ASP.

Trong quá trình hoàn thiện đồ án, do còn có nhiều thiếu sót mong được các thầy cô góp ý, giúp đỡ để chương trình của em ngày càng hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

- [1]. D.Chaum, A.Fiat, and M.Naor, *Untraceable electronic cash*, In Advances in Cryptology-Crypto '88.
- [2]. Brands Stefan, *An efficient Off-line electronic cash system based on the representation problem*, Technical report.
- [3]. Rüçhan Ziya, *Encryption Techniques, Cash Security Protocols, Cash systems*, The degree of master of Sciences in Engineering Management.
- [4]. Yiannis Tsiounis, *Efficient Electronic Cash New Notions and Techniques*.
- [5]. *Giải pháp thanh toán điện tử* - Báo cáo KH – Sv. Nguyễn Viết Huy – ĐHDL HP.
- [6]. *Thanh toán điện tử* - Luận văn tốt nghiệp – Sv. Lê Duy Hưng – ĐH Kinh tế.
- [7]. *Kiến thức thương mại điện tử* - Ts. Nguyễn Đăng Hậu – Viện Đào tạo Công nghệ & Quản lý Quốc tế.
- [8]. *Tổng quan về Thương mại điện tử* - Trần Hữu Linh – Vụ thương mại điện tử, Bộ Thương mại.