BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN TRẦN HƯNG

TRẦN THỊ THẬP

BÀI GIẢNG

THANH TOÁN ĐIỆN TỬ

Tháng 12 năm 2019

MỞ ĐẦU

Học phần Thanh toán điện tử là học phần kiến thức chuyên môn trong chương trình đào tạo đại học ngành Quản trị Kinh doanh và ngành Thương mại Điện tử của Học viện Công nghệ Bưu chính Viễn thông.

Bài giảng Thanh toán điện tử được biên soạn nhằm hỗ trợ cho hoạt động nghiên cứu và học tập học phần này. Bài giảng được kết cấu thành bốn chương.

Chương 1: Tổng quan về thanh toán điện tử. Chương này trình bày các vấn đề chính như: Cơ sở hình thành và phát triển thanh toán điện tử; Những vấn đề chung về thanh toán điện tử; Tình hình thanh toán điện tử tại Việt Nam và trên thế giới.

Chương 2: Hệ thống thanh toán điện tử. Chương này giới thiệu các hệ thống thanh toán điện tử điển hình gồm: Thẻ điện tử; Ví điện tử; Vi thanh toán điện tử; Chuyển khoản điện tử; Séc điện tử; Thanh toán bằng thư tín dụng và bao thanh toán; Thanh toán bằng trao đổi dữ liệu điện tử (EDI).

Chương 3: Bảo mật trong thanh toán điện tử. Chương này trình bày các vấn đề chính như: Vấn đề bảo mật trong thanh toán điện tử; Các loại hình tấn công; Các biện pháp bảo mật trong thanh toán điện tử;

Chương 4: Lựa chọn giải pháp trong thanh toán điện tử; Chương này bao gồm các nội dung chính: Cổng thanh toán điện tử; Tiêu chí lựa chọn cổng thanh toán điện tử; Một số cổng thanh toán điện tử điển hình.

Bài giảng do TS. Nguyễn Trần Hưng và TS. Trần Thị Thập biên soạn. Mặc dù tập thể tác giả đã có nhiều cố gắng nhưng chắc chắn bài giảng khó tránh khỏi những thiếu sót. Chúng tôi rất mong nhận được ý kiến đóng góp của bạn đọc để tiếp tục hoàn thiện và nâng cao hơn nữa chất lượng bài giảng.

Chúng tôi xin chân thành cảm ơn các bạn đồng nghiệp đã góp ý, giúp đỡ trong quá trình biên soạn bài giảng này.

Tập thể tác giả

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VỀ THANH TOÁN ĐIỆN TỬ

1.1 Cơ sở hình thành và phát triển thanh toán điện tử

1.1.1 Lịch sử phát triển của các hình thái tiền tệ

1.1.1.1 Hóa tệ

Hóa tệ là hình thái cổ xưa và sơ khai nhất của tiền tệ, theo đó một loại hàng hóa nào đó do được nhiều người ưa chuộng nên có thể tách ra khỏi thế giới hàng hóa nói chung để thực hiện các chức năng của tiền tệ, tức là thực hiện các chức năng mà các hàng hóa thông thường khác không có được. Loại hàng hóa trung gian này phải thực sự có giá trị, được nhiều người chấp nhận, được dùng để trao đổi. Hàng hóa đặc biệt này đóng vai trò vật ngang giá chung và được sử dụng thường xuyên để trao đổi với những hàng hóa khác. Hóa tệ có thể chia thành hai loại: *hóa tệ phi kim loại* và *hóa tệ kim loại*.

- ✓ **Hoá tệ phi kim loại / hóa tệ phi kim**

Trong thời kỳ đầu, khoảng hai nghìn năm trước công nguyên, vật trung gian trao đổi thường được chọn từ một loại hàng hoá có giá trị sử dụng cần thiết chung cho nhiều người, có thể bảo tồn lâu ngày đồng thời mang tính chất phổ biến, đặc trưng cho từng địa phương, nơi diễn ra quan hệ trao đổi.

Hoá tệ phi kim là tiền tệ dưới dạng các hàng hoá (trừ kim loại). Đây là hình thái cổ nhất của tiền tệ, rất thông dụng trong các xã hội cổ xưa. Trong lịch sử đã có rất nhiều loại hàng hoá khác nhau từng được con người dùng làm tiền tệ. Trong cuốn "Primitive money" – Tiền nguyên thủy, của Paul Einzig viết năm 1964, ông đã đưa ra những thống kê khá thú vị sau về những loại tiền cổ xưa mà theo ông nhiều số trong đó vẫn còn được sử dụng cho đến cả ngày nay. Đó là: răng cá voi ở đảo Fiji, gỗ đàn hương ở Hawaii, lụa ở Trung Quốc, gạo ở Philippines, nô lệ ở Châu Phi xích đạo, Nigeria, Ailen, tuần lộc ở nhiều nơi thuộc Nga, bơ ở Na Uy, da ở Pháp và Ý, rượu Rum ở Australia, bộ lông vẹt đỏ ở quần đảo Santa Cruz (vẫn còn cho đến năm 1961), hạt tiêu ở Sumatra, đường ở đảo Barbados, những chuỗi vỏ sò của những thổ dân da đỏ Bắc Mỹ, bò và cừu ở Hy Lạp và La mã, muối ở nhiều nơi…

Hóa tệ phi kim là hình thức sơ khai nhất của hình thái tiền tệ, chính vì vậy nên sau khi được sử dụng, hóa tệ phi kim đã bộc lộ một số hạn chế. Việc sử dụng hàng hoá làm tiền tệ gây nhiều khó khăn, bất lợi. Mỗi loại hàng hóa làm hóa tệ phi kim có giá trị trong mỗi địa phương nhất định, chính vì thế hóa tệ phi kim có phạm vi trao đổi hạn chế trong vùng, một địa phương nhất định. Nhược điểm tiếp theo là dễ hư hỏng, khó bảo quản, thường cồng kềnh, tốn kém chi phí vận chuyển. Đặc biệt là khó có thể chia nhỏ theo những tỷ lệ nhất định khi trao đổi mà không làm biến đổi chất lượng của nó. Chính điều này đã khiến cho hoá tệ phi kim loại dần bị đào thải và thay thế vào đó là thời kỳ sử dụng hoá tệ kim loại.

- ✓ **Hóa tệ kim loại**

Khi phát hiện ra kim loại, người ta nhận thấy kim loại có thể khắc phục được những nhược điểm của hóa tệ phi kim loại, chẳng hạn như bền hơn, dễ bảo quản hơn, dễ vận chuyển hơn, có thể chia nhỏ. Với những thuộc tính ưu việt này, người ta có khuynh hướng nhanh chóng chuyển sang sử dụng kim loại làm tiền tệ. Kim loại được sử dụng để làm hóa tệ kim loại đầu tiên là kẽm sau đó đồng rồi đến bạc. Đầu thế kỷ thứ mười chín, với những tính chất

ưu việt của mình, vàng bắt đầu đóng vai trò là vật ngang giá chung. Vàng lúc đó được sử dụng làm loại tiền tệ chính, còn bạc, đồng được sử dụng khi thiếu vàng.

Vàng làm hóa tệ kim loại có một số ưu điểm: Không bị giới hạn về phạm vi địa lý. Do đặc tính lý hóa của vàng, đây là một kim loại tương đối trơ (hầu như không tác động với các hóa chất trong môi trường), không bị biến đổi dưới tác động của môi trường/ bền, dễ bảo quản, dễ chia nhỏ, dễ dát mỏng. Ngoài ra việc chia nhỏ thành đơn vị và nhập những đơn vị nhỏ thành đơn vị lớn hơn rất dễ dàng và hầu như vẫn bảo tồn được giá trị của chúng, không bị biến đổi về màu sắc và chất lượng. Dùng vàng, bạc làm tiền tệ thì rất tiện lợi cho lưu thông, không cần khối lượng lớn nhưng có thể trao đổi được với những hàng hóa có giá trị cao…

Bên cạnh đó, vàng rất hấp dẫn, được nhiều người ưa thích. Nhu cầu sử dụng vàng xuất hiện sớm, nhu cầu ngày càng tăng. Chúng ta biết rằng, vàng chưa chắc đã là kim loại quý hiếm nhất nhưng nhu cầu của xã hội về vàng đã xuất hiện rất sớm trong lịch sử và ngày càng tăng làm cho vàng trở thành một thứ hàng hoá rất hấp dẫn, được nhiều người ưa thích. Vì vậy, việc dùng vàng trong trao đổi dễ dàng được chấp nhận trên phạm vi rộng lớn. Bên cạnh đó, giá trị vàng rất ổn định. Giá trị của vàng ổn định trong thời gian tương đối dài, ít chịu ảnh hưởng của năng suất lao động tăng lên như các hàng hoá khác. Sự ổn định của giá trị vàng là do năng suất lao động sản xuất ra vàng tương đối ổn định. Ngay cả việc áp dụng tiến bộ kỹ thuật vào khai thác cũng không làm tăng năng suất lao động lên nhiều. Điều này làm cho tiền vàng luôn có được giá trị ổn định, một điều kiện rất cần thiết để nó có thể chấp hành tốt các chức năng tiền tệ.

Tuy nhiên, dùng vàng làm hóa tệ cũng có một số nhược điểm, khi nền kinh tế ngày càng phát triển, nhu cầu trao đổi hàng hoá ngày càng tăng đòi hỏi cần thêm nhiều tiền hơn thì tiền vàng và bạc không đáp ứng được nhu cầu của nền kinh tế dẫn đến việc thiếu hụt vàng trong lưu thông. Bên cạnh đó, nếu trao đổi với một lượng hàng hóa, dịch vụ có giá trị lớn các vùng, quốc gia với nhau thì sử dụng vàng để thanh toán trở nên cồng kềnh, khó vận chuyển, và rất dễ bị cướp bóc. Mặt khác, trong quá trình lưu thông, tiền vàng dần bị hao mòn tự nhiên, hàm lượng vàng pháp định trong đồng tiền bị giảm đi nhưng khi thực hiện chức năng phương tiện thanh toán người dân vẫn chấp nhận những đồng tiền này như những đồng tiền mới đúc. Phát hiện ra điều này, sở đúc tiền của các quốc gia đã chủ động giảm bớt hàm lượng vàng trong các đồng tiền này. Dần dần, người ta không dùng vàng để làm tiền nữa mà dùng các kim loại rẻ tiền như kẽm, đồng hoặc hợp kim làm ra tiền. Xã hội chuyển sang sử dụng một loại tiền mới đó là tín tệ.

1.1.1.2 Tín tệ

Tín tệ là loại tiền tệ được đưa vào lưu thông nhờ vào sự tín nhiệm của công chúng, chứ bản thân nó không có hoặc có giá trị không đáng kể. Nó được sử dụng thay thế cho tiền vàng và tiền bạc (là những loại tiền thực). Tín tệ có hai loại: tín tệ kim loại và tiền giấy.

- ✓ **Tín tệ kim loại**

Tín tệ kim loại là loại tín tệ được đúc bằng kim loại. Đặc điểm của tín tệ kim loại là giá trị của kim loại đúc thành tiền và giá trị ghi trên bề mặt đồng tiền không có liên hệ gì với nhau, tức là giá trị danh nghĩa cao hơn giá trị thực tế.

Tín tệ kim loại ra đời giúp sản xuất và trao đổi hàng hoá diễn ra thuận lợi hơn, nhu cầu tiền không còn phải phụ thuộc vào khối lượng vàng nữa. Tuy nhiên, với nền kinh tế ngày

càng phát triển thì tín tệ kim loại lại bộc lộ những nhược điểm vốn có của kim loại. Nếu trao đổi với khối lượng hàng hoá lớn, chủ thể trao đổi cách xa nhau về địa lý thì việc thanh toán rất bất tiện, nặng nề, tốn kém chi phí lưu thông. Vòng quay của tiền dài nên cần nhiều tiền hơn nhu cầu thực tế. Bên cạnh đó, sử dụng tín tệ là kim loại cũng rất khó lưu trữ, bất tiện trong việc mang đi lại. Để giải quyết nhược điểm này, xã hội chuyển sang sử dụng một loại tiền mới có nhiều ưu điểm hơn đó là tiền giấy.

✓ **Tín tệ là tiền giấy**

Tiền giấy là tín tệ phi kim loại. Tiền giấy làm tín tệ có một số ưu điểm: Thanh toán dễ dàng, dễ mang theo để làm phương tiện trao đổi hàng hóa, thanh toán nợ; thuận lợi khi thực hiện chức năng dự trữ giá trị. Trong phát hành, bằng cách thay đổi các con số trên mặt đồng tiền, một lượng giá trị lớn hay nhỏ được biểu hiện.

Bên cạnh đó, tín tệ là tiền giấy cũng có một số hạn chế: Chỉ có ngân hàng nhà nước mới có quyền phát hành ra tiền tệ; thủ tục rườm ra khi gửi tiền, chuyển tiền; bị rào cản giới hạn về không gian và thời gian; bên cạnh đó chi phí quản lý tiền giấy vẫn còn cao dẫn tới khó khăn trong việc quản lý.

1.1.1.3 Tiền điện tử

Với sự phát triển của CNTT và viễn thông đã cho phép các ngân hàng thay đổi cách thức truyền thông từ việc xử lý các chứng từ giấy bằng hình thức thông tin hiện đại hơn đó là thanh toán điện tử.

Trong thanh toán điện tử, tiền nằm trong các tài khoản của ngân hàng nào được lưu trữ trong hệ thống máy tính của ngân hàng đó. Khi tiền được lưu trữ trong hệ thống máy tính gọi là tiền số hóa hay tiền điện tử. Tiền điện tử là tiền tệ tồn tại dưới hình thức dữ liệu điện tử được số hoá. Tiền điện tử ra đời không phủ nhận sự tồn tại của tiền giấy, nó là một mặt biểu hiện của tiền giấy.

1.1.2. Quá trình phát triển của thanh toán điện tử

Tiền điện tử ra đời cũng là lúc đánh dấu sự phát triển của thanh toán điện tử. Khi nói đến thanh toán điện tử nói chung, người ta gắn sự phát triển của thanh toán điện tử với thẻ thanh toán.

- Năm 1949

Thẻ thanh toán đầu tiên được biết đến, ra đời vào năm 1949 do ông Frank McNamara, một doanh nhân người Mỹ sáng chế. Có một lần sau khi dùng bữa tối tại một nhà hàng với đối tác ở New York, ông bỗng phát hiện ra mình không mang theo tiền mặt. Ông phải gọi điện cho vợ nhanh chóng mang tiền đến thanh toán. Tình trạng khó xử này đã khiến ông mày mò chế tạo một phương tiện chi trả tiền mặt trong những trường hợp tương tự như thế. Và quyết tâm một năm sau trở lại, ông sẽ không bị tình trạng khó xử đó nữa. Thế là lần đầu tiên Frank McNamara cho ra đời loại thẻ mang tên "Diners Club".

- Năm 1950

Vào đầu những năm 1950, nhờ vật liệu tổng hợp PVC (Polyvinylclorua) giá rẻ, người ta đã sản xuất hàng loạt thẻ nhựa phù hợp cho việc sử dụng hàng ngày thay cho việc dùng thẻ bằng giấy trước đây. Thẻ thanh toán bằng nhựa đầu tiên được phát hành bởi "Diners Club" vào năm 1950. Chính điều đó đã gợi lên một ý tưởng kinh doanh thẻ đối với Frank

McNamara, trong vòng một năm đã có 200 người dùng loại thẻ đa công dụng đầu tiên trên thế giới. Thẻ cho phép người dùng có thể ghi nợ tại một số nhà hàng và khu giải trí. Thời gian đầu chỉ có khoảng 27 nhà hàng và khách sạn chấp nhận những thẻ này.

Ban đầu chức năng của những thẻ này khá đơn giản, đó là phương tiện lưu trữ dữ liệu được bảo vệ nhằm tránh giả mạo và sửa đổi. Thông tin chung như tên nhà phát hành thẻ được in trên bề mặt thẻ, trong khi những thông tin cá nhân như tên của chủ thẻ và số thẻ thì được dập nổi. Nhiều thẻ có thêm chỗ ký tên để chủ thẻ ký tên dành cho tham khảo. Trong thế hệ thẻ phát hành đầu tiên này, việc bảo vệ chống lại sự giả mạo dựa trên những đặc điểm trực quan như phần in trên thẻ và phần ký tên. Vì thế sự an toàn của hệ thống phụ thuộc khá nhiều sự tỉnh táo của người chịu trách nhiệm chấp nhận thẻ. Sau này việc dùng thẻ phát triển tăng vọt nên những đặc điểm trực quan này không còn hiệu quả, đặc biệt là các mối đe dọa từ các tổ chức tội phạm đang phát triển nhanh. Một số tài liệu gọi còn gọi thế hệ này là *thẻ khắc chữ nổi* (embossing card).

Tiến bộ đầu tiên của thẻ nhựa là dùng dải từ trên mặt sau của thẻ, cho phép dữ liệu số được lưu trữ trên thẻ dưới dạng máy có thể đọc được để hỗ trợ thêm vào thông tin trực quan. Điều này làm giảm khả năng dùng biên nhận giấy, tuy nhiên đối với loại thẻ này chữ ký khách hàng vẫn được yêu cầu trên ứng dụng thẻ tín dụng truyền thống như là một hình thức định danh người dùng. Một số tài liệu còn gọi thế hệ này là *thẻ băng từ* (magnetic strip).

Sự phát triển tiếp theo của thẻ là thay thế giao dịch dựa trên giấy bằng xử lý dữ liệu điện tử. Vì vậy cần thiết phải có một phương pháp khác được sử dụng để xác thực định danh người dùng. Phương pháp được sử dụng rộng rãi liên quan đến một con số định danh cá nhân bí mật, hay còn gọi là PIN (personal identification number). Những thẻ dập nổi với dải từ vẫn còn là loại thẻ được sử dụng thông thường cho các giao dịch tài chính đến thời điểm hiện nay.

Tuy nhiên, công nghệ từ có một điểm yếu quan trọng là dữ liệu lưu trữ trên dải từ có thể bị đọc, xóa và thay đổi bởi bất cứ người nào với thiết bị cần thiết. Vì thế không thích hợp cho việc lưu trữ dữ liệu bí mật.

- Năm 1974

Thế hệ thẻ cải tiến tiếp theo sau thẻ từ là thẻ thông minh. Sự phát triển của thẻ thông minh đi liền với sự phát triển của các hệ thống xử lý dữ liệu điện tử, dẫn đến khả năng sáng chế ra nhiều giải pháp mới. Sự phát triển to lớn của vi điện tử những năm 1970 cho phép tích hợp dữ liệu và xử lý logic trong một con chip silicon đơn có kích thước chỉ bằng một vài mili mét vuông. Ý tưởng kết hợp một mạch tích hợp vào một thẻ định danh đã được sáng chế bởi hai nhà phát minh người Đức Jurgen Dethloff và Helmut Grotrupp năm 1968. Sau đó, năm 1979 ra đời một sáng chế tương tự của Kunitaka Arimura ở Nhật Bản. Tuy nhiên sự phát triển thật sự đầu tiên của thẻ thông minh là khi Roland Moreno đăng ký sáng chế thẻ thông minh ở Pháp năm 1974. Và chỉ lúc đó công nghệ bán dẫn mới có khả năng cung cấp các mạch tích hợp cần thiết với giá chấp nhận được.

- Năm 1984

Một bước đột phá lớn của thẻ vào năm 1984 là khi French PTT (post, telegraph and telephone) đã thành công trong việc thử nghiệm thẻ điện thoại. Trong lĩnh vực thử nghiệm này, thẻ thông minh đã chứng minh được sự nổi trội về tính an toàn cao, ngoài ra thẻ thông minh còn có khả năng được sử dụng linh hoạt trong các ứng dụng trong tương lai.

Các mạch tích hợp ban đầu được sử dụng trong thẻ điện thoại là những *chip nhớ* (memory chip) nhỏ, đơn giản và không đắt tiền với một sécurity logic chuyên biệt cho phép số dư thẻ giảm xuống trong khi vẫn chống lại các thao tác bất hợp pháp. Những chip vi xử lý sau này thường lớn hơn và phức tạp hơn, lần đầu tiên được sử dụng số lượng lớn ở các ứng dụng truyền thông, đặc biệt trong truyền thông di động.

Năm 1988, bưu điện Đức đóng vai trò tiên phong trong việc giới thiệu thẻ vi xử lý hiện đại dùng công nghệ EEPROM như một thẻ chứng thực cho các *mạng điện thoại di động tương tự* (analog mobile).

Năm 1991, tại các nước Châu Âu, thẻ thông minh được ứng dụng vào công nghệ di động GSM, thẻ SIM cho điện thoại di động ra đời, đặt nền tảng cho sự phát triển vũ bão của công nghệ di động ở hơn 170 quốc gia như hiện nay.

Sự bùng nổ dùng thẻ thông minh bắt đầu trong thập niên 90, khi có sự xuất hiện của SIM dùng trong thiết bị điện thoại di động GSM ở châu Âu. Cùng với việc mạng di động mở rộng khắp châu Âu, thẻ thông minh ngày càng trở nên thông dụng.

Không giống như thành công rực rỡ của thẻ thông minh trong lĩnh vực truyền thông, việc áp dụng thẻ thông minh trong lĩnh vực tài chính nhằm thay thế thẻ từ gặp khó khăn do đòi hỏi về an toàn và bảo mật thông tin do đặc thù thông tin nhạy cảm của lĩnh vực tài chính.

- Năm 1994

Một mốc quan trọng trong việc sử dụng thẻ thông minh cho việc thanh toán trên toàn thế giới trong tương lai là sự hoàn thiện của chuẩn kỹ thuật EMV. Đó là một sản phẩm kết quả của nỗ lực liên kết giữa ba tổ chức thẻ lớn nhất thế giới Europay, MasterCard và Visa. Phiên bản kỹ thuật đầu tiên là vào năm 1994. Đến năm 1998, một phiên bản khác tin cậy hơn ra đời. EMVco, công ty chịu trách nhiệm bảo trì lâu dài hệ thống này, đã nâng cấp chuẩn kỹ thuật vào năm 2000 và một lần nữa gần đây nhất là năm 2004. Mục tiêu của công ty EMV là phải đảm bảo với các tổ chức tài chính và các đại lý rằng các chuẩn kỹ thuật dù phát triển nhưng vẫn phải giữ được tương thích với phiên bản 1998.

Các liên minh này đã khuyến cáo các nước về việc cần thiết phải chuyển đổi từ thẻ từ có tính bảo mật thấp sang thẻ chíp có tính năng bảo mật cao hơn rất nhiều. Khuyến cáo này được đưa ra từ năm 2004, sau những con số thiệt hại do gian lận thẻ ngày càng lớn. Sau mốc thời gian quy định, nếu ngân hàng nào còn sử dụng thẻ từ, có thể chịu phạt lên tới 50 nghìn đô la Mỹ một năm tính theo các vụ gian lận thẻ. Mức phạt này áp dụng cho cả ngân hàng phát hành thẻ và ngân hàng chấp nhận thẻ.

Chuyển đổi thẻ thanh toán nội địa từ thẻ từ sang thẻ chip là một trong những giải pháp trọng tâm của ngành ngân hàng Việt Nam, được nêu trong Đề án Phát triển thanh toán không dùng tiền mặt giai đoạn 2016-2020 do Thủ tướng Chính phủ phê duyệt. Tính đến tháng 5 năm 2019, Việt Nam có 48 ngân hàng phát hành thẻ nội địa với số lượng khoảng 76 triệu thẻ, hơn 261.000 máy POS và 18.600 máy ATM, trong đó phần lớn POS đã tuân theo tiêu chuẩn EMV. Ngày 28/5, Hội thẻ Ngân hàng Việt Nam phối hợp với Công ty CP Thanh toán Quốc gia Việt Nam (NAPAS) và 07 ngân hàng đầu tiên gồm Vietcombank, VietinBank, BIDV, Agribank, Sacombank, TPBank, ABBank chính thức công bố ra mắt sản phẩm thẻ chip nội địa.

1.2 Những vấn đề chung về thanh toán điện tử

1.2.1 Khái niệm thanh toán điện tử

- Hiểu nguyên nghĩa của e-payment (electronic payment)

Về bản chất, thanh toán điện tử là việc sử dụng, chuyển giao và thanh toán tiền thông qua các phương tiện điện tử thay cho việc trao tay tiền mặt.

- Tiếp cận dưới góc độ tài chính

Thanh toán điện tử được hiểu là việc chuyển giao các phương tiện tài chính từ một bên sang một bên khác thông qua việc sử dụng các phương tiện điện tử.

- Tiếp cận dưới góc độ viễn thông

Thanh toán điện tử được hiểu là việc truyền tải các thông tin về phương tiện thanh toán qua các mạng viễn thông và các phương tiện điện tử.

- Tiếp cận dưới góc độ CNTT

Thanh toán điện tử được hiểu là việc thanh toán dựa trên nền tảng CNTT để xử lý các chứng từ điện tử, các thông điệp điện tử, giúp cho quá trình thanh toán được diễn ra một cách nhanh chóng và hiệu quả, an toàn.

- Tiếp cận dưới góc độ phương tiện sử dụng

Thanh toán điện tử được hiểu là việc sử dụng các phương tiện điện tử để tiến hành các hoạt động mua bán hàng hóa, dịch vụ, các phương tiện bao gồm: ATM, POS, các website.

- Tiếp cận dưới góc độ tự động hóa

Thanh toán điện tử được hiểu là việc ứng dụng công nghệ, chủ yếu là CNTT để tự động hóa các hoạt động tài chính và các kênh thông tin, thanh toán.

- Tiếp cận dưới góc độ trực tuyến

Thanh toán điện tử được hiểu là việc chi tiêu cho các hàng hóa và dịch vụ, các thông tin trao đổi trực tiếp trên Internet cùng nhiều loại dịch vụ trực tuyến khác.

1.2.2 Lợi ích và hạn chế của thanh toán điện tử

1.2.2.1 Lợi ích của thanh toán điện tử

- Hoàn thiện và phát triển TMĐT

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

- Không bị hạn chế, giới hạn bởi không gian, thời gian

Trong thanh toán trực tuyến với sự số hóa của đồng tiền giao dịch, giúp cho những hoạt động thanh toán được diễn ra theo thời gian thực, bỏ qua những rào cản của không gian và thời gian mà những hình thức trong thanh toán truyền thống chưa bao giờ có được.

- Tiết kiệm được thời gian, đơn giản hóa quá trình thanh toán

Lợi ích này đến với cả người mua và người bán, và cả những trung gian thanh toán. Tất cả những bên tham gia đều tiết kiệm được thời gian và đơn giản hóa được quá trình thanh toán.

Điểm khác biệt lớn nhất so với thanh toán truyền thống là thanh toán điện tử loại bỏ được hầu hết việc giao nhận giấy tờ, sử dụng chữ ký truyền thống cùng việc xem xét tiền thật, tiền giả, thay vào đó là những phương pháp xác thực mới trên các thiết bị điện tử, sự tiện lợi tối đa cho khách hàng sử dụng đồng thời giúp cho quá trình thanh toán diễn ra nhanh chóng, dễ dàng và tiết kiệm thời gian.

- Tăng tốc độ chu chuyển tiền và tận dụng hiệu quả của đồng tiền

Đối với tiền số hóa thì tiền được chuyển từ tài khoản của người mua sang tài khoản của người bán, hầu như ngay lập tức, người bán có thể nhận được và sử dụng. Tiền sẽ rất nhanh chóng được tiêu dùng hoặc tái đầu từ và do đó làm tăng tốc độ chu chuyển của tiền.

- Tính an toàn cao đặc biệt là khi mua các sản phẩm có giá trị lớn

Đồng tiền là số hóa chính vì vậy cho phép người dùng có thể tiến hành thanh toán điện tử mà không cần mang theo một lượng tiền mặt lớn, tính an toàn tăng cao.

- Mất phương tiện thanh toán nhưng vẫn giữ được tiền trong tài khoản

Khác với những phương thức thanh toán truyền thống khác, chủ thẻ thanh toán có thể mất phương tiện thanh toán nhưng vẫn lưu trữ được tiền trong tài khoản nhờ việc sử dụng những hình thức xác thực đặc biệt.

1.2.2.2 Hạn chế của thanh toán điện tử

- Nguy cơ bị tiết lộ thông tin tài chính cá nhân

Nguy cơ bị tiết lộ thông tin cá nhân có thể xuất phát từ nhiều nguồn: CNTT ngày càng phát triển, các hacker trình độ ngày càng cao, vì thế nếu không có phương thức đảm bảo an toàn cho tài khoản thanh toán thì nguy cơ bị tiết lộ thông tin của người dùng là rất cao, điều này tạo ra tâm lý hoang mang, lo lắng và hạn chế một số lượng người ko nhỏ tham gia vào hoạt động thanh toán điện tử. Lo ngại về sự an toàn trong giao dịch cũng là một trở ngại, từ chỗ lo ngại dẫn đến việc không tiếp cận do vậy không thấy được lợi ích của thanh toán điện tử.

Thông tin tài khoản cá nhân của khách hàng cũng có thể bị bên thứ ba, hoặc người bán tiết lộ; hoặc lừa đảo khách hàng chuyển tiền tới tài khoản của họ.

- Khó kiểm soát được việc chi tiêu trong thẻ tín dụng

Đối với khách hàng được sử dụng thẻ tín dụng, được chi tiêu trước, trả tiền sau, thường không khống chế được sự chi tiêu của mình, khi nhận được sao kê của ngân hàng thì thường là một số tiền lớn, vượt quá khả năng thanh toán cùng một lúc dẫn tới tạo ra cú sốc về thấu chi thẻ tín dụng cho người dùng.

Đối với khách hàng mới thường tham gia vào những giao dịch trực tuyến, thường có tâm lý hưng phấn, thích trải nghiệm với hình thức mới này, và đối với người này thì chi tiêu nhiều cho thanh toán trực tuyến.

- Kiến thức và khả năng thực hiện của người dùng

Để có thể thực hiện giao dịch thanh toán, đòi hỏi người dùng phải có kiến thức và kỹ năng nhất định, tuy nhiên trên thực thế có rất nhiều người dùng không thể thực hiện được hoạt động thanh toán điện tử mặc dù họ có thể sở hữu những phương tiện thanh toán điện tử. Bên cạnh đó, số lượng người dùng biết sử dụng thiết bị bảo mật, biết bảo quản mật mã và không giao dịch với tổ chức cá nhân ko rõ danh tính còn rất hạn chế, điều này ngăn cản sự phát triển của thanh toán điện tử.

- Tập quán tiêu dùng và thói quen thanh toán

Phần lớn thì người tiêu dùng đều có thói quen sử dụng tiền mặt trao tay, tâm lý thích tiền mặt luôn thường trực, vì thế rất nhiều người thích cầm và sử dụng tiền mặt hơn là sử dụng hình thức thanh toán điện tử.

Ngoài ra không thể phủ nhận hoạt động mua sắm truyền thống giúp người mua giải tỏa được áp lực trong cuộc sống, tạo ra sự gắn kết giữa người mua và bạn bè hoặc là người thân vì thế nhiều người mua thích thanh toán truyền thống hơn là thanh toán thông qua những phương tiện điện tử.

1.2.3 Phân loại các hình thức thanh toán điện tử

✓ **Phân loại theo thời gian thực**

- Thanh toán trực tuyến: Là tập con của thanh toán điện tử, có đầy đủ các đặc điểm của thanh toán điện tử. Tuy nhiên nó ưu việt hơn do phá vỡ phạm vi không gian và thời gian thanh toán.

- Thanh toán ngoại tuyến: Là những phương thức thanh toán được diễn ra trên các thiết bị điện tử khác như ATM, POS. Chuyển khoản điện tử tại ngân hàng hoặc qua ATM.

✓ **Phân chia theo bản chất giao dịch**

- Thanh toán trong TMĐT B2C: Là loại hình thanh toán được diễn ra giữa doanh nghiệp và người tiêu dùng cuối cùng, phù hợp với những giao dịch vừa và nhỏ. Các phương tiện thanh toán phổ biến như: thẻ thanh toán, ví điện tử.

- Thanh toán trong TMĐT B2B: Là loại hình thanh toán được diễn ra giữa doanh nghiệp với doanh nghiệp khác, hoặc giữa doanh nghiệp với các tổ chức kinh doanh khác nhau. Phù hợp với những giao dịch có giá trị và khối lượng lớn. Một số phương tiện phổ biến như: chuyển khoản điện tử, séc điện tử.

✓ **Phân chia theo cách thức tiếp nhận phương tiện thanh toán**

- Thanh toán trên website/điện thoại: Là loại hình thanh toán độc lập diễn ra trên website hoặc điện thoại. Quá trình thanh toán chỉ yêu cầu khai báo thông tin về phương tiện thanh toán mà không cần bất kỳ sự xác nhận vật lý nào về phương tiện thanh toán đó.

- Thanh toán trên các phương tiện điện tử khác: Sử dụng các thiết bị điện tử như ATM, POS để tiếp nhận, chuyển tải các thông tin về phương tiện thanh toán. Quá trình thanh toán yêu cầu sự xác nhận vật lý các phương tiện thanh toán và có thể bao gồm chữ ký xác nhận của chủ phương tiện thanh toán.

✓ **Phân chia theo các phương tiện thanh toán**

- Thẻ thanh toán (Thẻ tín dụng – credit card; Thẻ ghi nợ - debit card): là phương tiện thanh toán phổ biến nhất trong TMĐT hiện nay. Các loại thẻ thường được sử dụng: thẻ tín dụng, thẻ ghi nợ, thẻ trả trước.

- Ví điện tử (e-wallet): là một tài khoản điện tử được sử dụng để mua sắm trên các website có tích hợp thanh toán điện tử. Có thể kết nối liên thông với một hệ thống ngân hàng: chuyển tiền từ ví sang ngân hàng và ngược lại.

- Vi thanh toán điện tử (micropayment): là loại hình thanh toán được thực hiện đối với các giao dịch dưới 10 đô la Mỹ.

- Chuyển khoản điện tử (electronic fund transfer): là nghiệp vụ chuyển tiền thanh toán từ tài khoản này sang tài khoản khác có thể cùng hệ thống ngân hàng hoặc là khác hệ thống ngân hàng.

- Séc điện tử (electronic cheque): là loại hình thanh toán kết hợp giữa tính hiệu quả, thuận tiện, an toàn của các nghiệp vụ điện tử với các bước tiến hành của séc giấy truyền thống.

- Thanh toán bằng xuất trình hóa đơn điện tử: đây không phải là loại hình thanh toán độc lập. Tạo ra sự chủ động rất lớn cho người thanh toán, cho phép các khách hàng có thể trình bày hóa đơn và xử lý thanh toán.

1.2.4 Yêu cầu đối với thanh toán điện tử

Một hệ thanh toán điện tử được gọi là tốt nếu nó thoả mãn các yêu cầu về tính bảo mật, độ tin cậy, tính quy mô, tính ẩn danh, tính chấp nhận được, tính mềm dẻo, tính chuyển đổi được, tính hiệu quả, tính dễ kết hợp với ứng dụng và dễ sử dụng. Một mô hình thanh toán điện tử tốt phải đáp ứng càng cao càng tốt các yêu cầu nêu trên, trong đó tính bảo mật đóng vai trò tối thượng.

Khả năng có thể chấp nhận được

Để đạt được thành công thì cơ sở hạ tầng của việc thanh toán phải được công nhận rộng rãi, 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 các tổ chức thanh toán. Cần xây dựng và không ngừng nâng cao trình độ công nghệ thông qua phát triển cơ sở hạ tầng kĩ thuật như mạng máy tính, khả năng tiếp nối của mạng với các cơ sở dữ liệu thông tin toàn cầu, và các phần mềm hỗ trợ ngày càng hoàn hảo, tốc độ đường truyền nhanh để đáp ứng tốt nhất cho việc thanh toán.

Tính an toàn và bảo mật

An toàn là yêu cầu hàng đầu cho các giao dịch tài chính qua các mạng mở như Internet vì đây sẽ là mục tiêu cho các tội phạm, các kẻ sử dụng thẻ tín dụng trái phép, các hacker… do các dịch vụ trên Internet hiện nay được cung cấp toàn cầu với mọi tiện ích phục vụ cho mọi khách hàng, mọi thành phần trong xã hội. Một trong những ví dụ đó là hiện tượng chặn và thay đổi nội dung các thông tin truyền đi, như thay đổi địa chỉ nhận đối với một chuyển khoản điện tử của ngân hàng và do vậy chuyển khoản này được chuyển đến tài khoản khác của kẻ xâm nhập gửi. Chính vì vậy phải đảm bảo khả dụng nhưng chống lại được sự tấn công để tìm kiếm thông tin mật, thông tin cá nhân hoặc điều chỉnh thông tin, thông điệp được truyền.

Để đảm bảo yêu cầu này một số giải pháp công nghệ đang được tiến hành, với các công cụ và kĩ thuật cơ bản như: kĩ thuật mã hóa thông tin (bao gồm mã hóa bí mật và mã hóa công khai), giao thức thỏa thuận mã khóa, chữ kí điện tử, an ninh mạng và tường lửa, nhưng hữu hiệu nhất là chữ kí điện tử và chứng thực điện tử. Riêng trong lĩnh vực thanh toán bằng

thẻ tín dụng, để đảm bảo yêu cầu này người ta có sử dụng sử dụng *giao thức SSL* (sécure socket layer) để cung cấp sự bảo mật và bảo vệ sự riêng tư. Nhưng Visa và MasterCard đã cùng nhau phát triển một giao thức an toàn hơn, được gọi là *SET* (sécure electronic transaction). Về lý thuyết, đó là một giao thức hoàn hảo. Ví dụ, một sự khác biệt điển hình giữa SET và SSL được sử dụng rộng rãi là SSL không bao gồm một chứng thực khách hàng yêu cầu phần mềm đặc biệt (được gọi là ví số - digital wallet) tại máy tính cá nhân của họ. SSL được thiết lập trong trình duyệt, do đó không cần một phần mềm đặc biệt nào. Kế hoạch Visa và MasterCard phải chấp nhận các thông điệp chỉ khi chúng tuân thủ giao thức SET. Tuy nhiên, SET không phổ biến nhanh như nhiều người mong đợi do tính phức tạp, thời gian phản hồi chậm, và sự cần thiết phải cài đặt ví số ở máy tính của khách hàng.

Tính ẩn danh

Không giống với thẻ tín dụng và séc, nếu người mua dùng tiền mặt, rất khó truy tìm dấu tích người mua sau giao dịch, các hệ thống thanh toán điện tử nếu yêu cầu cung cấp thông tin cá nhân, hình ảnh và những đặc điểm nhận dạng thì đặc điểm nhận dạng hoặc thông tin cá nhân của các chủ thể phải được giữ kín. Phải đảm bảo không làm lộ các thông tin cá nhân của khách hàng.

Tính chuyển đổi, hoán đổi

Là sự chuyển đổi từ hình thức này sang hình thức khác. Ví dụ: tiền số có thể chuyển thành các kiểu loại tiền khác. Có thể dễ dàng chuyển từ tiền điện tử sang tiền mặt hay chuyển tiền từ quỹ tiền điện tử về tài khoản của cá nhân. Từ tiền điện tử có thể phát hành séc điện tử, séc giấy. Tiền số bằng ngoại tệ này có thể dễ dàng chuyển sang ngoại tệ khác với tỷ giá tốt nhất.

Tính hiệu quả

Chi phí cho mỗi giao dịch nên chỉ là một con số rất nhỏ (gần bằng 0), đặc biệt với những giao dịch giá trị thấp. Trong thực tế, việc thanh toán điện tử giúp cho tất cả các bên tiết kiệm được rất nhiều thời gian và các chi phí giao dịch hữu hình khác, cho nên, dịch vụ thanh toán điện tử hoàn toàn có thể được cung cấp ở mức phí giao dịch thấp nhất.

Tính linh hoạt

Nên cung cấp nhiều phương thức thanh toán, tiện lợi cho mọi đối tượng dù khách hàng là doanh nghiệp hay người tiêu dùng cuối cùng. Có thể thanh toán bằng hệ thống thanh toán thẻ tín dụng, hệ thống chuyển khoản điện tử và thẻ ghi nợ trên Internet, ví tiền điện tử, hệ thống séc điện tử, hóa đơn điện tử, thẻ thông minh. Các hình thức thanh toán luôn được cập nhật và thay đổi để phù hợp với môi trường công nghệ, xã hội.

Tính hợp nhất

Để hỗ trợ cho sự tồn tại của các ứng dụng này thì giao diện nên được tạo ra theo sự thống nhất của từng ứng dụng. Khi mua hàng trên bất cứ website nào cũng cần có những giao diện với những bước giống nhau và công nghệ áp dụng đồng bộ ở các ngân hàng cũng như tại các tổ chức thanh toán.

Dịch vụ ngân hàng điện tử có thể thực sự phát huy tác dụng và hỗ trợ hiệu quả cho thanh toán điện tử, đặc biệt là giao dịch B2C và C2C, cần có sự liên thông rất cao giữa các ngân hàng cũng như một *cổng trung gian thanh toán* (payment gateway) với năng lực hoạt

động mạnh cho phép khách hàng thực hiện giao dịch chuyển tiền và thực hiện các giao dịch thương mại trực tuyến ở những ngân hàng khác nhau.

Tính co dãn

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 TMĐT tăng. Hạ tầng mạng, phần mềm hỗ trợ, ngân hàng và hệ thống phục vụ đáp ứng được các tốc độ mua bán, thanh toán nhanh cả những thời điểm rất nhiều người thanh toán cùng môt lúc.

Tính tiện lợi, dễ sử dụng

Tính tiện lợi dễ sử dụng là cho bất kỳ ai, doanh nghiệp, khách hàng đều có thể sử dụng dễ dàng. Nên tạo sự thuận lợi cho việc thanh toán trên mạng như trong thực tế.

1.2.5 Các bên tham gia thanh toán điện tử

1.2.5.1. Người bán hàng (Merchant)

Người bán rất đa dạng, có thể là doanh nghiệp, tổ chức có thể là cá nhân. Tuy nhiên trong tài liệu này chúng tôi chủ yếu đề cập đến người bán là tổ chức, doanh nghiệp.

Người bán được chia thành hai loại: người bán tự xây dựng website và người bán hàng trên website khác

Người bán tự xây dựng website và bán hàng trực tiếp trên website. Đối với loại người bán này sẽ tự tích hợp dịch vụ thanh toán trên hệ thống website, chi phí thanh toán người bán sẽ phải trả cho nhà cung cấp dịch vụ thanh toán mà mình tích hợp. Chi phí này có thể là chi phí định kỳ hoặc giao dịch là do sự thỏa thuận giữa người bán và nhà cung cấp dịch vụ thanh toán.

Người bán hàng trên website khác, người bán trong trường hợp này sẽ thuê một nền tảng của bên thứ ba để thông qua đó bán hàng hóa, dịch vụ của mình. Đối với loại người bán này thì hệ thống thanh toán sẽ do bên thứ ba tự tích hợp. Người bán sẽ không phải trả phí thanh toán, nhưng sẽ phải trả phí cho nền tảng bán hàng, phí này có thể là phí đăng ký hoặc phí giao dịch do thỏa thuận giữa người bán và website nền tảng. Ví dụ bán hàng trên nền tảng của doanh nghiệp khác như Tiki.vn; Adayroi.com; Lazada.vn.

1.2.5.2. Người mua (Buyer)

Người mua là người có phương tiện thanh toán và tiến hành thực hiện những giao dịch điện tử với người bán.

Người mua có thể là cá nhân hoặc tổ chức.

Những cá nhân mua hàng với khối lượng giao dịch nhỏ, có thể sử dụng một số phương tiện thanh toán như: ví điện tử, vi thanh toán, thẻ thanh toán (thẻ tín dụng, thẻ ghi nợ).

Tổ chức (thường là doanh nghiệp) mua với khối lượng giao dịch lớn, có thể sử dụng những hình thức như séc điện tử hay chuyển khoản điện tử.

1.2.5.3. Các ngân hàng (Bank)

Ngân hàng ở đây bao gồm: ngân hàng của người mua, ngân hàng của người bán, và ngân hàng của tổ chức trung gian thanh toán - là tổ chức tin cậy thứ ba được người mua và người bán tin tưởng, nhằm đảm bảo các giao dịch được xác thực, xử lý chính xác.

1.2.5.4. Các tổ chức, trung gian cung cấp dịch vụ thanh toán (PSP - Processing service

provider)

Các PSP cung cấp dịch vụ cho các thương nhân và bên bán hàng trực tuyến trên Internet có thể chấp nhận những hình thức thanh toán điện tử mà khách hàng sử dụng khi khách hàng tiến hành thanh toán trên website của những người bán này.

Một PSP đầy đủ có thể quản lý các kết nối kỹ thuật, các mối liên hệ với các ngân hàng và các tổ chức tài chính khác, giúp cho người bán có thể giảm được những chi phí để thiết lập kết nối và tránh được sự lệ thuộc quá lớn vào các tổ chức tài chính.

Trên website, đa phần các PSP sẽ tính hai loại phí cơ bản là phí đăng ký định kỳ và phí giao dịch, hoặc có thể cả hai loại phí kết hợp.

Ví dụ các PSP ở Việt Nam hiện nay: Napas (napas.com.vn), Ngân Lượng (nganluong.vn), Bảo Kim (baokim.vn), Momo (momo.vn), Vnpay (vnpay.vn). Trên thế giới: Paypal (paypal.com), 2checkout (2checkout.com), Authorize (authorize.net), Payoneer (payoneer.com)…

1.2.5.5. Các tổ chức phát hành phương tiện thanh toán

Tổ chức phát hành phương tiện thanh toán là những tổ chức phát hành ra những phương tiện thanh toán cho người mua, người bán để phục vụ quá trình thanh toán điện tử.

Ví dụ: Tổ chức thẻ Visa, tổ chức thẻ Mastercard, công ty thẻ American Express, công ty thẻ JCB: là hiệp hội các tổ chức tài chính, tín dụng tham gia phát hành và thanh toán thẻ quốc tế.

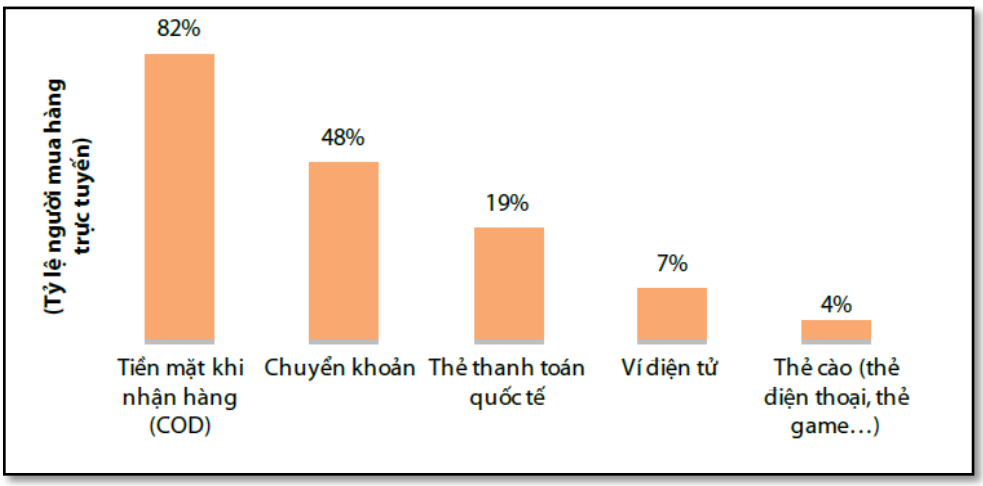
Tổ chức phát hành ví điện tử: Paypal (paypal.com), Momo (momo.vn), Vnpay (vnpay.vn)…là những nhà cung cấp phương tiện thanh toán là ví điện tử cho khách hàng.

1.3 Tình hình thanh toán điện tử tại Việt Nam và trên thế giới

1.3.1 Thanh toán điện tử ở Việt Nam

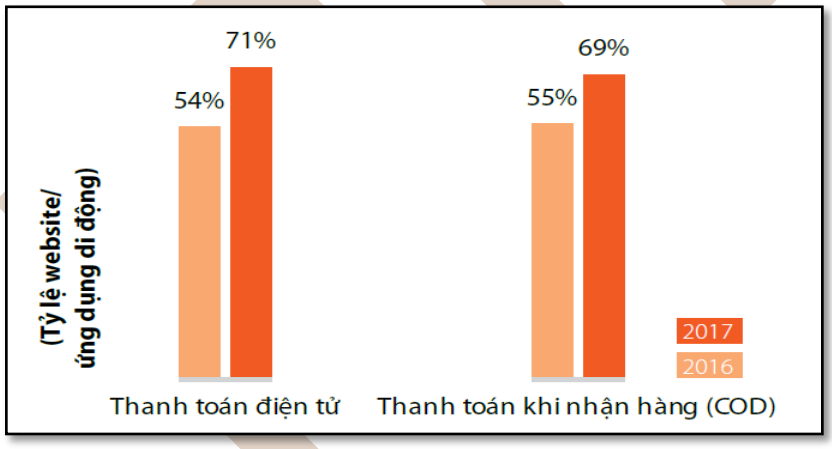
Theo thông tin tại Hội nghị thường niên Hội thẻ Ngân hàng Việt Nam năm 2017 vừa được tổ chức mới đây, các giao dịch qua ATM vẫn chủ yếu là giao dịch rút tiền mặt, chiếm 86,81% doanh số sử dụng của thẻ nội địa, doanh số rút tiền mặt/ATM/năm vẫn tăng qua các năm (từ 60 tỷ đồng năm 2012 lên 106 tỷ đồng năm 2016), điều đó cho thấy thói quen sử dụng tiền mặt của người dân vẫn còn rất phổ biến.

Theo Báo cáo thương mại điện tử 2018, ước tính số lượng người mua sắm trực tuyến trong TMĐT B2C đạt 33,6 triệu người, giá trị mua sắm trung bình mỗi người khoảng 186 USD. Phần lớn người mua hàng trực tuyến vẫn lựa chọn hình thức thanh toán tiền mặt khi nhận hàng với 82% đối tượng khảo sát cho biết có sử dụng phương thức này, tiếp theo là 48% sử dụng phương thức chuyển khoản qua ngân hàng, 19% người tham gia khảo sát cho biết từng sử dụng các loại thẻ thanh toán quốc tế, ví điện tử được sử dụng với tỷ lệ thấp (7%) (Hình 1.1).

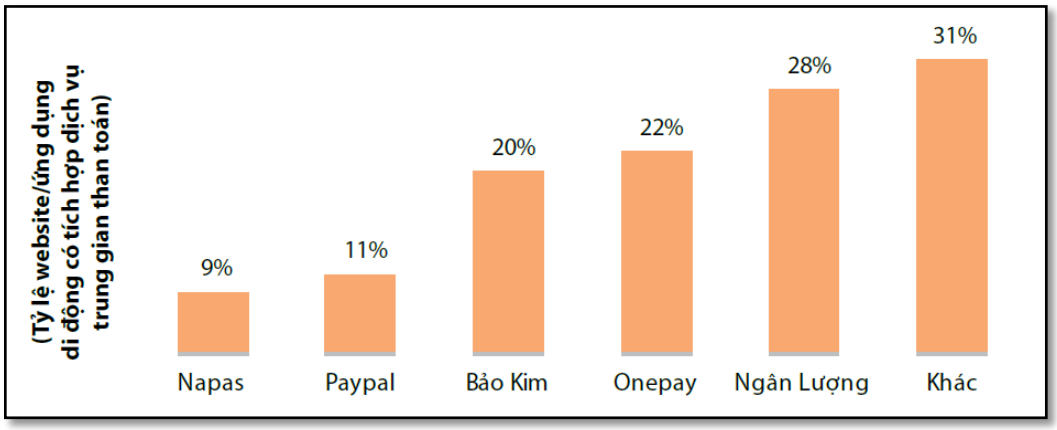


Hình 1.1: Các hình thức thanh toán phổ biến trong mua sắm trực tuyến tại Việt Nam 2018

Bên cạnh đó, tỷ lệ những website/ ứng dụng tích hợp thanh toán điện tử năm 2016 là 54% và tăng lên đến 71% vào năm 2017. Thanh toán khi nhận hàng (COD) được tích hợp vào website cũng có xu hướng tăng từ 55% đến 69% (Hình 1.2). Đối với các website có tích hợp giải pháp thanh toán trực tuyến, các nhà cung cấp dịch vụ trung gian thanh toán phổ biến được doanh nghiệp lựa chọn sử dụng là Ngân Lượng (28%), Onepay (22%), Bảo Kim (20%), Paypal (11%), Napas (9%) và còn lại là những trung gian khác (31%) (Hình 1.3).



Hình 1.2: Các hình thức thanh toán website/ ứng dụng di động chấp nhận



Hình 1.3: Tỷ lệ tích hợp các đơn vị trung gian thanh toán năm 2018

✓ **Cơ sở hạ tầng thanh toán điện tử**

Tính đến tháng 11/2019, nước ta đã có 48 ngân hàng thương mại, 32 tổ chức trung gian thanh toán, số lượng thẻ cũng được các ngân hàng quan tâm phát triển và vẫn tăng trưởng đều qua các năm, hiện giờ lên đến 164 triệu thẻ thanh toán. Số lượng các máy chấp nhận thẻ (POS) có tốc độ tăng trưởng nhanh. Theo số liệu từ Ngân hàng nhà nước, đến cuối tháng 11/2019, trên toàn quốc có 18.741 ATM và hơn 259.889 POS được lắp đặt, chưa kể một số lượng lớn các website TMĐT chấp nhận giao dịch thẻ trực tuyến. Ngân hàng Nhà nước cũng quan tâm chỉ đạo phát triển thanh toán POS trên thiết bị di động (mPOS), ứng dụng công nghệ hiện đại với chi phí thấp, dễ sử dụng và đảm bảo an toàn bảo mật, mở ra khả năng mới để phát triển nhanh các điểm chấp nhận thẻ quy mô nhỏ, tăng cường khả năng cung ứng dịch vụ cho khu vực nông thôn.

Việc sáp nhập thành công Smartlink vào Banknetvn và đổi tên thành Công ty Cổ phần thanh toán quốc gia Việt Nam (Napas) tạo thuận lợi và hiệu quả hơn trong việc kết nối, chuyển mạch thẻ tại Việt Nam. Đây là bước đi quan trọng nhằm tạo nền tảng kỹ thuật cho việc phát triển thanh toán thẻ. Từ tháng 5/2019, dưới sự chỉ đạo của Ngân hàng Nhà nước, Hội thẻ Ngân hàng Việt Nam (VBCA) phối hợp với Công ty Cổ phần Thanh toán Quốc gia Việt Nam (NAPAS) và 7 ngân hàng đầu tiên gồm: Vietcombank, Vietinbank, BIDV, Agribank, Sacombank, TPBank, ABBank chính thức công bố ra mắt sản phẩm thẻ chip nội địa của các ngân hàng. Lần đầu tiên thị trường thanh toán Việt Nam triển khai áp dụng một tiêu chuẩn kỹ thuật thống nhất tương thích với tiêu chuẩn quốc tế EMV, khẳng định tính tự chủ và ứng dụng kịp thời những thành tựu tiến bộ của CMCN 4.0 trong hoạt động thanh toán của ngành ngân hàng ; giúp cho các giao dịch thanh toán an toàn, bảo mật hơn, tạo điều kiện thuận lợi cho các ngân hàng phát triển tính năng thanh toán mới, hiện đại cho sản phẩm thẻ nội địa ; mở ra cơ hội để thẻ nội địa tham gia hội nhập quốc tế. Theo kế hoạch đặt ra, đến 31/12/2019, các ngân hàng thương mại thực hiện chuyển đổi ít nhất 30% số lượng thẻ từ nội địa, 35% số lượng ATM và 50% số lượng POS hiện có sang công nghệ chip tiếp xúc và không tiếp xúc. Toàn bộ máy ATM và POS trên thị trường đảm bảo tuân thủ Tiêu chuẩn VCCS vào 31/12/2020. Chậm nhất vào 31/12/2021, toàn bộ thẻ từ nội địa đang lưu hành của tổ chức phát hành thẻ tuân thủ TCCS về thẻ chip nội.

Cơ sở hạ tầng và công nghệ phục vụ thanh toán điện tử, thanh toán thẻ tiếp tục được chú trọng đầu tư, nâng cao chất lượng và phát huy hiệu quả. Thống đốc Ngân hàng Nhà nước đã có quyết định nâng cấp Hệ thống thanh toán điện tử liên ngân hàng áp dụng theo các thông lệ, chuẩn mực, tiến bộ về thanh toán và công nghệ của các nước phát triển trên thế giới, bảo đảm phù hợp với lộ trình độ CNTT của các ngân hàng Việt Nam. Các giao dịch thanh toán đã chuyển dần sang phương thức xử lý tự động, sử dụng chứng từ điện tử, đến việc các giao dịch thanh toán được xử lý điện tử chiếm tỷ trọng lớn, thời gian xử lý hoàn tất một giao dịch được rút ngắn xuống còn vài phút, thậm chí chỉ trong vòng vài giây hoặc tức thời.

✓ **Cơ sở pháp lý thanh toán điện tử**

Cho đến nay, chưa có một văn bản pháp lý riêng quy định đầy đủ về những hoạt động liên quan tới thanh toán điện tử nói chung để tạo dựng khuôn khổ pháp lý chặt chẽ, thống nhất cho việc ứng dụng thanh toán điện tử trong hoạt động TMĐT. Hoạt động thanh toán điện tử sẽ được điều chỉnh dựa trên một số căn cứ vào: Luật các Tổ chức tín dụng, Luật Ngân hàng

Nhà nước, Luật giao dịch điện tử, Luật công nghệ thông tin.

Bên cạnh đó chịu sự hướng dẫn của một số nghị định và thông tư:

- Nghị định số 101/2012/NĐ-CP ngày 22/11/2012 của Chính phủ về Thanh toán không dùng tiền mặt, nghị định đã đưa ra các quy định mang tính khuôn khổ về các dịch vụ trung gian thanh toán và điều kiện cung ứng dịch vụ cũng như quy trình, thủ tục, hồ sơ cấp, thu hồi và cấp lại Giấy phép hoạt động cung ứng dịch vụ trung gian thanh toán tại Điều 5.3; Điều 15 và Điều 16.

- Nghị định số 64/2001/NĐ-CP về hoạt động thanh toán qua các tổ chức cung ứng dịch vụ thanh toán).

- Thông tư số 23/2010/TT-NHNN quy định về việc quản l., vận hành và sử dụng Hệ thống Thanh toán điện tử liên ngân hàng.

- Thông tư số 46/2014/TT-NHNN hướng dẫn về dịch vụ thanh toán không dùng tiền mặt.

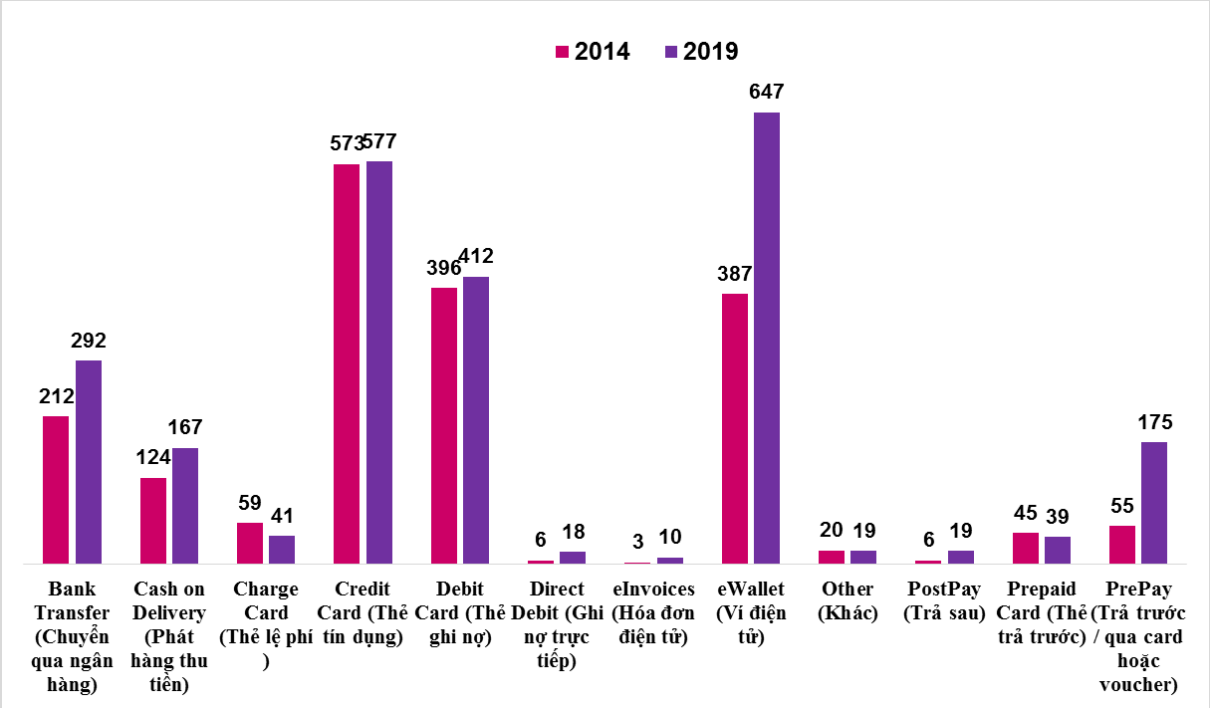
- Thông tư số 39/2014/TT-NHNN hướng dẫn về dịch vụ trung gian thanh toán.

Thanh toán điện tử ở Việt Nam đã có những bước phát triển nhất định nhưng vẫn đang phải đối mặt với nhiều thách thức, rào cản lớn, môi trường pháp lý chưa hoàn thiện, đầy đủ và đồng bộ, các chính sách và điều kiện hỗ trợ phát triển dịch vụ thanh toán điện tử còn yếu và thiếu, trình độ phát triển kinh tế, xã hội còn chưa cao, trình độ công nghệ còn nhiều hạn chế, thói quen thanh toán tiền mặt và sự thiếu tin tưởng của xã hội đối với thanh toán điện tử...

1.3.2 Thanh toán điện tử trên thế giới

1.3.2.1. Các hình thức thanh toán điện tử phổ biến trên thế giới

Báo cáo của WorldPayvề hoạt động thanh toán toàn cầu (World Payments Report) công bố hàng năm cho thấy nhịp độ khai thác các dịch vụ thanh toán điện tử tăng lên rất nhanh. Nếu như năm 2015, thị trường TMĐT toàn cầu có giá trị 1,66 nghìn tỷ USD - tăng 14% so với năm 2014 thì đến năm 2019 con số này là 2,4 nghìn tỷ USD với 23% trong số này được thực hiện chỉ qua các thiết bị di động. Trong số các phương thức thanh toán điện tử, mặc dù thanh toán qua thẻ ghi nợ (Debit Card) vẫn chiếm tỷ trọng lớn nhưng có mức tăng trưởng không cao, chỉ từ 573 tỷ USD vào năm 2014 và dự báo lên đến 577 tỷ USD vào năm 2019. Thanh toán qua ví điện tử (eWallet) sẽ là phương thức thanh toán dẫn đầu với 674 tỷ USD vào năm 2019. Tuy nhiên hình thức trả trước (PrePay) qua thẻ hoặc phiếu mua hàng (Voucher) là hình thức thanh toán có mức tăng trưởng vượt bậc, từ 55 tỷUSD năm 2014 lên đến 175 tỷUSD vào năm 2019.



Hình 2… Các hình thức thanh toán điện tử phổ biến trong tương lai

(Nguồn: Global payments report preview, WorldPay 2015)

1.3.2.2. Các hình thức bảo hiểm và cơ chế an toàn bảo mật

Bảng so sánh dưới đây (bảng 1.1) cho thấy hầu hết các quốc gia có trình độ phát triển TMĐT cao đều có quan tâm tâm hợp lý tới vấn đề rủi ro thanh khoản đối với các định chế tài chính tham gia TTĐT và phát hành tiền điện tử ở mức độ quản lý quốc gia, đặc biệt trong bối cảnh doanh số thanh toán điện tử tăng trưởng liên tục trong những năm vừa qua. Đây là lý do chính của việc 11/17 quốc gia được khảo sát đưa ra các chế tài bắt buộc các định chế tài chính tham gia TTĐT và phát hành tiền điện tử phục vụ TMĐT phải có những biện pháp bảo hiểm tiền gửi (ở các mức độ và giải pháp tùy thuộc vào từng quốc gia). Tuy nhiên các chế tài này cũng tạo ra cản trở nhất định đối với việc phát triển TTĐT trong TMĐT do chi phí lưu thông tiền tệ tăng cao, vì vậy những quốc gia như Thái lan, Malaysia, Indonesia vv… với trình độ phát triển TMĐT và doanh số mậu dịch còn thấp thì chế tài về bảo hiểm cho các loại hình thanh toán điện tử vẫn chưa đặt ra.

Liên quan tới bảo vệ quyền lợi khách hàng thì quan điểm của các chính phủ là khách hàng cần được lựa chọn sử dụng một sản phẩm dịch vụ nào đó khi mà họ đã hiểu thấu đáo về đặc điểm, chi phí, rủi ro có liên quan của sản phẩm đó. Vì vậy cần phải có sự công khai các thông tin về quyền lợi của người sử dụng, thông tin về nhà phát hành, nghĩa vụ của nhà phát hành đối với người sử dụng và ngược lại, các hình thức thanh toán và đảm bảo khả năng thanh toán, những yêu cầu và khả năng bảo mật thông tin cá nhân.

Bảng 1.1: Hình thức bảo hiểm và cơ chế an toàn bảo mật tại một số quốc gia trên thế giới

Nước	Bảo hiểm tiền gửi và các hình thức bảo hiểm khác	Bảo mật thông tin cá nhân

Bỉ	Áp dụng chương trình bảo hiểm tiền gửi đối với các sản phẩm tiền điện tử	Luật Bỉ đồng nhất với định hướng EC về bảo vệ các dữ liệu cá nhân.
Canada	Áp dụng chương trình bảo hiểm tiền gửi đối với các sản phẩm tiền điện tử	Các quy chế ban hành năm 1997 đối với các định chế tài chính chịu sự quản lý của trung ương. Pháp luật công bố thông tin cá nhân ở cấp trung ương được xây dựng năm 2000. Quebec đã thông qua luật bảo mật thông tin cá nhân áp dụng cho khu vực tư nhân. Các định chế tài chính thông qua các điều luật bảo mật thông tin cá nhân của hiệp hội tiêu chuẩn Canada năm 1997. Hiệp hội thanh toán Canada áp đặt các nghĩa vụ chung về bảo mật thông tin cá nhân.
Pháp	Chương trình bảo hiểm áp dụng cho gửi tiền điện tử	Áp dụng chung cho bộ luật dân sự. Áp dụng luật ngân hàng Pháp. Phải có sự chấp thuận của người tiêu dùng đối với việc chuyển giao thông tin cá nhân
CHLB Đức	Các quy tắc đối với các tổ chức tín dụng	Áp dụng chung cho bộ luật dân sự
Italia	Chương trình bảo hiểm tiền gửi áp dụng đối với tiền điện tử. Người mang thẻ được loại trừ	Định hướng của EC gần đây được quốc hội áp dụng
Nhật bản	Áp dụng bảo hiểm tiền gửi đối với tiền điện tử. Theo luật thẻ trả trước thì chủ thẻ có quyền ưu tiên đối với khoản tiền mà nhà phát hành phải gửi vào văn phòng nhận tiền gửi	Các tập đoàn của ngành đã phát hành những hướng dẫn chi tiết về bảo mật thông tin cá nhân của người tiêu dùng đối với các định chế tài chính. Luật bảo mật thông tin cá nhân có hiệu lực
Hà lan	Áp dụng chương trình bảo hiểm tiền gửi đối với các sản phẩm tiền điện tử. Các ngân hàng tham gia vào hệ thống tiền điện tử đã phát triển chia sẻ rủi ro trong trường hợp một thành viên của nhóm bị mất khả năng chi	Luật Hà lan về việc đăng ký các dữ liệu cá nhân và định hướng EC áp dụng đối với tiền điện tử.

	trả	
Thụy điển	Các công ty bảo hiểm đã xác định chương trình bảo hiểm tiền gửi được áp dụng đối với các thẻ hiện hành do các ngân hàng phát hành	Các luật chung về bảo mật thông tin áp dụng cho các tổ chức tín dụng và ngân hàng
Thụy sĩ	Các ngân hàng tham gia vào hệ thống tiền điện tử đã phát triển chia sẻ rủi ro trong trường hợp một thành viên của nhóm bị mất khả năng chi trả	Luật liên bang về bảo vệ dữ liệu, luật an toàn ngân hàng, Bộ luật hình sự Thụy sĩ về tội phạm máy tính, Bộ luật dân sự Thụy sĩ có thể áp dụng đối với tiền điện tử
Vương quốc Anh	Việc áp dụng bảo hiểm tiền gửi đối với tiền điện tử là không rõ ràng	Luật bảo vệ dữ liệu
Australia	N/A	Theo luật bí mật các nhân 1988, Luật thực hành chuyển tiền điện tử được sửa đổi vào tháng 4/2001 bao gồm các loại hình tài chính điện tử, kể cả telephone banking và internet banking, thẻ tiết kiệm và thẻ tín dụng điện tử đều quy định đảm bảo bí mật cá nhân
Indonesia	N/A	Chưa có luật bảo vệ khác hàng riêng mà áp dụng luật bảo vệ khách hàng nói chung
Hàn quốc	N/A	Áp dụng luật về sử dụng bảo mật thông tin tín dụng Quy chế của các tổ chức tài chính quy định việc bảo vệ bí mật của khách hàng từ năm 2001
Malaysia	N/A	Ngân hàng trung ương Negara ban hành hướng dẫn về Bảo mật khách hàng trong chuyển tiền điện tử từ năm 1989. Đang soạn thảo Luật bảo mật dữ liệu cá nhân mới.
New Zealand	N/A	Áp dụng chung các luật bảo vệ người tiêu dùng hiện hành.
Thái lan	N/A	Áp dụng chung các luật bảo vệ người tiêu dùng hiện hành

Mỹ	Tập đoàn bảo hiểm tiền gửi liên bang đã xác định rằng bảo hiểm tiền gửi không áp dụng cho hầu hết các thẻ lưu trữ tiền do các định chế nhận tiền gửi phát hành	Các bảo vệ về mặt pháp lý của liên bang có hạn chế và các luật của từng bang đối với các định chế tài chính có thể áp dụng.

1.3.2.3. Rủi ro và an toàn hệ thống tài chính

An toàn về tài chính của bất cứ nhà phát hành và hệ thống thanh toán nào đều dựa trên sự an toàn về khả năng thanh toán, về vốn, kiểm soát nội bộ và độ ổn định hệ thống. Việc quản lý phải đảm bảo các chính sách, trình tự quản lý rủi ro và kiểm soát nội bộ để bảo vệ sự toàn vẹn tài chính của định chế tài chính đó. Các biện pháp đảm bảo an toàn về mặt kỹ thuật đóng vai trò rất lớn đối với sự tin cậy và chắc chắn về tài chính và việc triển khai xây dựng một hệ thống phát hành và thanh toán điện tử.

Bảng 1.2: Đánh giá rủi ro và an toàn hệ thống tài chính tại một số quốc gia trên thế giới

Nước	Rủi ro
Australia	Rủi ro hoạt động, ảnh hưởng danh tiếng, rủi ro sử dụng đối tác bên ngoài, rủi ro chiến lược, rủi ro pháp lý, rủi ro mất khả năng thanh toán. Nhận thức của khách hàng về nhà cung cấp dịch vụ cũng như người phải chịu trách nhiệm pháp lý trong trường hợp có xung đột về lợi ích là chưa rõ ràng
Canada	Dự thảo về hành vi pháp lý đối với các hệ thống giao dịch thay thế của nước ngoài
Trung quốc	N/A
Hồng Kông	Rủi ro chiến lược, hoạt động, an toàn và danh tiếng. Vấn đề bảo vệ người sử dụng và thông tin cho người sử dụng trong môi trường Internet
Indonesia	Vấn đề bảo vệ dữ liệu giao dịch khi sử dụng mạng Internet
Hàn quốc	Các tổ chức phi tài chính gặp vấn đề khi gia nhập vào hoạt động dịch vụ thanh quyết toán. Vấn đề công nhận chữ ký điện tử
Malaysia	Rủi ro trong bảo vệ dữ liệu và vấn đề hạ tầng CNTT
Mehico	Vấn đề an toàn hệ thống điện tử và rửa tiền
New	Các rủi ro thông thường đối với hoạt đông tài chính đều có thể xảy ra

Zealand	
Singapore	Vấn đề khuôn khổ pháp lý liên quan tới việc mở rộng dịch vụ qua mạng Internet
Đài loan	N/A
Thái lan	Vấn đề an toàn cho hệ thống và dữ liệu, quản lý rủi ro, phòng ngừa và kiểm soát nội bộ, bảo vệ người sử dụng và bảo mật thông tin giao dịch trong môi trường mạng mở, các hoạt động gian lận kể cả rửa tiền
Mỹ	Những thiệt hại tài chính hoặc trong trường hợp gây rối quan trọng

1.3.2.4. Những trở ngại và thách thức trong việc triển khai hệ thống thanh toán điện tử

Mức độ trở ngại và thách thức trong việc triển khai hệ thống thanh toán điện tử phụ thuộc vào điều kiện đặc thù và trình độ phát triển của từng quốc gia, tuy nhiên nội dung các trở ngại chính được các quốc gia quan tâm đề cập tới là:

- Hạ tầng pháp lý liên quan tới tranh chấp thương mại, bảo vệ người tiêu dùng, an toàn dữ liệu, chữ ký điện tử

- Hạ tầng cơ sở viễn thông đối với các quốc gia đang phát triển

- Vấn đề an toàn hệ thống, quản lý rủi ro.

Đối với các quốc gia mới tham gia TMĐT, các doanh nghiệp còn đề cập tới thách thức trong việc tăng tốc độ phổ cập TMĐT, giảm khoảng cách với các quốc gia phát triển mà ở đó chính phủ các nước đang phát triển chưa đề ra được những chính sách khuyến khích hỗ trợ rõ ràng, liên tục.

Bảng 1.3: Những trở ngại và thách thức trong việc triển khai hệ thống thanh toán điện tử tại một số quốc gia trên thế giới

Nước	Trở ngại và thách thức
Australia	Rủi ro hoạt động, ảnh hưởng danh tiếng, rủi ro sử dụng đối tác bên ngoài, rủi ro chiến lược, rủi ro pháp lý, rủi ro mất khả năng thanh toán. Nhận thức của khách hàng về nhà cung cấp dịch vụ cũng như người phải chịu trách nhiệm pháp lý trong trường hợp có xung đột về lợi ích là chưa rõ ràng.
Canada	Dự thảo về hành vi pháp lý đối với các hệ thống giao dịch thay thế của nước ngoài
Trung quốc	N/A
Hồng Kông	Rủi ro chiến lược, hoạt động, an toàn và danh tiếng Vấn đề bảo vệ người sử dụng và thông tin cho người sử dụng trong môi trường Internet

Indonesia	Vấn đề bảo vệ dữ liệu giao dịch khi sử dụng mạng Internet
Hàn quốc	Các tổ chức phi tài chính gặp vấn đề khi gia nhập vào hoạt động dịch vụ thanh quyết toán. Vấn đề công nhận chữ ký điện tử
Malaysia	Rủi ro trong bảo vệ dữ liệu và vấn đề hạ tầng CNTT
Mehico	Vấn đề an toàn hệ thống điện tử và rửa tiền
New Zealand	Các rủi ro thông thường đối với hoạt đông tài chính đều có thể xảy ra
Singapore	Vấn đề khuôn khổ pháp lý liên quan tới việc mở rộng dịch vụ qua mạng Internet
Đài loan	N/A
Thái lan	Vấn đề an toàn cho hệ thống và dữ liệu, quản lý rủi ro, phòng ngừa và kiểm soát nội bộ, bảo vệ người sử dụng và bảo mật thông tin giao dịch trong môi trường mạng mở, các hoạt động gian lận kể cả rửa tiền. Chính sách quốc gia về TTĐT
Mỹ	Những thiệt hại tài chính hoặc trong trường hợp gây rối quan trọng

CÂU HỎI CHƯƠNG 1

[1]. Trình bày cơ sở hình thành và phát triển thanh toán điện tử?

[2]. Trình bày lịch sử phát triển của các hình thái tiền tệ?

[3]. Trình bày quá trình phát triển của thanh toán điện tử?

[4]. Nêu khái niệm thanh toán điện tử?

[5]. Phân tích lợi ích và hạn chế của thanh toán điện tử?

[6]. Phân loại các hình thức thanh toán điện tử?

[7]. Trình bày yêu cầu đối với thanh toán điện tử?

[8]. Trình bày về hoạt động và vai trò của các bên tham gia thanh toán điện tử?

[9]. Liên hệ thực tế tình hình thanh toán điện tử tại Việt Nam?

[10]. Liên hệ thực tế tình hình thanh toán điện tử trên thế giới?

TÀI LIỆU THAM KHẢO CHƯƠNG 1

[1]. Nguyễn Văn Hồng và Nguyễn Văn Thoan, Giáo trình TMĐT căn bản, NXB Bách Khoa – Hà Nội, 2013

[2]. Nguyễn Văn Hùng (chủ biên), TMĐT - cẩm nang, NXB Kinh tế TP Hồ Chí Minh 2013

[3]. Lê Quân & Hoàng Văn Hải, Giáo trình quản trị tác nghiệp doanh nghiệp thương mại, NXB Thống Kê, 2010

[4]. Thái Thanh Sơn và Thái Thanh Tùng, TMĐT trong thời đại số, NXB Thông tin và Truyền thông, 2017

TIẾNG NƯỚC NGOÀI

[5]. Andreas Meier & Henrik Stormer, eBusiness & eCommerce - Managing the Digital Value Chain, Springer, 2009

[6]. Dave Chaffey, E-business and E-commerce Management: Strategy, Implementation and Practice – 6th, Pearson Education, 2015

[7]. Arch G. Woodside & Peter J. LaPlaca, Handbook of Strategic e-Business Management, Springer-Verlag Berlin Heidelberg, 2014.

[8]. Kenneth C. Laudon & Carol Guercio Traver: E-commerce Business, Technology, Society: 13th edition: Pearson Publishing House, 2017.

CHƯƠNG 2: HỆ THỐNG THANH TOÁN ĐIỆN TỬ

2.1. Hệ thống thanh toán thẻ

2.1.1 Khái niệm thẻ thanh toán

Thẻ thanh toán là một phương tiện thanh toán tiện dụng và tiên tiến trên thế giới. Thẻ thanh toán ra đời và phát triển gắn liền với sự phát triển và việc ứng dụng công nghệ tin học vào hoạt động của các ngân hàng thương mại. Đối với thẻ thanh toán có rất nhiều khái niệm để diễn đạt. Sau đây là một số khái niệm về thẻ thanh toán:

- Thẻ thanh toán là một phương tiện thanh toán tiền mua hàng hoá, dịch vụ hoặc có thể được dùng để rút tiền mặt tại các ngân hàng đại lý hoặc các máy rút tiền tự động.

- Thẻ thanh toán là một loại thẻ giao dịch tài chính được phát hành bởi ngân hàng, các tổ chức tài chính hay các công ty.

- Thẻ thanh toán là một phương tiện thanh toán không dùng tiền mặt mà người chủ thẻ có thể sử dụng để rút tiền mặt hoặc thanh toán tiền mua hàng hóa, dịch vụ tại các điểm chấp nhận thanh toán bằng thẻ.

Trong nội dung này, chúng tôi tiếp cận thẻ thanh toán là loại thẻ do ngân hàng phát hành. Thẻ thanh toán là phương tiện thanh toán không dùng tiền mặt, do ngân hàng phát hành thẻ cấp cho khách hàng sử dụng để thanh toán tiền hàng hóa dịch vụ hoặc để rút tiền mặt ở các máy rút tiền tự động hay tại các ngân hàng đại lý trong phạm vi số dư của tài khoản tiền gửi hoặc hạn mức tín dụng được ký kết giữa ngân hàng phát hành thẻ và chủ thẻ.

Sử dụng thẻ thanh toán trong giao dịch thể hiện một số nổi trội:

Sự tiện lợi: Là một phương tiện thanh toán không dùng tiền mặt, thẻ cung cấp cho khách hàng sự tiện lợi mà không một phương tiện thanh toán nào có thể mang lại được. Bằng việc sở hữu một chiếc thẻ khách hàng có thể thanh toán ở bất cứ nơi nào mà không cần phải mang theo tiền mặt hay séc du lịch, và không phụ thuộc vào khối lượng tiền họ cần thanh toán đặc biệt đối với những người hay phải đi ra nước ngoài đi công tác hay là đi du lịch. Thẻ được coi là phương tiện thanh toán ưu việt nhất trong số các phương tiện thanh toán phục vụ tiêu dùng.

Sự linh hoạt: Với nhiều loại đa dạng, phong phú, thẻ thích hợp với mọi đối tượng khách hàng, từ những khách hàng có thu nhập thấp (thẻ thường) cho tới những khách hàng có thu nhập cao (thẻ vàng), khách hàng có nhu cầu rút tiền mặt (thẻ rút tiền mặt), cho tới nhu cầu du lịch giải trí… thẻ cung cấp cho khách hàng độ thỏa dụng tối đa, thoả mãn nhu cầu của mọi đối tượng khách hàng.

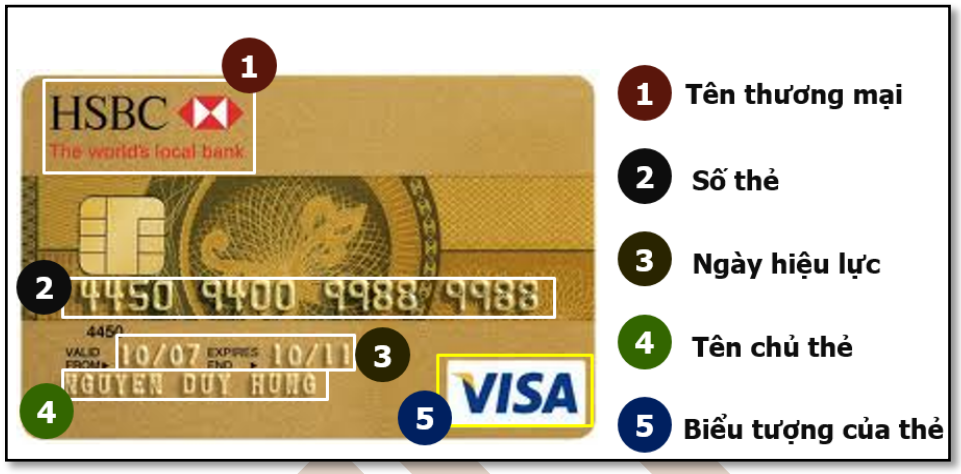
Sự an toàn và nhanh chóng: Chủ thẻ có thể hoàn toàn yên tâm về số tiền của mình trước nguy cơ bị mất cắp. Thậm chí, dù thẻ có thể bị lấy cắp, ngân hàng cũng bảo vệ tiền cho chủ thẻ bằng số PIN và chữ ký trên thẻ… nhằm tránh khả năng rút tiền của kẻ ăn trộm.

Hơn thế nữa, hầu hết các giao dịch thẻ đều được thực hiện qua mạng kết nối trực tuyến từ cơ sở chấp nhận thẻ hay điểm rút tiền mặt tới ngân hàng thanh toán, ngân hàng phát hành và các tổ chức thẻ Quốc tế. Việc ghi Nợ - Có cho các chủ thể tham gia quy trình thanh toán được thực hiện một cách tự động do đó quá trình thanh toán dễ dàng, tiện lợi và nhanh chóng.

2.1.2 Cấu tạo thẻ thanh toán

Các loại thẻ thường có đặc điểm chung là được làm bằng plastic, có kích thước theo tiêu chuẩn quốc tế là 85,60 × 53,98 x 0,76 (mm). Trên thẻ có in các thông số nhận dạng như: nhãn hiệu thương mại của thẻ, tên và logo của nhà phát hành thẻ, số thẻ, tên chủ thẻ và ngày có hiệu lực của thẻ và một số đặc tính khác tùy theo quy định của các tổ chức thẻ quốc tế hoặc hiệp hội phát hành thẻ…

Mặt trước của thẻ:



Hình 2.1: Mặt trước của thẻ thanh toán

- Biểu tượng: mỗi loại thẻ có một biểu tượng riêng, mang tính đặc trưng của tổ chức phát hành thẻ, đây được xem như một đặc tính mang tính an ninh nhằm chống giả mạo. Ví dụ:

+ VISA: hình chữ nhật ba mầu: xanh, trắng, vàng có chữ Visa chạy ngang giữa màu trắng, trên hình chữ nhật ba mầu là hình chim bồ câu đang bay in chìm.

+ MASTERCARD: có hai hình tròn lồng nhau nằm ở góc dưới bên phải (một hình mầu da cam, một hình mầu đỏ) và dòng chữ Mastercard nằm ở giữa; trên hai hình tròn lồng nhau là hai nửa quả cầu lồng nhau in chìm.

+ JBC: biểu tượng ba mầu xanh công nhân, đỏ xanh lá cây, có chữ JBC chạy ngang giữa.

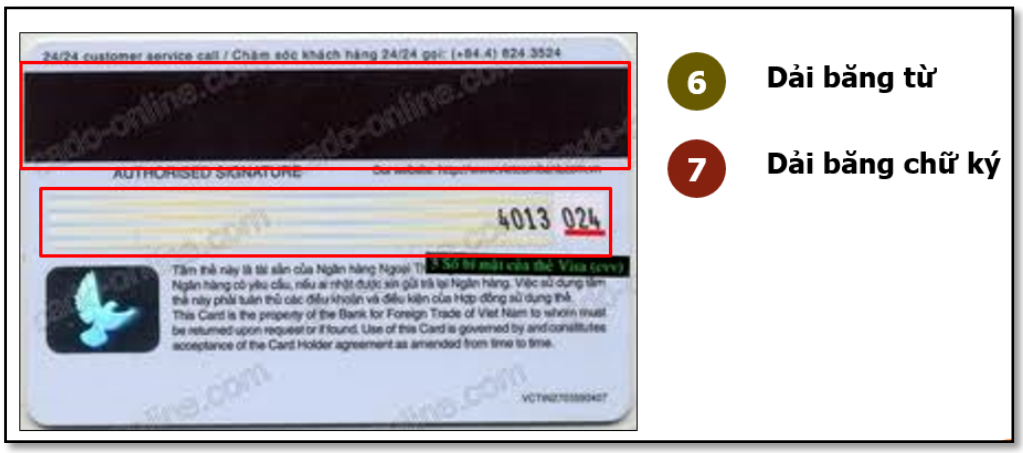
+ AMEX: biểu tượng hình đầu người chiến binh.

- Số thẻ: số này dành riêng cho mỗi chủ thẻ, được dập nổi trên thẻ và được in lại trên hóa đơn khi chủ thẻ thanh toán bằng thẻ. Tùy theo từng loại thẻ mà chữ số khác nhau và cách cấu trúc theo nhóm cũng khác nhau.

- Thời gian có hiệu lực của thẻ: là thời gian mà thẻ được phép lưu hành. Tùy theo từng loại thẻ mà có thể ghi ngày hiệu lực cuối cùng của thẻ hoặc ngày đầu tiên đến ngày cuối cùng được sử dụng thẻ.

- Họ và tên chủ thẻ: in chữ nổi, là tên của cá nhân nếu là thẻ cá nhân, tên của người được ủy quyền sử dụng nếu là thẻ công ty. Ngoài ra, có thẻ còn có cả ảnh của chủ thẻ.

Mặt sau của thẻ:



Hình 2.2: Mặt sau của thẻ thanh toán

- Dải băng từ có khả năng lưu trữ các thông tin như: số thẻ, ngày hiệu lực, tên chủ thẻ, ngân hàng phát hành

- Dải băng chữ ký: trên dải băng này phải có chữ ký của chủ thẻ để cơ sở chấp nhận thẻ có thể đối chiếu chữ ký khi thực hiện thanh toán thẻ.

- Mã bảo mật của thẻ: thẻ Visa, MasterCard, JCB gọi là CVV, là một dãy gồm ba chữ số nằm ở mặt sau của thẻ, đối với thẻ Amercian Express gọi là CSC, là một dãy gồm bốn chữ số nằm ở mặt trước của thẻ.

2.1.3 Một số loại thẻ thanh toán

2.1.3.1 Thẻ tín dụng

✓ **Khái niệm**

Thẻ tín dụng là thẻ cho phép chủ thẻ thực hiện giao dịch thẻ trong phạm vi hạn mức tín dụng đã được cấp theo thỏa thuận với tổ chức phát hành thẻ. Đây là loại thẻ được sử dụng phổ biến nhất trong thanh toán trực tuyến hiện nay, theo đó người chủ thẻ được sử dụng một hạn mức tín dụng tuần hoàn để mua sắm hàng hoá, dịch vụ tại những cơ sở chấp nhận loại thẻ này.

Về bản chất đây là một dịch vụ tín dụng thanh toán với hạn mức chi tiêu nhất định do ngân hàng cung cấp cho khách hàng căn cứ vào khả năng tài chính, số tiền ký quỹ hoặc tài sản thế chấp của khách hàng. Hiện tại, trên thế giới Visa và MasterCard là hai tổ chức thẻ lớn nhất cung cấp chịu trách nhiệm phát hành thẻ quốc tế.

Visa International (Tổ chức thẻ quốc tế Visa): thẻ Visa, tiền thân là Bank Americard do Bank of America phát hành vào năm 1960, hiện nay là loại thẻ có quy mô phát triển lớn nhất trên toàn cầu. Tính đến tháng 9/2019, doanh thu của Visa Inc. tăng 11,49% trong năm tài chính 2019 so với năm tài chính 2018 lên thành 22,98 tỷ đo la Mỹ, thu nhập ròng tăng 17,18 % lên thành 11,65 tỷ đô la Mỹ [1]

Master Card International (Tổ chức thẻ quốc tế Mastercard): MasterCard ra đời vào năm 1966 với tên gọi là Master Charge do hiệp hội thẻ liên Ngân hàng ICA (Interbank Card Association) phát hành thông qua các Ngân hàng thành viên trên thế giới. Năm 1990, một hệ

[1] https://www.msn.com/vi-vn/money/stockdetails/financials/fi-a256cw Truy cập ngày 24 tháng 11 năm 2019

thống ATM lớn nhất thế giới được sử dụng phục vụ cho những người dùng thẻ MasterCard. Cũng năm này, MasterCard đã phát hành được hơn 178 triệu thẻ, có 5.000 thành viên phát hành và 9 triệu điểm tiếp nhận thẻ. Doanh thu của Master Card Inc. tăng 19,63 % trong năm tài chính 2018 so với năm tài chính 2017 lên thành 14,95 tỷ đô la Mỹ, thu nhập ròng tăng 49,66 % lên thành 5,86 tỷ đô la Mỹ (nguồn (1) đã dẫn).

✓ **Phân loại thẻ tín dụng**

- Phân loại theo hạn mức

Tùy vào từng loại ngân hàng sẽ cấp những hạn mức khác nhau cho khách hàng, về cơ bản sẽ là thẻ thường (thẻ chuẩn), thẻ vàng, thẻ kim cương (bạch kim); và cũng tùy vào từng ngân hàng mà mỗi hạng thẻ sẽ có mức tín dụng là khác nhau.

Ví dụ đối với ngân hàng Agribank: Thẻ chuẩn (hạn mức tín dụng tối đa là 50 triệu đồng), thẻ vàng (hạn mức tín dụng tối đa từ 50 triệu đồng đến 300 triệu đồng), thẻ bạch kim (hạn mức tín dụng tối đa từ 300 triệu đồng đến 500 triệu đồng).

Còn đối với ngân hàng Techcombank: Có ba loại tương ứng với ba hạn mức khác nhau: hạng chuẩn (hạn mức tín dụng tối đa 40 triệu đồng), hạng vàng (hạn mức tín dụng tối đa 80 triệu đồng), thẻ visa platinum (hạn mức tín dụng lên tới 1 tỷ đồng).

- Phân loại theo khu vực

+ Thẻ tín dụng nội địa

Đây là loại thẻ tín dụng chỉ có thể thanh toán các dịch vụ hoặc hàng hóa trong nước. Ưu điểm của loại thẻ này là phí quản lý và phí dịch vụ không quá cao. Tuy nhiên thẻ tín dụng nội địa có hạn mức không lớn, thấp hơn thẻ tín dụng quốc tế. Điều này có thể đưa đến một số trở ngại khi khách hàng sử dụng. Đối với loại thẻ tín dụng nội địa không nhiều ngân hàng cung cấp, và mức phí thường niên cũng như một số mức phí khác rẻ hơn, điều kiện tạo lập thẻ cũng không đòi hỏi cao như đối với thẻ tín dụng quốc tế. Ví dụ: Thẻ tín dụng nội địa Sacombank family, hoặc thẻ tín dụng nội địa của ACB là ACB Express.

+ Thẻ tín dụng quốc tế

Đây là loại thẻ có thể thanh toán trong và ngoài nước, đưa đến sự thuận tiện cho khách hàng đặc biệt khi mua sắm hoặc đi du lịch ở nước ngoài. Khách hàng có thể thanh toán trực tiếp bằng các loại thẻ tín dụng quốc tế mà không cần đổi tiền mặt. Đặc biệt, hạn mức của thẻ tín dụng quốc tế có thể lên đến vài tỷ đồng. Tuy nhiên, cũng như thẻ tín dụng nội địa, phí rút tiền mặt của thẻ tín dụng quốc tế khá cao, vào khoảng 3 đến 5% số tiền giao dịch tùy từng ngân hàng. Bên cạnh đó, với loại thẻ này người dùng cũng có thể gặp trường hợp không kiểm soát được tài chính khi chi tiêu quá nhiều. Hầu hết các ngân hàng hiện nay đều cung cấp thẻ tín dụng quốc tế với những thương hiệu thẻ lớn như Visa, MasterCard, American Express.

✓ **Đặc điểm của thẻ tín dụng**

Thẻ tín dụng là loại thẻ mà chủ sở hữu thẻ tạo lập được bằng cách sử dụng uy tín cá nhân của mình hoặc tài sản thế chấp

+ Sử dụng uy tín cá nhân: Với hình thức tín chấp uy tín cá nhân càng cao thì hạn mức càng cao. Cách thức phổ biến nhất mà các ngân hàng hay sử dụng để xem xét điều kiện tín chấp đó là bảng lương, thu nhập.

+ Sử dụng tài sản thế chấp: Thông thường hiện nay các ngân hàng cho phép thế chấp

bằng sổ tiết kiệm là chủ yếu. Tuy nhiên vấn đề mở thẻ tín dụng bằng tài sản thế chấp cũng khá khó khăn, không phải cứ có tài sản thế chấp/sổ tiết kiệm là có thể mở thẻ tín dụng ngay lập tức. Ví dụ: Ngân hàng Sacombank quy định tài khoản tiền gửi hoạt động ít nhất 6 tháng và số dư tối thiểu là 32 triệu đồng/tháng. Có thu nhập ổn định đảm bảo khả năng trả nợ 4 triệu đồng/tháng. Khi tiến hành thủ tục mở thẻ tín dụng thế chấp bằng sổ tiết kiệm khách hàng phải ký giấy xác nhận phong tỏa tài sản tiền gửi. Hoặc nếu sử dụng bất động sản làm tài sản thế chấp thì khách hàng phải ký hợp đồng cầm cố tài sản.

Đặc biệt một số ngân hàng nước ngoài ví dụ ANZ, điều kiện còn khó khăn hơn: sổ tiết kiệm trị giá ít nhất phải từ 50 triệu đồng trở lên với kỳ hạn từ 2 tháng trở lên và hạn mức tối đa là 80% tài sản thế chấp.

Chi tiêu trước trả tiền sau

Đây là đặc trưng của thẻ tín dụng, cho khách hàng chi tiêu trước để mua hàng hóa và dịch vụ, sau đó khách hàng sẽ phải thanh toán tiền. Khách hàng khi có thẻ tín dụng sẽ được chi tiêu trong hạn mức của thẻ, đến hạn khách hàng sẽ nhận được bản sao kê của ngân hàng về các khoản đã mua và phải thanh toán những khoản đó.

Chủ thẻ không phải trả bất kỳ một khoản lãi nào nếu việc thanh toán khoản tiền là đúng thời hạn

Thông thường các ngân hàng sẽ cho phép khách hàng thanh toán tiền là 15 ngày kể từ ngày gửi sao kê hoặc là được hưởng tối đa là 45 ngày không phải chịu lãi suất (nếu ngày giao dịch trùng với ngày đầu tiên trong chu kỳ của tháng sau). Tuy nhiên cũng tùy vào từng hạng thẻ mà thời hạn thanh toán là khác nhau. Ví dụ thẻ bạch kim hoặc thẻ premier của ngân hàng HSBC sẽ được hưởng tối đa 55 ngày không phải chịu lãi suất.

Ngoài ra thẻ tín dụng còn một số đặc trưng khác :

- Các tài khoản hoặc tài sản thế chấp để phát hành thẻ tín dụng độc lập với việc chi tiêu.

- Nếu tài khoản thế chấp là tiền mặt, chủ thẻ sẽ được hưởng lãi suất ngân hàng với kỳ hạn phụ thuộc vào thời hạn hiệu lực của thẻ.

- Thẻ tín dụng quốc tế có thể chi tiêu bằng tất cả các loại tiền

- Thẻ tín dụng mất phí cao khi rút tiền mặt

- Chủ thẻ có thể thanh toán toàn bộ số dư phát sinh trong hóa đơn hoặc một phần số dư trong hóa đơn tuy nhiên, phần số dư trả chậm sẽ phải chịu lãi suất và cộng dồn vào hóa đơn tháng tiếp theo.

2.1.3.2 Thẻ ghi nợ

- ✓ **Khái niệm**

Thẻ ghi nợ là loại thẻ cho phép chủ sở hữu thẻ chi tiêu trực tiếp trên tài khoản tiền gửi của mình tại ngân hàng phát hành thẻ. Với loại thẻ này, chủ thẻ có thể chi trả tiền hàng hoá, dịch vụ dựa trên số dư tài khoản tiền gửi của mình tại ngân hàng phát hành thẻ. Thẻ thanh toán không có hạn mức tín dụng vì nó phụ thuộc vào số dư hiện hữu trên tài khoản của chủ thẻ. Số tiền chủ thẻ chi tiêu sẽ được khấu trừ ngay vào tài khoản của chủ thẻ thông qua những thiết bị điện tử đặt tại cơ sở chấp nhận thẻ. Trong một số trường hợp, chủ thẻ cũng có thể được ngân hàng cấp cho một mức thấu chi, tuỳ theo sự thoả thuận giữa chủ thẻ và ngân hàng.

Đó là một khoản tín dụng ngắn hạn mà ngân hàng cấp cho chủ thẻ.

✓ **Phân loại thẻ ghi nợ**

Phân loại theo phương thức khấu trừ tài khoản

- Thẻ ghi nợ trực tuyến (online): Là loại thẻ mà giá trị những giao dịch được khấu trừ ngay lập tức vào tài khoản của chủ thẻ. Những thông tin về giao dịch được kết nối trực tiếp từ thiết bị điện tử đặt tại cơ sở chấp nhận thẻ hoặc điểm rút tiền mặt tới ngân hàng phát hành. Giá trị những giao dịch được khấu trừ trực tiếp và lập tức vào tài khoản của chủ thẻ. Với thẻ ghi nợ online thì khi thanh toán đòi hỏi được cấp phép ngay lập tức.

- Thẻ ghi nợ ngoại tuyến (offline): Là loại thẻ mà giá trị những giao dịch được khấu trừ vào tài khoản chủ thẻ sau đó vài ngày. Thông tin giao dịch được lưu tại máy điện tử của cơ sở chấp nhận thẻ và được chuyển đến ngân hàng phát hành muộn hơn (không có kết nối trực tiếp vào thời điểm thanh toán). Giá trị những giao dịch sẽ được khấu trừ vào tài khoản của chủ thẻ sau đó vài ngày, thường là từ hai đến ba ngày.

Phân loại theo phạm vi khu vực

- Thẻ ghi nợ nội địa: Là loại thẻ được sử dụng để giao dịch ở trong nước, hiện nay đa phần chúng ta đều sử dụng thẻ ghi nợ nội địa. Các thẻ nội địa ở Việt Nam đa phần vẫn được làm bằng công nghệ thẻ từ.

- Thẻ ghi nợ quốc tế : Là loại thẻ được sử dụng để giao dịch ở nước ngoài, số lượng người sử dụng thẻ ghi nợ quốc tế thì ít hơn. Hiện nay tất cả các thẻ ghi nợ quốc tế ở Việt Nam đều sử dụng công nghệ chip thông minh.

✓ **Đặc điểm của thẻ ghi nợ**

Chi tiêu tới đâu, khấu trừ tài khoản luôn tới đó

Thẻ ghi nợ đơn giản là một tài khoản tiền gửi của khách hàng tại ngân hàng, khách hàng chi tiêu dựa trên chính số dư của mình vì thế đối với thẻ ghi nợ khách hàng chi tiêu tới đâu sẽ bị khấu trừ tiền luôn tới đó.

Chi tiêu bằng tất cả các loại tiền

Đây là đặc điểm đối với thẻ ghi nợ quốc tế, đối với thẻ ghi nợ quốc tế chủ thẻ có thể chi tiêu bằng tất cả các loại tiền, tuy nhiên sẽ phải mất phí chuyển đổi ngoại tệ.

Không phải mất phí hoặc mất một khoản phí rất nhỏ khi rút tiền

Đó là sự khác biệt rất lớn giữa thẻ tín dụng và thẻ ghi nợ, thẻ tín dụng sẽ phải mất phí cao do tiền chủ thẻ sử dụng chính là tiền đi vay của ngân hàng, còn đối với thẻ ghi nợ, chủ thẻ sẽ chi tiêu bằng chính số dư trên tài khoản tiền gửi của mình.

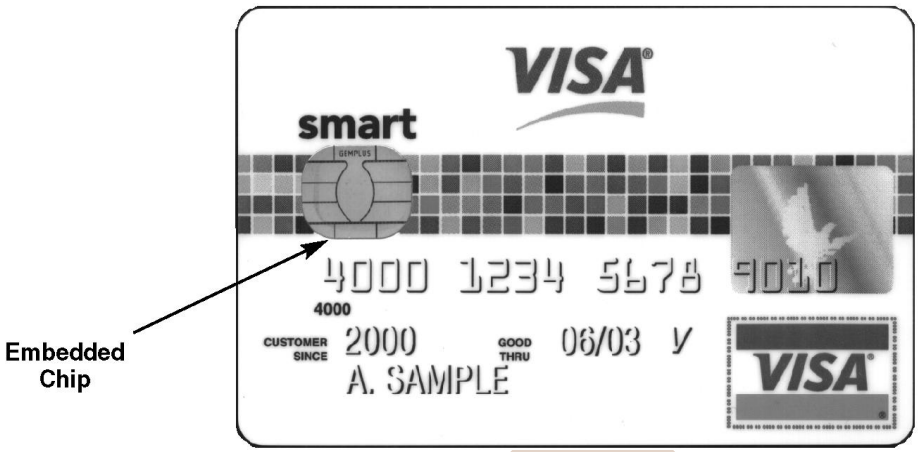
Số dư trong tài khoản được hưởng lãi suất không kỳ hạn

2.1.3.3 Thẻ thông minh

✓ **Khái niệm**

Thẻ thông minh là loại thẻ có kích thước như một chiếc thẻ tín dụng thông thường nhưng trên đó có gắn một con chip – vi mạch điện tử. Vi mạch điện tử này bao gồm một thiết bị ra vào đặc trưng, một bộ vi xử lý, một bộ nhớ. Tất cả những thiết bị này sẽ giúp lưu trữ rất nhiều những loại thông tin khác nhau từ các thông tin như số thẻ tín dụng, hồ sơ sức khoẻ cá nhân, bảo hiểm y tế, hồ sơ công tác, bằng lái xe… với dung lượng lớn gấp hàng trăm lần so

với dung lượng của các thông tin có thể lưu trữ trên một thẻ tín dụng thông thường. Thẻ thông minh có khả năng lưu trữ và xử lý thông tin với độ an toàn cao nên được sử dụng trong rất nhiều ngành như ngân hàng, tài chính, y tế hay bưu chính viễn thông. Hiện nay, thẻ thông minh được sử dụng tại rất nhiều nước. Công nghệ thẻ thông minh được khởi đầu tại Pháp nhưng ít thông dụng hơn ở Mỹ, nơi mà người ta hay sử dụng thẻ tín dụng là chủ yếu.



Hình 2.3: Thẻ thông minh

- ✓ **Phân loại**

Dựa trên phương thức đọc thẻ, người ta chia thẻ thông minh thành hai loại cơ bản:

Thẻ tiếp xúc vật lý (thẻ có khả năng liên kết) – Contact smart card

Thẻ tiếp xúc vật lý là thẻ thông minh mà trên mạch vi xử lý có gắn một miếng kim loại nhỏ mạ vàng. Thẻ sẽ được kích hoạt khi đưa thẻ này vào thiết bị đọc thẻ. Khi đưa thẻ tiếp xúc với thiết bị đọc thẻ, thông tin dữ liệu trên thẻ sẽ được truyền từ chip qua miếng kim loại nhỏ mạ vàng sang thiết bị đọc thẻ.

Để đọc, ghi thông tin, bề mặt con chip phải tiếp xúc trực tiếp với đầu đọc thẻ. Loại thẻ này được sử dụng nhiều trong tài chính (công nghệ của thẻ tiếp xúc phi vật lý thường được sử dụng để tạo ra thẻ ghi nợ và thẻ tín dụng). Truyền thông (sim điện thoại) vì ưu điểm giá cả không quá đắt, đáp ứng nhiều tiêu chuẩn về công nghệ, độ bảo mật cao. Khi được đưa vào máy đọc, chip trên thẻ sẽ giao tiếp với các tiếp điểm điện tử cho phép đọc các thông tin từ chip và viết thông tin lên nó. Thẻ thông minh loại này không có pin, năng lượng làm việc sẽ được cấp trực tiếp từ máy đọc thẻ.

Thẻ phi tiếp xúc (thẻ có khả năng liên kết ở phạm vi gần) – Contactless smart card

Thẻ phi tiếp xúc là loại thẻ thông minh mà trên mạch vi xử lý có gắn anten. Khi đưa thẻ lại gần thiết bị đọc thẻ, thông tin dữ liệu trên thẻ sẽ được truyền từ chip qua anten sang anten của thiết bị đọc thẻ. Hiện nay với công nghệ thẻ phi tiếp xúc được ứng dụng ở nhiều quốc gia và thanh toán cực nhanh (dưới 2 giây), ví dụ như thẻ thông minh của IBM.

Tốc độ xử lý của thẻ phi tiếp xúc là cao hơn so với các thẻ tiếp xúc. Vì vậy thẻ phi tiếp xúc thường được ứng dụng tại những nơi cần phải xử lý nhanh như các hệ thống quá cảnh, trên các phương tiện giao thông công cộng, siêu thị, tàu điện ngầm. Thẻ phi tiếp xúc đắt hơn nhưng lại không an toàn bằng thẻ tiếp xúc.

Thẻ lưỡng tính (thẻ lai ghép) - Hybrid smart card

Là thẻ kết hợp các đặc điểm của thẻ tiếp xúc và thẻ không tiếp xúc. Dữ liệu được truyền hoặc bằng phương pháp tiếp xúc trực tiếp thẻ với đầu đọc hoặc qua tín hiệu vô tuyến. Thẻ lưỡng tính đắt hơn rất nhiều so với hai loại thẻ trên. Đối với loại thẻ lưỡng tính, một số phần thẻ không tiếp xúc hay dùng để quản lý ra vào, thanh toán cước phí giao thông; còn phần thẻ có chip tiếp xúc thường để quản lý một số thông tin bảo mật khác liên quan đến chủ thẻ. Ví dụ như thẻ giao thông nhiều ứng dụng của Porto, gọi là Andante, mà dùng một chip cho cả tiếp xúc và phi tiếp xúc.

Đối với tất cả các loại thẻ, thiết bị đọc thẻ là rất quan trọng trong sự hoạt động của hệ thống. Thiết bị đọc thẻ bản chất là một thiết bị đọc và ghi. Mục đích chủ yếu của thiết bị đọc thẻ là hoạt động như thiết bị liên kết giữa thẻ và hệ thống chủ lưu giữ dữ liệu ứng dụng và xử lý dữ liệu. Có hai loại thẻ cơ bản nên có hai loại thiết bị đọc thẻ (tiếp xúc và phi tiếp xúc) phù hợp với các loại thẻ riêng.

- ✓ **Ứng dụng của thẻ thông minh**

Sự thay đổi trong cách sử dụng thẻ thông minh được định hướng bởi những ứng dụng của nó. Sau đây là những ứng dụng quan trọng nhất:

Thanh toán trong mua bán lẻ

Ứng dụng cơ bản nhất của thẻ thông minh là tích hợp trong thẻ thanh toán quốc tế (thẻ ATM) để thực hiện những giao dịch thanh toán. Người mua hàng sử dụng thẻ để mua hàng tại tất cả các điểm thanh toán chấp nhận thanh toán. Thẻ thông minh cũng có thể dùng như ví điện tử dùng trả tiền tại các trạm đỗ xe và các máy bán hàng tự động.

Trong lĩnh vực bán lẻ, nhiều loại dịch vụ này hướng đến những thị trường mà thanh toán thường được thực hiện bằng tiền mặt và tốc độ, sự tiện lợi là rất quan trọng, ví dụ các cửa hàng tiện dụng, trạm xăng, nhà hàng dịch vụ nhanh và thức ăn nhanh, rạp chiếu phim. Thanh toán phi tiếp xúc là ví dụ cho loại hình dịch vụ giá trị gia tăng này.

Chuyển tiếp phí trong giao thông công cộng

Trong những thành phố lớn ở Mỹ nhiều nước khác, người đi làm thường phải lái xe tới nơi đậu xe, lên tàu và sau đó di chuyển qua một hoặc nhiều xe điện ngầm, xe buýt để tới nơi làm việc. Nếu quá trình đó đòi hỏi sự kết hợp của tiền mặt và nhiều loại vé khác nhau thì nó sẽ rất phức tạp và rắc rối. Sự bất tiện này đã không khuyến khích người đi làm sử dụng phương tiện công cộng. Để loại bỏ sự bất tiện này, hầu hết người vận hành chuyển tiếp chính ở Mỹ đang thực hiện những hệ thống vé phí thẻ thông minh. Chính phủ Liên bang Mỹ cũng cũng khuyến khích những người chủ trợ cấp cho nhân viên sử dụng giao thông công cộng. Các nhà vận hành chuyển tiếp của nhiều thành phố lớn trên thế giới đang chuyển từ hệ thống phí không hợp nhất, phức tạp sang hệ thống đòi hỏi chỉ một thẻ phi tiếp xúc duy nhất, dù có bao nhiêu kiểu giao thông hoặc có bao nhiêu hãng giao thông và các công ty liên quan tham gia.

Một số nhà vận hành chuyển tiếp ở Mỹ đang tìm kiếm đối tác là các đại lý bán lẻ và các tổ chức tài chính để kết hợp thẻ chuyển tiếp của họ với thẻ thanh toán có thể được sử dụng để mua hàng hóa và dịch vụ như bữa ăn nhỏ, phí qua cầu, phí đỗ xe, mua thức ăn trong nhà hàng hoặc cửa hàng tạp phẩm gần trạm chuyển tiếp.

Định dạng điện tử (electronic identification – e-ID)

Bởi vì thẻ thông minh có khả năng lưu trữ thông tin cá nhân bao gồm ảnh, nhận dạng sinh trắc học, chữ ký số hóa và chìa khóa an toàn cá nhân nên chúng được sử dụng trong nhiều loại nhận dạng, kiểm soát truy cập và ứng dụng xác nhận. Ví dụ, một vài nước như Trung Quốc, Ấn Độ, Bỉ đã lên kế hoạch hoặc thử nghiệm đưa ra chương trình thẻ thông minh định dạng quốc gia. Thẻ được thiết kế để giảm thủ tục ID và người dân có thể di chuyển tự do hơn trong nước. Thẻ ID có kích thước như thẻ ngân hàng tiêu chuẩn và sẽ sử dụng con chip phi tiếp xúc.

Một ứng dụng đang ngày càng phát triển rất nhanh đó là dùng chứng minh nhân dân kỹ thuật số. Trong ứng dụng này, thẻ thông minh được dùng như một bằng chứng để xác minh. Thẻ thông minh được sử dụng kết hợp với hệ thống mã hóa công khai (PKI) lưu trữ các thông tin liên quan và cần thiết về người chủ thẻ. Hệ thống này đã được áp dụng cho tất cả các công dân tại nhiều nước. Thẻ thông minh không tiếp xúc hiện đang được tích hợp vào hộ chiếu theo chuẩn ICAO (International Civil Aviation Organization - Tổ chức Hàng không Dân dụng Quốc tế) để tăng cường giải pháp an ninh trên phạm vi toàn thế giới. Khi dùng chung với các đặc điểm sinh trắc học, thẻ thông minh có độ tin cậy và an ninh tăng gấp hai đến ba lần.

Bảo vệ sức khỏe

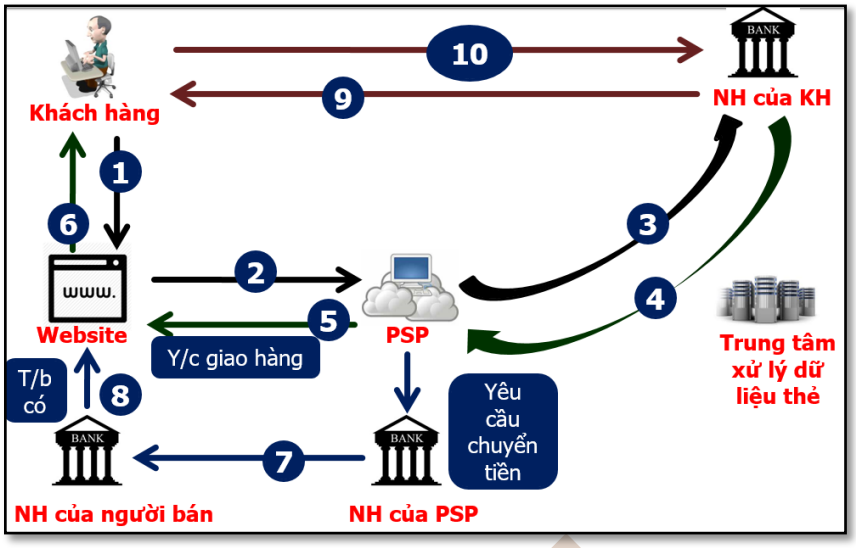
Nói chung, thẻ thông minh được sử dụng để lưu trữ dữ liệu, định dạng và xác nhận chủ thẻ, cho phép hoặc giới hạn khả năng truy cập tới các công trình vật lý hoặc nguồn thông tin. Trong việc bảo vệ sức khỏe, thẻ thông minh có những khả năng khác nhau, bao gồm:

- Lưu trữ thông tin y khoa cần thiết trong các trường hợp khẩn cấp.
- Tránh cho bệnh nhân phải cầm nhiều đơn thuốc của các bác sĩ khác nhau.
- Kiểm tra định dạng của bệnh nhân và thông tin về bảo hiểm
- Rút ngắn thời gian làm thủ tục nhập viện và khi giải quyết các trường hợp khẩn cấp.
- Cung cấp cho các bác sĩ đa khoa sự truy cập an toàn vào bệnh án của một bệnh nhân.
- Đẩy nhanh quá trình thanh toán và khiếu nại.
- Bệnh nhân có thể truy cập vào hồ sơ bệnh án qua Internet.

Mặc dù thẻ thông minh bảo vệ sức khỏe đã được xúc tiến đối với việc lưu kho dữ liệu (ví dụ lưu giữ thông tin y khoa cần thiết), nhưng trên thực tế hầu hết những thẻ này chỉ được sử dụng để kiểm tra quyền đối với các dịch vụ bảo vệ sức khỏe. Đây là lĩnh vực sử dụng trước hết của chúng, ví dụ ở Đức và Pháp có hai chương trình thẻ thông minh bảo vệ sức khỏe lớn nhất thế giới.

2.1.4 Quy trình thanh toán thẻ trực tuyến

Dưới đây là quy trình mua hàng sử dụng thẻ thanh toán trực tuyến ở góc độ tổng quát nhất:



Hình 2.4: Quy trình thanh toán thẻ trực tuyến

- Bước 1: Khách hàng truy cập vào website bán hàng, lựa chọn sản phẩm, lựa chọn phương thức thanh toán bằng thẻ, và bắt đầu tiến hành thanh toán bằng việc khai báo thông tin cá nhân / khai báo thông tin thẻ.

- Bước 2: Khách hàng được điều hướng để truy cập vào website của *nhà cung cấp dịch vụ thanh toán trung gian* (PSP : processing service provider) thông qua một kết nối an toàn (truy cập thông qua kết nối an toàn).

- Bước 3: Trên website này, khách hàng tiến hành khai báo thông tin về thẻ thanh toán. Thông tin về thẻ thanh toán mà khách hàng khai báo sẽ được máy chủ xử lý giao dịch của PSP truyền tải tới ngân hàng phát hành thẻ của khách hàng thông qua trung tâm xử lý dữ liệu thẻ.

- Bước 4: Ngân hàng phát hành thẻ tiến hành kiểm tra các thông tin về thẻ thanh toán mà khách hàng khai báo, sau đó xác thực việc thanh toán với nhà cung cấp dịch vụ thanh toán PSP thông qua trung tâm xử lý dữ liệu thẻ. Cụ thể ngân hàng phát hành thẻ tiến hành chuyển tiền từ tài khoản của khách hàng sang tài khoản ngân hàng của nhà cung cấp dịch vụ thanh toán PSP một số tiền mà khách hàng giao dịch.

- Bước 5: Nhà cung cấp dịch vụ thanh toán PSP sẽ gửi thông báo về phát sinh có trong tài khoản điện tử của website bán hàng được thiết lập bởi PSP và yêu cầu website bán hàng tiến hành giao hàng.

- Bước 6: Website bán hàng tiến hành giao hàng tới địa chỉ mà khách hàng yêu cầu

- Bước 7: Nhà cung cấp dịch vụ PSP yêu cầu ngân hàng của mình chuyển tiền vào tài khoản ngân hàng của website bán hàng với một số tiền bằng số tiền mà khách hàng giao dịch (số tiền đó có thể trừ phí giao dịch nếu có).

- Bước 8: Ngân hàng của website bán hàng gửi thông báo phát sinh có trong tài khoản tới người bán hoặc website bán hàng.

- Bước 9: Ngân hàng phát hành thẻ tiến hành gửi sao kê chi tiết về giao dịch cùng với yêu cầu thanh toán tới khách hàng.

- Bước 10: Khách hàng tiến hành kiểm tra sao kê và thanh toán với ngân hàng phát

hành thẻ.

2.1.5 Rủi ro thường gặp trong thanh toán thẻ

Rủi ro trong thanh toán thẻ là một trong những rủi ro thường gặp, có nhiều kiểu phân loại, nếu phân chia theo loại hình rủi ro thì sẽ có: rủi ro tín dụng, rủi ro kỹ thuật, rủi ro đạo đức. Nếu phân loại theo quy trình chịu rủi ro sẽ có: rủi ro trong phát hành, rủi ro trong thanh toán. Nếu phân loại theo đối tượng tiếp nhận rủi ro: rủi ro đối với ngân hàng, rủi ro đối với cơ sở chấp nhận thẻ, rủi ro đối với chủ thẻ, trong đó ngân hàng và chủ thẻ là những bên tham gia chịu nhiều rủi ro hơn cả.

2.1.5.1 Rủi ro đối với ngân hàng

Đơn xin phát hành thẻ giả: Do không thẩm định kĩ thông tin của khách hàng, ngân hàng có thể phát hành thẻ cho khách hàng đăng kí với những thông tin giả mạo. Và như vậy, ngân hàng có thể gặp rủi ro khi khách hàng không có khả năng thanh toán. Tuy vậy trên thực tế, điều này rất hiếm khi xảy ra vì hợp đồng thẻ rất dễ kiểm tra và có đảm bảo cao do có thế chấp hoặc tài khoản tiền gửi của khách hàng tại ngân hàng.

Chủ thẻ thật không nhận được thẻ đã phát hành: Ngân hàng gửi thẻ cho chủ thẻ qua đường bưu điện nhưng trên đường vận chuyển thẻ bị đánh cắp và bị sử dụng mà chủ thẻ không hay biết gì về việc thẻ đã được gửi cho mình. Trong trường hợp này, ngân hàng phát hành thẻ phải chịu hoàn toàn phí tổn về những giao dịch được thực hiện.

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 kiểm tra tính xác thực của thông báo đó, thẻ được gửi về địa chỉ mới không phải là địa chỉ của chủ thẻ đích thực, dẫn đến tài khoản của chủ thẻ bị lợi dụng. Việc này sẽ chỉ được phát hiện khi chủ thẻ hỏi ngân hàng phát hành về thẻ mới của mình hoặc khi nhận được sao kê thanh toán nợ cho những khoản mà mình không hề chi tiêu. Rủi ro này thông thường chủ thẻ và ngân hàng phát hành cùng phải chịu.

Sự cố hoạt động: Các phương tiện thanh toán điện tử có thể bị sự cố ngẫu nhiên hoặc bị mất các dữ liệu lưu trên thiết bị, một chức năng nào đó ngừng hoạt động, như chức năng kế toán hoặc chức năng bảo mật, hoặc lỗi trong quá trình truyền tải, xử lý thông tin.

Chủ thẻ mất khả năng thanh toán do những lý do khách quan: Chủ thẻ có thể đã giao dịch bằng thẻ tín dụng, nhưng không may gặp phải rủi ro như bị tai nạn, qua đời, dẫn đến tình trạng mất khả năng thanh toán, với những rủi ro này ngân hàng phát hành thẻ sẽ là đơn vị chịu trách nhiệm.

2.1.5.2 Rủi ro đối với chủ thẻ

Thẻ bị mất cắp, bị 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 sử dụng hoặc thu hồi thẻ. Thẻ này có thể bị các tổ chức tội phạm lợi dụng để in nổi và mã hoá lại thẻ để thực hiện các giao dịch giả mạo. Rủi ro này có thể dẫn đến tổn thất cho cả chủ thẻ và ngân hàng phát hành, thường chiếm tỷ lệ lớn nhất.

Thẻ giả: Đây là loại rủi ro nguy hiểm và khó quản lý vì có liên quan đến nhiều nguồn thông tin và nằm ngoài khả năng kiểm soát của ngân hàng phát hành. Thẻ giả được sử dụng tạo ra các giao dịch giả mạo, gây tổn thất cho các Ngân hàng mà chủ yếu là ngân hàng phát

hành vì theo quy định của Tổ chức thẻ quốc tế, ngân hàng phát hành chịu hoàn toàn trách nhiệm với mọi giao dịch thẻ giả mạo có mã số của ngân hàng phát hành. Tuy nhiên hiện nay, đối với tình trạng thẻ giả, nhiều ngân hàng sẽ đẩy rủi ro về phía khách hàng, đổ lỗi cho khách hàng và khách hàng phải chịu trách nhiệm.

Có nhiều cách để các đối tượng lừa đảo có được thông tin thẻ và làm thẻ giả mạo:

- Thẻ do các tổ chức tội phạm làm giả căn cứ vào các thông tin có được từ các giao dịch thẻ hoặc thông tin của thẻ bị mất cắp. Với các thông tin đã ăn cắp được bọn tội phạm sẽ dùng phôi thẻ trắng cho quét qua máy làm giả thẻ để tạo ra thẻ giả.

Tạo băng từ giả (Skimming):

- Tổ chức tội phạm dùng các thiết bị chuyên dụng thu thập thông tin thẻ trên băng từ của thẻ thật. Sau đó, chúng sử dụng các thiết bị riêng để mã hoá và in tạo các băng từ trên thẻ giả và thực hiện các giao dịch giả mạo. Loại giả mạo dựa vào kỹ thuật cao này rất đang phát triển tại các nước tiên tiến gây ra thiệt hại cho chủ thẻ, ngân hàng phát hành, ngân hàng thanh toán.

- Những tổ chức làm giả thường thuê đám bồi bàn và nhân viên thu ngân tải thông tin trên thẻ của khách hàng khi thanh toán. Sau khi đã lấy được dữ liệu, chiếc máy sẽ lập tức được trả lại cho các ông chủ của nó. Những thông số ăn cắp sẽ được truyền sang dải từ của chiếc thẻ giả và đem đi rút tiền ở chỗ khác. Khi sử dụng, những chi tiết của thẻ thật vẫn sẽ hiển thị qua hệ thống của ngân hàng và vì thế được xác nhận.

Chủ thẻ để lộ thông tin của thẻ, bị đánh cắp thông tin khi thanh toán: Đây là trường hợp thanh toán ở những website kém an toàn hoặc không uy tín, thông tin của chủ thẻ bị lộ hoặc bị ăn cắp bởi website hoặc bởi hacker, sau đó thông tin này được sử dụng để tạo ra thẻ giả đi mua hàng hoặc là để mua hàng trên website. Trong trường hợp này lỗi là do chủ thẻ vì thế chủ thẻ hoàn toàn chịu rủi ro.

2.2 Hệ thống thanh toán bằng ví điện tử

2.2.1 Khái niệm ví điện tử

Dịch vụ Ví điện tử là dịch vụ cung cấp cho khách hàng một tài khoản điện tử định danh do các tổ chức cung ứng dịch vụ tạo lập trên vật mang tin (như chip điện tử, sim điện thoại di động, máy tính...), cho phép lưu giữ một giá trị tiền tệ được đảm bảo bằng giá trị tiền gửi tương đương với số tiền được chuyển từ tài khoản thanh toán của khách hàng tại ngân hàng vào tài khoản đảm bảo thanh toán của tổ chức cung ứng dịch vụ ví điện tử theo tỷ lệ 1:1 và được sử dụng làm phương tiện thanh toán không dùng tiền mặt .[2]

Ví điện tử đơn giản được hiểu là một tài khoản điện tử được kết nối với một hệ thống thanh toán trực tuyến và hệ thống tài khoản ngân hàng, được sử dụng trong thanh toán trực tuyến.

Theo thống kê của Ngân hàng Nhà nước, tính đến giữa tháng 7/2019, có 30 đơn vị cung ứng dịch vụ trung gian thanh toán được cấp phép tại Việt Nam. Đa phần trong đó, tức hơn 27 đơn vị có dịch vụ ví điện tử. Còn lại là các dịch vụ khác như chuyển mạch tài tính, bù trừ điện tử, cổng thanh toán...

[2] Thông tư số 39/2014/TT-NHNN ngày 11 tháng 12 năm 2014 của Thống đốc Ngân hàng Nhà nước Việt Nam hướng dẫn về dịch vụ trung gian thanh toán

Luật Ngân hàng Nhà nước Việt Nam (2010) quy định: Mỗi một tổ chức phát hành ví điện tử chỉ được phát hành 01 (một) ví điện tử cho một tài khoản thanh toán của khách hàng tại một ngân hàng; việc nạp tiền vào ví điện tử, rút tiền ra khỏi ví điện tử của khách hàng phải thực hiện thông qua tài khoản thanh toán của khách hàng tại ngân hàng; nhà cung cấp dịch vụ ví điện tử không được cấp tín dụng cho khách hàng sử dụng ví điện tử, ko được trả lãi trên số dư ví điện tử hoặc bất kỳ hành động nào có thể làm tăng giá trị tiền tệ trên ví điện tử.

Một số ví điện tử trong nước : Ví Ngân lượng (Nganluong.vn), Ví Bảo Kim (Baokim.vn), Ví VnMart (VnMart.vn), Ví VinaPay (Vinapay.com.vn); một số ví di động mới xuất hiện: Ví Airpay, Ví Moca, Ví ZaloPay, Ví Vimo. Trên thế giới, một số ví khá nổi tiếng: Ví Paypal (Paypal.com); Ví Alipay (Alipay.com), Ví Payoneer (Payoneer.com).

2.2.2 Đặc điểm ví điện tử

Ví điện tử có những đặc điểm sau :

(1) Dòng tiền liên thông giữa tài khoản ví và tài khoản ngân hàng

Tiện ích cho phép chuyển đổi một phần hoặc toàn bộ số tiền từ tài khoản ngân hàng sang tài khoản ví điện tử và ngược lại là yêu cầu bắt buột theo luật quy định đối với các tổ chức cung cấp dịch vụ ví điện tử. Trước đây kể từ năm 2014 trở về trước chưa có đặc điểm này, nên một số nhà cung cấp dịch vụ ví điện tử cung cấp khá linh hoạt các cách thức để nạp, rút tiền từ ví điện tử, tuy nhiên kể từ năm 2014 *(theo thông tư 39/2014 – Hướng dẫn về dịch vụ trung gian thanh toán)* thì bắt buộc phải có sự liên thông giữa tài khoản ví và tài khoản thẻ.

(2) Ví điện tử là một dịch vụ nhạy cảm về mặt tài chính, nó sẽ hoạt động như một ngân hàng điện tử

Theo luật quy định, một nhà cung cấp dịch vụ ví điện tử là một tổ chức tín dụng phi ngân hàng. Mà một tổ chức tín dụng : là doanh nghiệp thực hiện một, một số hoặc tất cả các hoạt động ngân hàng. Hoạt động ngân hàng là những nghiệp vụ: Nhận tiền gửi; cấp tín dụng; cung ứng dịch vụ thanh toán qua tài khoản, chính vì vậy ví điện tử hoạt động như một ngân hàng điện tử bao gồm những hoạt động: thanh toán trực tuyến, nhận và chuyển tiền, lưu trữ thông tin bao gồm thông tin cá nhân, thông tin thẻ thanh toán, và tiền điện tử.

Bản thân ví điện tử nó sẽ chịu sự điều chỉnh của luật ngân hàng và các tổ chức tín dụng, để tránh trường hợp nhà cung cấp dịch vụ thanh toán ví điện tử nắm giữ tiền của người mua và người bán.

(3) Ví điện tử đòi hỏi phải được kết nối với một cổng thanh toán trực tuyến

Ví điện tử chỉ là một phương tiện thanh toán giống như những phương tiện thanh toán khác như : thẻ thanh toán, vi thanh toán, séc điện tử,… vì thế nếu mà người bán hàng muốn cung cấp dịch vụ này cho người mua hàng thì đều phải kết nối với một cổng thanh toán trực tuyến hoặc một nhà cung cấp dịch vụ ví điện tử. Bản thân nó không thể tồn tại riêng lẻ và tham gia vào các hoạt động thanh toán trực tuyến.

(4) Thanh toán tạm giữ là phương thức than toán chủ đạo

Thanh toán tạm giữ là hình thức thanh toán an toàn của nhà cung cấp dịch vụ ví điện tử, vì sau khi xác nhận thanh toán (bằng OTP gửi tới điện thoại di động hoặc mật khẩu thanh toán), số tiền thanh toán sẽ bị "treo" (chưa thực sự chuyển sang tài khoản của người bán, người bán không thể rút ra và người mua cũng không dùng số tiền này để thực hiện một giao

dịch khác). Người mua và người bán có một khoảng thời gian (thông thường mặc định là 7 ngày) để thực hiện các giao kèo (như chuyển nhận hàng,....). Trong thời gian tạm giữ, chỉ khi nào người mua nhấn vào nút phê chuẩn - đồng ý chuyển tiền cho người bán thì tiền mới thực sự chuyển đi. Dịch vụ tích hợp ví điện tử bảo vệ an toàn cho khách hàng khỏi các rủi ro và nguy cơ lừa đảo trên Internet vì vậy thanh toán tạm giữ là phương thức thanh toán chủ đạo đối với ví điện tử.

Một số ví điện tử cung cấp hình thức thanh toán tạm giữ: Ngân lượng, Bảo Kim, Paypal, Alipay,…

(5) Chưa có sự liên thông giữa các tài khoản ví điện tử khác hệ thống như tài khoản thẻ

Tài khoản ví điện tử khác biệt so với tài khoản ngân hàng ở chỗ hiện giờ hầu như các hệ thống tài khoản thẻ được liên thông với nhau, do sự liên minh của các hệ thống ngân hàng, nhưng tài khoản ví điện tử không có đặc điểm này.

2.2.3 Phân loại ví điện tử

2.2.3.1 Phân loại theo đối tượng sử dụng

- ✓ **Ví điện tử cá nhân**

Mỗi ví điện tử cá nhân gắn liền duy nhất với một số điện thoại di động, để mua hàng hóa/ dịch vụ trên website của các doanh nghiệp chấp nhận thanh toán, quý khách thực hiện đăng ký ví điện tử cá nhân và nạp tiền cho ví.

Thông thường ví điện tử cá nhân sẽ có chức năng sau:

- Nạp tiền cho ví
- Rút tiền từ ví
- Chuyển khoản giữa các ví trong cùng hệ thống
- Thanh toán đơn hàng
- Xem số dư, lịch sử giao dịch, in sao kê

- ✓ **Ví điện tử của doanh nghiệp**

Mỗi doanh nghiệp tạo ví cũng phải có thông tin cơ bản:

- Có số điện thoại di động để xác thực giao dịch
- Số chứng thực: số đăng ký giấy phép kinh doanh, số giấy đăng ký mã số thuế, số giấy phép đầu tư, số quyết định thành lập.

Ngoài những tính năng thông thường của ví điện tử cá nhân, ví điện tử doanh nghiệp còn có thêm một số tính năng khác dành cho người bán nhằm hỗ trợ doanh nghiệp đẩy mạnh hoạt động bán hàng trực tuyến và rút ngắn quy trình giao nhận hàng hóa, mở thêm tiện ích thanh toán mới cho khách hàng khi mua hàng trên website của doanh nghiệp, tuy không làm thay đổi nghiệp vụ mô hình hiện tại của doanh nghiệp và còn thuận tiện trong việc thanh toán giữa ngân hàng và doanh nghiệp, quay vòng vốn nhanh, giảm chi phí bán hàng, hỗ trợ marketing, theo dõi giao dịch, xử lý đơn hàng – cập nhật tình trạng hóa đơn, vấn tin số dư, in sao kê, quản lý (thêm mới, chỉnh sửa, xóa bỏ ..) cửa hàng, quản lý đơn hàng, khách hàng và lịch sử hóa đơn chưa thanh toán…

2.2.3.2 Phân loại theo nơi mà thông tin được lưu trữ

✓ **Lưu giữ trên máy chủ (server side electronic wallet)**

Đây là loại ví điện tử mà thông tin về tài khoản của khách hàng sẽ được lưu trữ trên máy chủ (có thể là máy chủ của người bán, hoặc máy chủ của nhà cung cấp dịch vụ ví điện tử). Ví dụ như những khách hàng sử dụng ví của Ngân lượng, Bảo kim, Paypal, Momo, Payoo,… Khách hàng sẽ đăng ký tài khoản ví điện tử trên website của nhà cung cấp dịch vụ ví điện tử và những thông tin về tài khoản của khách hàng sẽ được nhà cung cấp dịch vụ quản lý. Đối với loại hình này, thông tin của khách hàng phải được nhà cung cấp hoặc người bán hết sức bảo mật, nếu không thì sẽ gặp rất nhiều nguy hiểm cho khách hàng. Hiện nay hầu hết các ví điện tử ở Việt Nam đều có cơ chế bảo mật cho khách hàng, đều đạt Chứng nhận Bảo mật quốc tế PCI DSS (Payment card industry data sécurity standard) cấp độ nhà cung cấp dịch vụ (Service provider). PCI là tiêu chuẩn bảo mật thông tin cho các tổ chức xử lý thẻ tín dụng từ các chương trình thẻ chính. Tiêu chuẩn PCI được ủy quyền bởi các nhãn hiệu thẻ và được quản lý bởi Hội đồng tiêu chuẩn bảo mật ngành thẻ thanh toán.

✓ **Lưu trữ trên máy khách (Client side electronic wallet)**

Đây là loại ví điện tử mà thông tin về tài khoản của khách hàng sẽ được lưu trữ ở chính máy tính/ thiết bị cá nhân của mình. Đối với loại ví này, yêu cầu là phải tải phần mềm về máy tính của mình, hoặc app về thiết bị điện tử của mình, và người dùng sẽ gặp bất lợi khi phải sử dụng một thiết bị điện tử khác (máy tính khác, thiết bị khác).

Ví dụ: Hình thức ví của Samsung pay và Apple pay ko lưu lại thông tin thanh toán và tài khoản của khách hàng ở trên máy chủ của Samsung hay Apple.

2.2.4 Quy trình thanh toán bằng ví điện tử

Dưới đây là quy trình mua hàng sử dụng ví điện tử của Ngân lượng, với những nhà cung cấp dịch vụ ví khác, quy trình cũng diễn ra tương tự.

- Bước 1: Khách hàng truy cập vào website Nganluong.vn tiến hành đăng ký và tạo tài khoản trên ví điện tử.

- Bước 2: Khách hàng nạp tiền vào tài khoản ví điện tử bằng nhiều cách do nhà cung cấp dịch vụ ví điện tử hỗ trợ.

- Bước 3: Trên các website bán hàng, khách hàng lựa chọn sản phẩm và lựa chọn ngân lượng để thanh toán.

- Bước 4: Khi lựa chọn Ngân lượng để thanh toán, khách hàng sẽ được điều hướng ngay về website Nganluong.vn, trên website khách hàng có quyền lựa chọn hình thức chuyển tiền cho người bán.

Khách hàng có thể thực hiện hai cách thức để tiến hành thanh toán.

C1: Thanh toán ngay, tiền sẽ được chuyển từ tài khoản Ngân Lượng của người mua sang tài khoản Ngân Lượng của người bán, người bán có thể thực hiện rút tiền mặt, hoặc chuyển đổi sang tài khoản ngân hàng nếu muốn.

C2: Thanh toán tạm giữ, tiền thanh toán của khách hàng người mua sẽ được Ngân Lượng tạm giữ và Ngân Lượng phát ra yêu cầu chuyển hàng hóa tới địa chỉ của người mua hàng và thông báo với người bán về sự thanh toán của khách hàng mua.

Đối với C2, sẽ có hai trường hợp xảy ra:

- Khi người mua nhận được hàng và phê chuẩn giao dịch, tiền thanh toán sẽ được

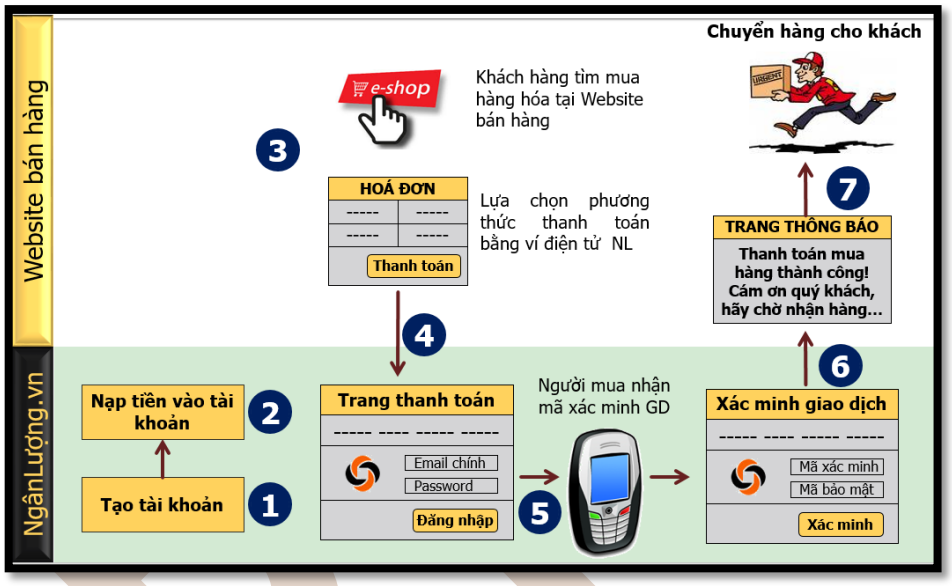
chuyển vào tài khoản ví điện tử của người bán, người bán sẽ có thể chuyển đổi sang tài khoản ngân hàng hoặc rút tiền mặt nếu họ muốn

- Nếu người mua có phàn nàn, khiếu kiện gì về giao dịch, Ngân lượng sẽ đứng ra giải quyết tranh chấp trên cơ sở tôn trọng quyền và lợi ích hợp pháp của các bên.

- Bước 5: Sau khi điền đầy đủ thông tin trên trang thanh toán và lựa chọn hình thức chuyển tiền cho người bán, khách hàng sẽ nhận được mã xác minh giao dịch được Ngân lượng nhắn tin vào điện thoại đi động. Khách hàng sẽ điền nốt mã xác minh và mã bảo mật để hoàn thiện đơn hàng.

- Bước 6: Khách hàng được thông báo là đã mua hàng thành công trên website của người bán.

- Bước 7: Website chuyển hàng cho khách hàng.



Hình 2.5: Quy trình thanh toán ví điện tử Nganluong.vn

2.3 Hệ thống vi thanh toán điện tử

2.3.1 Khái niệm vi thanh toán điện tử

Xuất phát từ nhu cầu của người dùng rất đa dạng, chỉ cần mua một bài hát trong một album do thích mỗi bài hát đó; hay một bài báo trong một quyển tạp chí khoa học; hay một chương trong một cuốn sách,.. tuy nhiên nếu sử dụng những loại hình thanh toán điện tử hiện có thì chi phí cho mỗi giao dịch thanh toán khá cao, thậm chí còn cao hơn cả lợi nhuận của người bán. Xuất phát từ những rào cản về sản phẩm có giá trị nhỏ và hạn chế của những phương thức thanh toán hiện tại nên vi thanh toán ra đời.

Vi thanh toán là một tên gọi chung để chỉ những hệ thống thanh toán cho phép người dùng thanh toán hàng hóa, giao dịch với số lượng tiền là nhỏ. Và tùy vào tổ chức khác nhau, sẽ có những quy định khác nhau. Theo Efraim Turban (2018)[3]: vi thanh toán là hình thức thanh toán cho những giao dịch có giá trị nhỏ hơn 10 đô la Mỹ. Paypal quy ước thì vi thanh toán là hình thức thanh toán cho những giao dịch có giá trị nhỏ hơn 12 đô la Mỹ, Visa thì xác

[3] Efraim Turban (2018), Electronic Commerce 2018 : A Managerial and Social Networks Perspective, Springer International Publishing AG.

định vi thanh toán là hình thức thanh toán cho những giao dịch có giá trị nhỏ hơn đô la Mỹ.

Trong thế giới web, vi thanh toán là một loại hình thanh toán chỉ ra cách thu tiền từ mỗi trang web, mặc dù có nhiều cách thức khác nhau của loại hình vi thanh toán nhưng tựu chung lại có ba mô hình mà các nhà cung cấp dịch vụ vi thanh toán thường dùng đó là mô hình trả trước, mô hình trả sau, và mô hình trả ngay.

Mô hình trả trước: Là mô hình người mua sẽ nạp một khoản tiền nhất định vào tài khoản thanh toán của mình với nhà cung cấp dịch vụ thanh toán / người bán. Thông thường người mua có thể nạp tiền bằng thẻ trả trước và nhập vào mã code đặc biệt ở mặt sau của thẻ trực tuyến để tài khoản của họ được ghi có cho số tiền họ đã thanh toán. Trả trước có thể mang hình thức thuê bao mà người dùng trả trước hàng tháng, hàng năm cho việc truy cập vào nội dung như những bài báo và nội dung cao cấp trong những trò chơi game trực tuyến. Ưu điểm, với mô hình này thanh toán trước một khoản tiền lớn sẽ làm cho giao dịch có giá trị hơn về chi phí xử lý được giải quyết. Hạn chế, người bán cần phải duy trì một hệ thống theo dõi lượng tín dụng mà mỗi người có trong tay; người dùng sẽ trả tiền trước để truy cập vào mọi thứ, cho dù họ muốn hay không.

Mô hình trả sau: Trong mô hình trả sau, thay vì trả tiền trước hoặc thanh toán khi mua hàng, người dùng trả tiền sau khi họ quyết định mua hàng, tương tự như các mô hình mua sắm trực tuyến truyền thống. Trả sau là một giải pháp thay thế hiệu quả để trả tiền khi bạn mua hàng, do các giao dịch vi mô được tổng hợp thay vì được tính riêng lẻ. Điều thường xảy ra là người bán sẽ theo dõi các giao dịch vi mô riêng lẻ của người dùng và sau một khoảng thời gian nhất định mà không có giao dịch nào được thực hiện, hoặc đạt đến một mức giá trị thanh toán nhất định (ví dụ: 100 đô la Mỹ) người bán sẽ tổng hợp các giao dịch mua riêng lẻ và lập hóa đơn cho họ dưới dạng một số tiền. Tương tự như trả trước, trả sau cũng có thể áp dụng mô hình đăng ký nơi người dùng có quyền truy cập không giới hạn vào một số tính năng nhất định và sau đó được lập hóa đơn một khoản phí chuẩn vào cuối tháng. Tuy nhiên, điều này ít phổ biến hơn các mô hình đăng ký trả trước. Ưu điểm, với mô hình này người dùng không cần phải trả trước một khoản tiền lớn hơn để bắt đầu mua hàng nên sẽ yên tâm hơn và thích hơn, không lo bị lãng phí tiền nếu không tiếp tục mua hàng, họ sẽ được mua với hình thức thanh toán trực tiếp cho từng món, nhưng là trả sau. Đối với người bán, việc tổng hợp các khoản thanh toán có thể làm giảm đáng kể số tiền phí giao dịch mà một người bán sẽ trả. Hạn chế, người bán cần tạo hệ thống theo dõi mua hàng và sau đó cố gắng tổng hợp chúng theo cách chu đáo để giảm phí giao dịch. Người dùng có thể chỉ mua một vài mặt hàng có giá trị rất nhỏ (ví dụ một bài hát giá trị 1 đến 2 đô la Mỹ), sau đó không mua bất kỳ thứ gì khác, để lại cho người bán không có lựa chọn nào khác ngoài việc tự xử lý giao dịch vi thanh toán với mức phí cao, gây khó khăn cho người bán.

Mô hình thanh toán ngay: Trong mô hình này**,** người dùng sẽ bị tính phí khi mua hàng mà họ muốn thực hiện. Điều này có nghĩa là ngay sau khi người dùng muốn mua quyền truy cập vào một bài viết hoặc một số hàng hóa ảo khác, thẻ tín dụng của họ sẽ bị tính phí cho số tiền của giao dịch. Ưu điểm, cho phép người dùng chỉ phải trả tiền cho sản phẩm / dịch vụ mà họ mua. Họ chỉ mua những gì họ muốn, và họ trả tiền khi họ muốn. Hạn chế rất lớn cho người bán, và với mô hình này gánh nặng đặt lên người bán.

2.3.2 Đặc điểm vi thanh toán điện tử

2.3.2.1 Đặc điểm kỹ thuật

- ✓ **Dựa trên token hoặc dựa trên tài khoản**

- Đối với loại hình vi thanh toán dựa trên token, nhìn chung, các khách hàng mua token từ một trung gian thanh toán để thanh toán cho những người bán. Sau đó, những người bán gửi token nhận được này tới các trung gian thanh toán để xác thực và thanh toán.

- Đối với hệ thống được xây dựng trên tài khoản, khách hàng và người bán hàng đều có tài khoản tại trung gian thanh toán hoặc ngân hàng, và khách hàng ủy quyền cho trung gian thanh toán chuyển tiền tới tài khoản của người bán.

- ✓ **Tính năng dễ sử dụng, thuận tiện**

Tính dễ sử dụng là việc hệ thống đó phải được thiết kế quy trình thực hiện với những bước đơn giản, dễ sử dụng tạo ra sự dễ dàng và thuận tiện cho người dùng bao gồm người dùng mới, người có kinh nghiệm; liên quan đến giao diện người dùng, phần mềm, phần cứng cơ bản, phải dễ dàng và thuận tiện.

- ✓ **Tính ẩn danh**

Tính ẩn danh ở đây chỉ liên quan tới khách hàng. Người bán/ thương gia thì không bao giờ ẩn danh. Chúng ta phân biệt tính ẩn danh ở đây là ẩn danh đối với người bán hay là đối với những nhà vận hành hệ thống vi thanh toán (MPSOs), khi tiến hành những giao dịch vi thanh toán.

- ✓ **Khả năng mở rộng**

Xác định rằng liệu một hệ thống vi thanh toán có thể để đối phó với sự gia tăng khối lượng thanh toán và cơ sở người dùng mà không làm giảm đáng kể hiệu quả hoạt động hay không.

- ✓ **Tính xác nhận / hợp lệ**

Tính xác nhận hợp lệ tức là xác định xem một hệ thống thanh toán có thể xử lý thanh toán những liên lạc trực tuyến hoặc ngoại tuyến với một bên thứ ba hay không. Xác nhận trực tuyến có nghĩa là một bên tham gia cho mỗi lần thanh toán. Bán trực tuyến có nghĩa là một bên tham gia, nhưng không phải cho mỗi thanh toán, có thể là xác nhận ngẫu nhiên, hay định kỳ. Xác nhận ngoại tuyến có nghĩa là các khoản thanh toán có thể được thực hiện mà không có một bên thứ ba nào tham gia (ví dụ, thanh toán bằng tiền mặt).

- ✓ **Tính an toàn**

Xác định xem liệu hệ thống này có an toàn, bảo mật ko, sử dụng kỹ thuật nào để bảo đảm an toàn.

- ✓ **Khả năng hợp tác (tương tác)**

Khả năng tương tác cho phép người sử dụng của một hệ thống thanh toán trả tiền hoặc được trả tiền bởi người sử dụng của một hệ thống khác. Khả năng cộng tác cũng có nghĩa là khả năng chuyển đổi của tiền tệ. Tiền tệ có khả năng chuyển đổi nếu nó cũng được chấp nhận bởi các hệ thống khác.

2.3.2.2 Đặc điểm phi kỹ thuật

- ✓ **Tính tin cậy / niềm tin**

Xác định sự tin cậy của người sử dụng đối với hệ thống vi thanh toán và người điều khiển của nó.

✓ **Độ bao phủ**

Được đưa ra thể hiện tỷ lệ phần trăm (hoặc số lượng) của các thương nhân và khách hàng có thể sử dụng hệ thống vi thanh toán.

✓ **Tính bảo mật/ riêng tư**

Liên quan đến việc bảo vệ cá nhân và những thông tin thanh toán. Một hệ thống thanh toán cung cấp sự bảo vệ sự riêng tư tùy thuộc vào các loại thông tin.

✓ **Hệ thống trả trước hoặc sau**

Xác định làm thế nào để khách hàng sử dụng được hệ thống vi thanh toán này. Hệ thống trả trước yêu cầu khách hàng chuyển tiền vào hệ thống trước khi họ có thể bắt đầu thanh toán. Hệ thống trả sau cho phép khách hàng bắt đầu thanh toán trước và trả tiền sau.

✓ **Phạm vi thanh toán và hỗ trợ nhiều đơn vị tiền tệ**

Phạm vi của các khoản thanh toán và hỗ trợ các đơn vị tiền tệ xác định các giá trị thanh toán tối thiểu và tối đa được hỗ trợ bởi một hệ thống, và xác định xem một hệ thống có hỗ trợ nhiều loại tiền tệ hay không.

2.3.3 Phân loại các loại hình của vi thanh toán

2.3.3.1 Vi thanh toán dựa trên token

✓ **Khái niệm**

Vi thanh toán dựa trên token là hình thức vi thanh toán trong đó khách hàng người mua sẽ tiến hành mua token từ nhà cung cấp dịch vụ vi thanh toán và sử dụng token này để thanh toán cho hàng hóa, dịch vụ giá trị nhỏ. Người bán sau khi nhận được token sẽ lập tức gửi ngược lại nhà cung cấp dịch vụ vi thanh toán để kiểm tra tính hợp lệ của token và xác thực thanh toán.

✓ **Các loại hình của vi thanh toán dựa trên token**

Thanh toán qua điện thoại (Phone billing)

Đây là loại hình vi thanh toán mà hóa đơn mua hàng của khách hàng sẽ được trừ vào tài khoản điện thoại, có thể là tài khoản trả trước hoặc trả sau.

Một ví dụ của hình thức này là dịch vụ m-Pay Bill của Vodafone / T-Mobile sử dụng để giao dịch những khoản tiền nhỏ. Nó cho phép tính phí vào hóa đơn điện thoại hoặc để ghi nợ vào một khoản tín dụng trả trước.

Thanh toán qua SMS (SMS premium)

Đây là hình thức mà tiền mua hàng hóa dịch vụ của khách hàng được thanh toán thông qua tin nhắn SMS.

Ví dụ của hình thức này là hệ thống Coinlet của Portalify của Phần Lan cung cấp hoạt động thanh toán qua tin nhắn SMS (SMS premium) và giọng nói (voice). Các hệ thống thanh toán như vậy vẫn chưa được cung cấp rộng rãi và thường không được thừa nhận trong thanh toán quốc tế.

- **Thanh toán qua đàm thoại (Voice pay)**

Đây là hình thức thanh toán mà khách hàng sẽ gọi điện đến tổng đài để yêu cầu mã truy cập, và sau đó sử dụng mã này để tiến hành thanh toán. Ví dụ: hipaymobile.com là website cung cấp dịch vụ này.

- Thanh toán bằng thẻ trả trước (Prepaid card)

Đây là hình thức thanh toán bằng cách mua một thẻ trả trước. Thẻ này có nhiều hình thức khác nhau do thiết lập của nhà cung cấp. Thông thường, thẻ chỉ được sử dụng một lần và không chứa thông tin nào khác ngoài mã PIN, số được che giấu dưới lớp giấy bạc.

Hệ thống trả trước cũng có tiềm năng phát triển cho hình thức vi thanh toán ví dụ: như Paysafecard Micromoney ở Đức, New Zealand với Payex cũng đã phát triển các loại công cụ này. Tuy nhiên, không có cơ chế thanh toán nào được áp dụng rộng rãi.

2.3.3.2 Vi thanh toán dựa trên tài khoản

Vi thanh toán dựa trên tài khoản là loại hình vi thanh toán đòi hỏi người bán và người mua thiết lập tài khoản nhà cung cấp dịch vụ vi thanh toán, loại hình thanh toán này có cách thức vận hành như ví điện tử, người mua ủy quyền cho nhà cung cấp dịch vụ vi thanh toán để chuyển tiền vào tài khoản của người bán.

2.3.4 Quy trình thực hiện vi thanh toán điện tử

2.3.4.1 Thanh toán qua điện thoại (Phone billing micropayment)

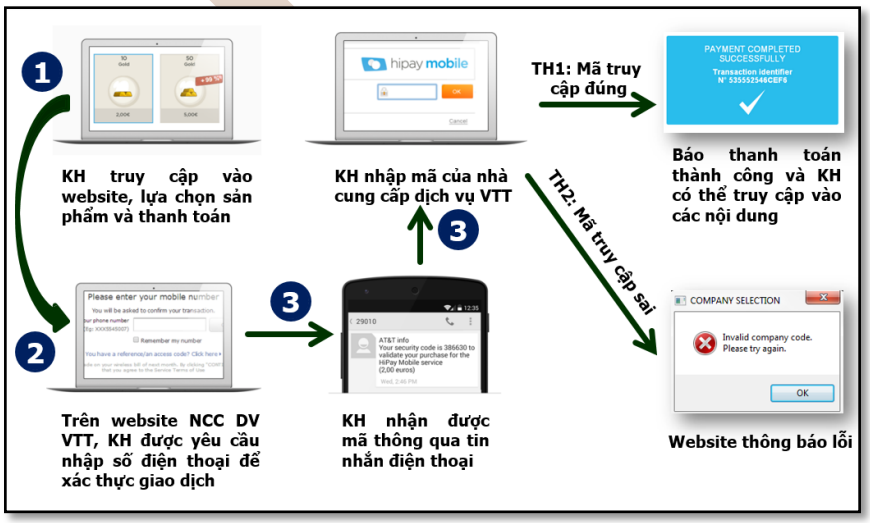
- Bước 1: Khách hàng truy cập vào website của người bán, lựa chọn sản phẩm và lựa chọn phương thức thanh toán Phone billing.

- Bước 2: Khách hàng sẽ được điều hướng về website của nhà cung cấp dịch vụ thanh toán. Trên website này, khách hàng được yêu cầu nhập số điện thoại vào để xác thực giao dịch.

- Bước 3: Khách hàng sẽ nhận được mã thông qua tin nhắn điện thoại, sau đó khách hàng sẽ điền vào để thanh toán.

+ Trường hợp 1: Nếu mã truy cập đúng, khách hàng sẽ thanh toán xong cho sản phẩm giá trị nhỏ mà mình đã lựa chọn

+ Trường hợp 2: Nếu mã truy cập sai, khách hàng sẽ được hướng tới một website thông báo lỗi.



Hình 2.6: Quy trình vi thanh toán dựa trên Phone billing

2.3.4.2 SMS premium – Thanh toán bằng tin nhắn

Hình thức thanh toán thông qua SMS tương tự như việc trả tiền thông qua việc nhắn tin đến tổng đài.

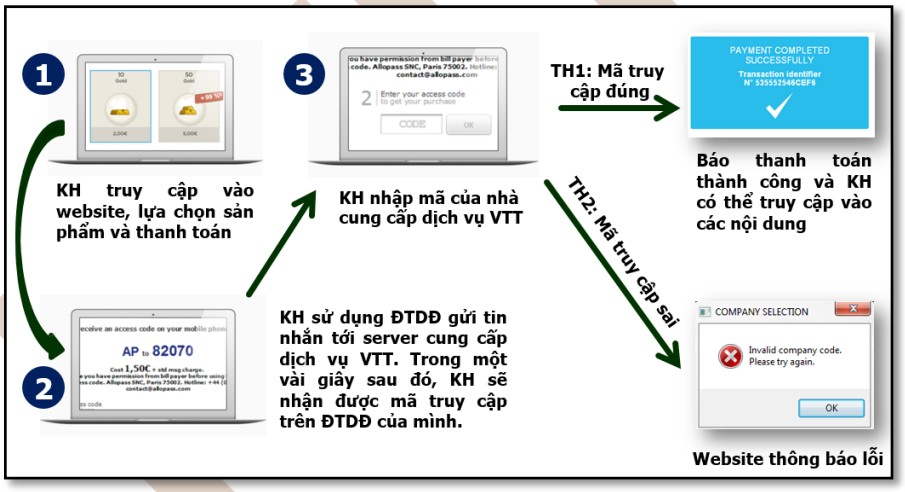
- Bước 1: Trên các website bán hàng hóa – dịch vụ giá trị nhỏ, khách hàng lựa chọn sản phẩm và lựa chọn phương thức thanh toán cho sản phẩm mình lựa chọn.

- Bước 2: Khách hàng người mua sử dụng điện thoại di động soạn tin nhắn theo mẫu và gửi tới tổng đài của nhà cung cấp dịch vụ thanh toán để nhận được mã truy cập trên điện thoại di động của mình.

- Bước 3: Khách hàng sẽ nhập mã của nhà cung cấp dịch vụ vi thanh toán. Thông tin về mã truy cập sẽ được truyền tải tới máy chủ của nhà cung cấp dịch vụ vi thanh toán.

+ Trường hợp 1: Nếu mã truy cập đúng, khách hàng sẽ thanh toán xong cho sản phẩm giá trị nhỏ mà mình đã lựa chọn.

+ Trường hợp 2: Nếu mã truy cập sai, khách hàng sẽ được hướng tới một website thông báo lỗi.



Hình 2.7: Quy trình vi thanh toán qua tin nhắn SMS

2.3.4.3 Thanh toán bằng đàm thoại (IVR - Interactive voice response)

- Bước 1: Trên các website bán hàng hóa – dịch vụ giá trị nhỏ, khách hàng lựa chọn sản phẩm và lựa chọn phương thức thanh toán cho sản phẩm mình lựa chọn.

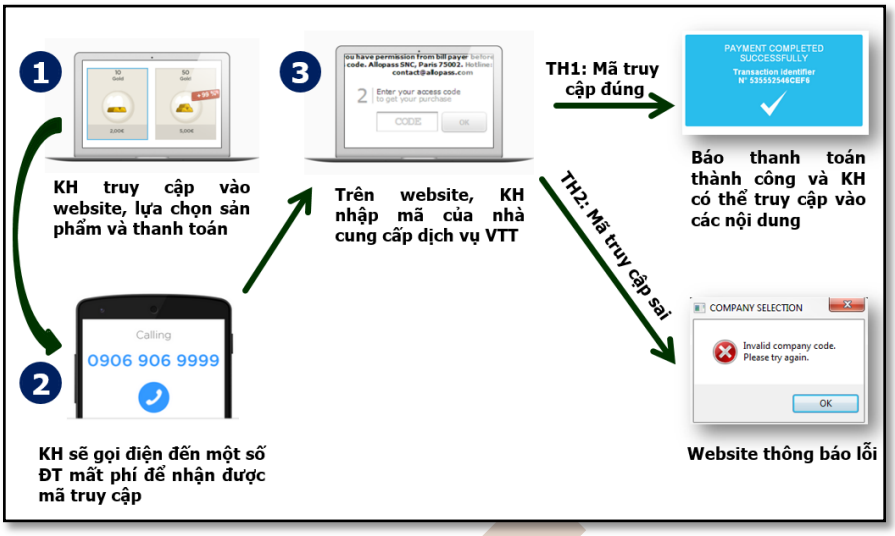
- Bước 2: Khách hàng người mua sử dụng số điện thoại gọi điện đến một tổng đài được yêu cầu để nhận được mã truy cập (thông thường sẽ mất phí để nhận được mã truy cập)

- Bước 3: Khách hàng nhập mã truy cập nhận được vào ô xác thực trên website để tiến hành thanh toán. Mã truy cập nhận được sẽ được truyền tải đến máy chủ của nhà cung cấp dịch vụ vi thanh toán.

+ Trường hợp 1: Nếu mã truy cập đúng, khách hàng sẽ thanh toán xong cho sản phẩm mình lựa chọn.

+ Trường hợp 2: Nếu mã truy cập sai, khách hàng sẽ được hướng tới một web thông

báo lỗi.



Hình 2.8: Quy trình vi thanh toán dựa trên đàm thoại

2.3.4.4 Thanh toán bằng thẻ trả trước (Prepaid card)

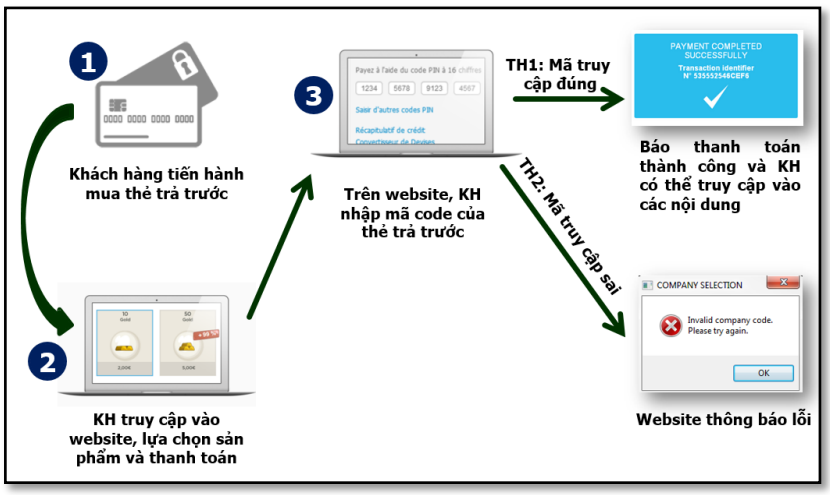
- Bước 1: Khách hàng tiến hành mua thẻ trả trước. Thẻ trả trước chỉ là một thẻ không chứa thông tin nào khác ngoài mã PIN số được che giấu dưới lớp giấy bạc, thông thường gồm 16 ký tự. Khách hàng hoàn toàn có thể sử dụng số dư còn lại trong thẻ, nếu lần thanh toán trước không sử dụng hết. Khách hàng có thể mua thẻ trả trước ở trên web thông qua những phương thức thanh toán khác, và sẽ được gửi về một mã code thông qua email hoặc điện thoại.

- Bước 2: Khách hàng truy cập vào website của người bán, lựa chọn sản phẩm và lựa chọn phương thức thanh toán Prepaid card.

- Bước 3: Khách hàng sẽ được điều hướng về website của nhà cung cấp dịch vụ thanh toán. Trên website này, khách hàng sẽ tiếp tục tiến hành điền mã số trên thẻ trả trước và tiến hành thanh toán.

+ Trường hợp 1: Nếu mã thẻ mà đúng, khách hàng sẽ thanh toán xong cho sản phẩm giá trị nhỏ mà mình đã lựa chọn.

+ Trường hợp 2: Nếu mã truy cập sai, khách hàng sẽ được hướng tới một website thông báo lỗi.



Hình 2.9: Quy trình vi thanh toán bằng thẻ trả trước

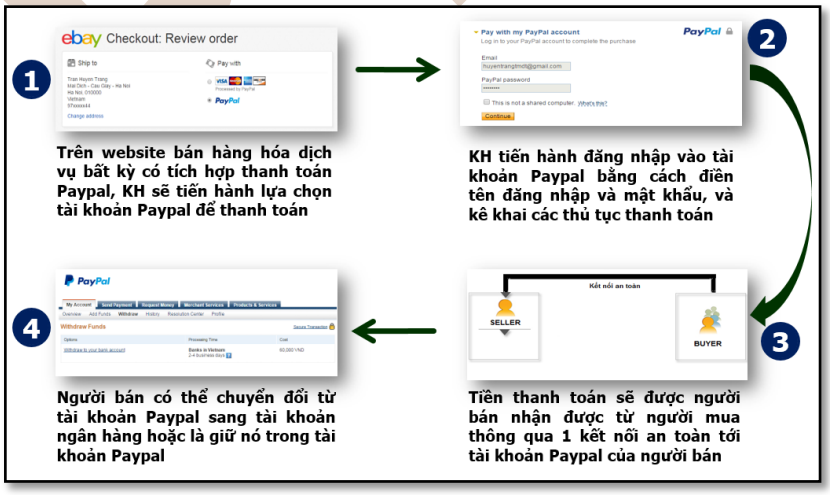
2.3.4.5 Quy trình thanh toán dựa trên tài khoản Paypal

- Bước 1: Trên website bán hàng hóa dịch vụ bất kỳ có tích hợp thanh toán Paypal, khách hàng tiến hành lựa chọn tài khoản Paypal để thanh toán.

- Bước 2: Khách hàng tiến hành đăng nhập vào tài khoản Paypal bằng cách điền tên đăng nhập và mật khẩu, và kê khai các thủ tục thanh toán. (Hoặc khi lựa chọn tài khoản Paypal để thanh toán, người mua có thể thanh toán với thẻ tín dụng, thẻ ghi nợ, tài khoản ngân hàng hoặc sử dụng số dư của tài khoản Paypal).

- Bước 3: Tiền thanh toán sẽ được người bán nhận được từ người mua thông qua một kết nối an toàn tới tài khoản Paypal của người bán.

- Bước 4: Người bán có thể chuyển đổi từ tài khoản Paypal sang tài khoản ngân hàng và thực hiện rút tiền mặt nếu muốn hoặc là giữ nó trong tài khoản Paypal.



Hình 2.10: Quy trình vi thanh toán dựa trên tài khoản

2.4 Hệ thống thanh toán bằng chuyển khoản điện tử

Chuyển khoản điện tử (Electronic funds transfer) là hệ thống thanh toán điện tử lâu đời nhất, ra đời sớm nhất mặc dù lúc đầu mới chỉ là chuyển khoản nội bộ. Trước đây thì chúng ta chuyển khoản ở ngân hàng, ở thiết bị ATM, và hiện giờ với công nghệ mới phát triển

thì chúng ta sẽ chuyển tiền thông qua website của ngân hàng.

2.4.1 Chuyển khoản cùng hệ thống

✓ **Khái niệm**

Chuyển khoản điện tử cùng hệ thống (thanh toán điện tử nội bộ) là nghiệp vụ chuyển tiền thanh toán giữa hai hoặc nhiều chi nhánh của cùng một ngân hàng. Việc thanh toán không có sự chuyển dịch của dòng tiền vật lý và tổng nguồn vốn ngân hàng trước và sau khi thanh toán là không đổi.

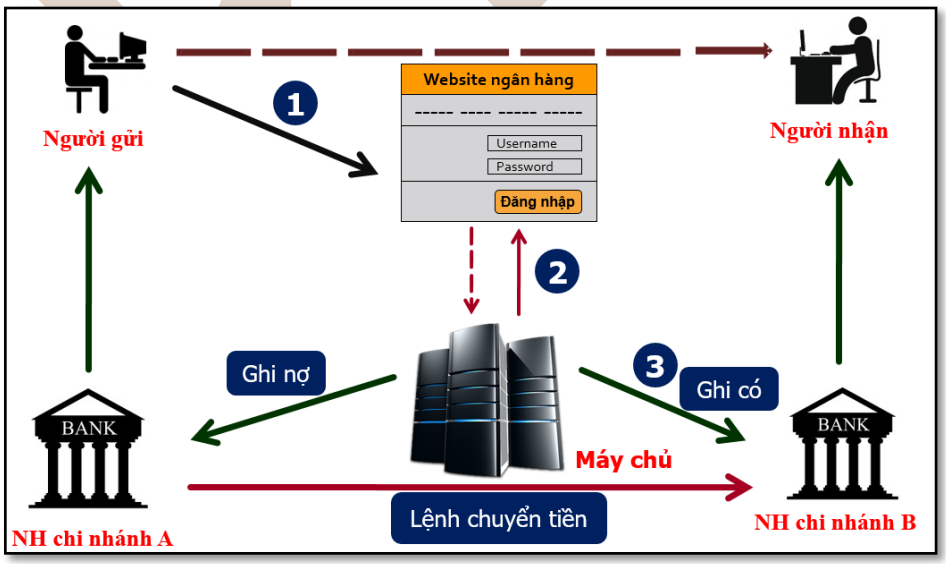
✓ **Quy trình chuyển khoản điện tử cùng hệ thống**

- Bước 1: Khách hàng (người chuyển tiền) tại chi nhánh A muốn chuyển một khoản tiền sang chi nhánh B của ngân hàng X thì việc đầu tiên là người chuyển tiền sẽ đăng nhập vào hệ thống ngân hàng điện tử bằng tên đăng nhập (user) và mật khẩu (pass) của mình, điền vào mẫu yêu cầu chuyển khoản được cung cấp trên website của ngân hàng X.

- Bước 2: Máy chủ xử lý giao dịch của ngân hàng X sẽ kiểm tra tính đúng đắn của thông tin trên mẫu đơn mà người chuyển tiền khai báo sau đó xác thực việc thanh toán chuyển khoản. Máy chủ sẽ thực hiện lệnh chuyển một số tiền bằng đúng với số tiền yêu cầu chuyển khoản từ tài khoản ngân hàng của người chuyển tiền tại chi nhánh A sang tài khoản ngân hàng của người thụ hưởng tại chi nhánh B.

- Bước 3: Máy chủ xử lý giao dịch gửi thông điệp báo về phát sinh Nợ, Có trong tài khoản của người chuyển tiền và tài khoản của người thụ hưởng. Đối với người chuyển tiền, ngân hàng gửi thông báo phát sinh nợ đúng bằng số tiền chuyển, cả số dư có của tài khoản và nội dung của quá trình thanh toán. Đối với người thụ hưởng, ngân hàng gửi thông báo phát sinh có, số dư có của tài khoản và nội dung của quá trình thanh toán.

Tuy chuyển khoản ở chi nhánh khác nhau nhưng đều diễn ra trong cùng một máy chủ nên thời gian diễn ra rất nhanh.



Hình 2.11: Quy trình chuyển khoản cùng hệ thống

2.4.2 Chuyển khoản khác hệ thống

✓ **Khái niệm**

Chuyển khoản điện tử khác hệ thống là nghiệp vụ chuyển tiền thanh toán giữa hai hoặc nhiều ngân hàng thương mại khác hệ thống (trong cùng địa bàn hoặc khác địa bàn). Việc thanh toán sẽ có sự chuyển dịch dòng tiền vật lý và nguồn vốn từ ngân hàng này sang ngân hàng khác.

✓ **Quy trình chuyển khoản điện tử khác hệ thống**

- Bước 1: Người gửi thực hiện lệnh chuyển khoản bằng cách truy cập vào ngân hàng trực tuyến của mình và điền vào mẫu đơn chuyển khoản.

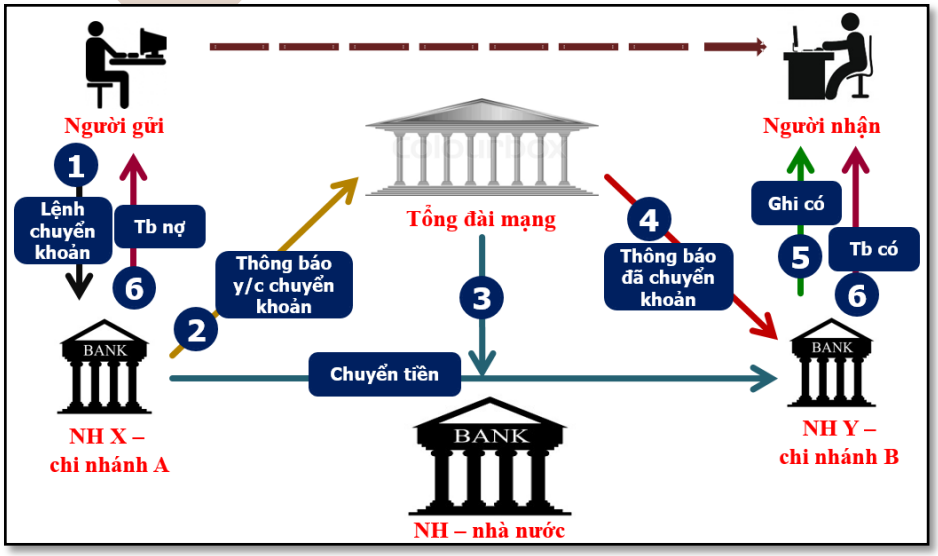
- Bước 2: Máy chủ xử lý giao dịch ngân hàng trực tuyến của người gửi sẽ kiểm tra tính đúng đắn của thông tin trên mẫu đơn chuyển khoản mà người gửi khai báo, sau đó gửi thông báo yêu cầu chuyển khoản lên tổng đài mạng chuyển khoản.

- Bước 3: Tổng đài mạng chuyển khoản sau khi nhận được yêu cầu chuyển khoản của ngân hàng vừa gửi sẽ yêu cầu ngân hàng thứ ba (ngân hàng trung ương / ngân hàng nhà nước) đứng ra chịu trách nhiệm thanh toán bù trừ. Cụ thể: Trích từ tài khoản tiền gửi của người gửi tại ngân hàng trung ương / ngân hàng nhà nước một số tiền bằng đúng với số tiền được yêu cầu trong lệnh chuyển khoản để chuyển sang tài khoản tiền gửi của ngân hàng người nhận (cùng được mở ở Ngân hàng Nhà nước).

- Bước 4: Tổng đài mạng chuyển khoản sau khi nhận được thông báo đã chuyển khoản của ngân hàng nhà nước, thì sẽ gửi thông báo về việc đã chuyển khoản tới ngân hàng của người nhận.

- Bước 5: Ngân hàng của người nhận sau khi nhận được thông báo về phát sinh có trong tài khoản tiền gửi của mình tại ngân hàng nhà nước cùng với thông tin chi tiết về giao dịch chuyển khoản sẽ lập tức ghi có vào trong tài khoản của người nhận một số tiền bằng đúng số tiền đã nhận được trong phát sinh có trên tài khoản tiền gửi của mình.

- Bước 6: Ngân hàng của người nhận gửi thông báo phát sinh có trong tài khoản tới người nhận và ngân hàng của người gửi sẽ gửi thông báo về phát sinh nợ trong tại khoản tiền gửi của người gửi.



Hình 2.12: Quy trình chuyển khoản khác hệ thống

2.5 Hệ thống thanh toán séc điện tử

2.5.1 Khái niệm séc điện tử

Séc là một tờ mệnh lệnh vô điều kiện của người chủ tài khoản ra lệnh cho ngân hàng trích từ tài khoản của mình để trả cho *người có tên trong séc* (payee), hoặc trả theo lệnh của người ấy hoặc trả cho *người cầm séc* (bearer) một số tiền nhất định bằng tiền mặt hay chuyển khoản.

Phương thức thanh toán bằng séc cũng chiếm tới gần 10% tổng các giao dịch trực tuyến trên thế giới. Tuy phương thức này trước đây khá phức tạp (sau khi giao dịch trực tuyến được thực hiện, người mua phải ra khỏi mạng và gửi séc qua thư đến cho người bán), tuy nhiên nhiều khách hàng vẫn sẵn sàng chấp nhận sự phức tạp đó để được thực hiện thanh toán bằng séc. Để thoả mãn mong muốn đó của khách hàng, một giải pháp mới cho phương thức thanh toán bằng séc ra đời, đó là việc sử dụng "séc điện tử".

Séc điện tử là phiên bản điện tử có giá trị pháp lý đại diện cho một tấm séc giấy. Séc điện tử là cơ chế thanh toán điện tử đầu tiên được kho bạc Mỹ lựa chọn để tiến hành các khoản thanh toán có giá trị lớn trên mạng Internet.

Về mặt nguyên tắc, hệ thống thanh toán séc điện tử được xây dựng trên các nguyên tắc của hệ thống thanh toán séc giấy, tuy nhiên được điện tử hóa toàn bộ quy trình thanh toán. Hiện nay có rất nhiều tổ chức cung cấp dịch vụ thanh toán séc điện tử: Authorize.net, Paysimple.com, Checkpay.us. Ở một số quốc gia phát triển, người ta hay đồng nhất các thuật ngữ: electronic checks, direct debit, or ACH transfer. Từ năm 2015, séc điện tử được coi là một hình thức thanh toán tiêu chuẩn, cùng với thẻ tín dụng hoặc những công cụ thanh toán của bên thứ ba.

Tại Việt Nam, hình thức thanh toán bằng séc truyền thống chỉ chiếm khoảng 2% trong tổng thanh toán phi tiền mặt, trong đó chủ yếu là thanh toán giữa các doanh nghiệp. Hầu hết người dân vẫn e ngại thanh toán bằng séc, và tính đến thời điểm hiện tại cũng chưa có tổ chức nào cung cấp dịch vụ thanh toán séc điện tử.

Thanh toán bằng séc điện tử có rất nhiều lợi ích:

- Người bán cắt giảm được chi phí quản lý

- Người bán nhận được tiền từ người mua nhanh hơn, an toàn hơn và không mất thời gian xử lý giấy tờ

- Cải tiến hiệu quả quy trình chuyển tiền đối với cả người bán và tổ chức tài chính

- Cung cấp thông tin chi tiết về việc mua hàng trên tài khoản của người mua

- Không yêu cầu khách hàng tiết lộ các thông tin về tài khoản của mình cho các nhân khác trong quá trình giao dịch

- Không yêu cầu khách hàng phải thường xuyên gửi các thông tin tài chính nhạy cảm trên web

- Tiết kiệm so với thanh toán bằng thẻ tín dụng cho người bán

- Nhanh và tiện lợi hơn so với séc giấy.

2.5.2 Đặc điểm séc điện tử

- ✓ **Đặc điểm của séc là có tính thời hạn như séc giấy**

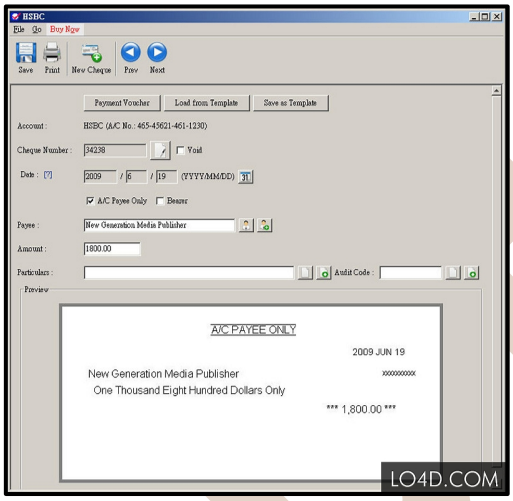
- Giống hệt séc giấy, chỉ có giá trị trong khoảng thời gian nhất định, được ghi rõ trên séc, quá thời gian này, séc hoàn toàn mất hiệu lực.

- Thời hạn của tấm séc sẽ tuỳ thuộc vào: loại séc, phạm vi không gian mà séc lưu hành và luật pháp các nước quy định.

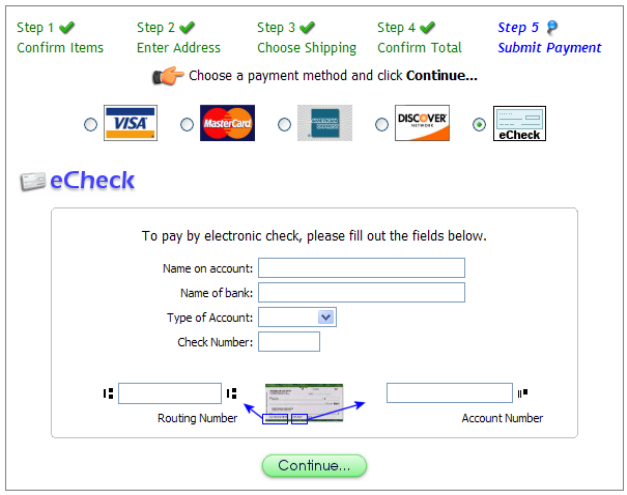
✓ **Chứa đựng thông tin giống séc giấy và dựa trên cùng một khung pháp lý như séc giấy**

Vì séc điện tử là phiên bản điện tử của séc giấy, nên thông tin cung cấp trên séc điện tử cũng tương tự như séc giấy. Khi thanh toán bằng séc điện tử, số tiền ghi trên séc phải rõ ràng, phải vừa ghi bằng số và vừa ghi bằng chữ khớp đúng nhau, có ký hiệu tiền tệ.

Trên séc phải ghi rõ thông tin: Số tài khoản của người mua hàng, 9 ký tự để phân biệt ngân hàng ở cuối tấm séc – số hiệu ngân hàng (đối với séc ở Mỹ), loại tài khoản ngân hàng cá nhân hoặc doanh nghiệp, tên chủ tài khoản, số tiền thanh toán.



Hình 2.13a: Séc điện tử theo phương pháp Print and Pay



Hình 2.13b: Séc điện tử theo phương thức thanh toán trực tuyến

✓ **Có thể kết nối thông tin không giới hạn và trao đổi trực tiếp giữa các bên (giống với các hệ thống khác)**

Có nghĩa có thể kết nối và liên thông giữa các hệ thống tài khoản séc với nhau, hay là giữa tài khoản séc với tài khoản thẻ.

✓ **Séc được viết (khai báo) và chuyển giao cho người nhận bằng cách sử dụng các phương tiện điện tử (chủ yếu là qua mạng máy tính có kết nối Internet)**

Trong thực tế hoạt động, séc điện tử chủ yếu được thực hiện thông qua mạng máy tính có kết nối Internet, qua các phương tiện điện tử khác rất hạn chế. Hầu hết các doanh nghiệp đều dựa vào nhà cung cấp dịch vụ thanh toán của bên thứ ba để thực hiện thanh toán séc điện tử. Có nhiều nhà cung cấp dịch vụ séc điện tử nổi tiếng: Authorize.net; Paysimple.com, Checkpay.us,…

2.5.3 Một số loại hình thanh toán séc điện tử

eCheck.Net là dịch vụ thanh toán của Authorize.Net cho phép người bán chấp nhận

thanh toán bằng séc điện tử cho hàng hóa và dịch vụ được mua qua một số phương pháp, bao gồm đặt hàng qua thư/ đặt hàng qua điện thoại và trang web TMĐT. Nó cũng cho phép người bán thu thập séc giấy và chuyển đổi chúng thành séc điện tử.

2.5.3.1 Chuyển đổi tài khoản phải thu (ARC:Accounts Receivable Conversion)

ARC là hình thức thanh toán séc điện tử xuất hiện từ năm 2002. ARC là một khoản ghi nợ đơn lẻ đối với tài khoản séc của khách hàng (cá nhân, doanh nghiệp). ARC cho phép người bán thu thập các khoản thanh toán nhận được qua thư (bưu điện Hoa Kỳ) hoặc để lại trong hộp thả xuống (drop-box) và chuyển đổi chúng sang thanh toán điện tử sau đó.

Drop box là hình thức mà người bán sẽ để lại séc trong hộp thả riêng biệt ở quầy hàng thanh toán. Đối với hình thức này, nhân viên của cửa hàng sẽ tập hợp séc tại một thời điểm thích hợp, điều đó sẽ tiết kiệm thời gian và giảm chi phí liên quan đến nhân lực đối với việc xử lý và chấp nhận séc. Tuy nhiên khách hàng gặp rủi ro rất lớn trong việc gửi séc vào hộp thả séc, vì khách hàng không có bất kỳ bằng chứng tài liệu nào về việc nộp séc cho ngân hàng, anh ta cũng không thể hỏi nhân viên cửa hàng về việc mất séc hoặc xuất trình séc một cách chậm trễ.

Hình 2.14: Hộp thả (drop-box)

Đối với hình thức ARC, người bán phải sử dụng thiết bị đọc séc để nắm bắt dòng MICR (Magnetic ink character recognition - số định tuyến, số tài khoản và số sê-ri của séc), tuy nhiên cũng có thể nhập số tiền giao dịch theo cách thủ công. Người bán sẽ không trả lại séc cho khách hàng và cũng không xuất trình séc giấy cho ngân hàng để thanh toán mà chuyển đổi tấm séc thông qua thiết bị đọc séc. Sau khi xử lý séc xong, người bán sẽ phải hủy séc trong 14 ngày theo quy định kể từ ngày thanh toán và chỉ được lưu bản sao hoặc hình ảnh của tấm séc trong thời gian 2 năm theo quy định của ngân hàng.

Hình 2.15: Thiết bị đọc séc và nhận dạng MIRC

2.5.3.2 Chuyển đổi trở lại văn phòng (BOC: Back office conversion)

BOC là hình thức thanh toán séc điện tử xuất hiện từ năm 2007, ra đời sau hình thức ARC. BOC là giao dịch đơn lẻ đối với tài khoản séc của khách hàng (cá nhân hoặc doanh nghiệp). BOC cho phép các thương gia thu thập séc viết tại một điểm bán hàng có người kiểm soát (hoặc bộ phận thanh toán nơi có người xử lý) và chuyển nó sang một khoản nợ ACH trong quá trình xử lý văn phòng.

Cách thức xử lý séc theo hình thức BOC cũng tương tự như ARC, người bán phải sử dụng thiết bị đọc séc để kiểm tra và chuyển đổi tấm séc sang dạng điện tử. Người bán sẽ không trả lại séc cho khách hàng và cũng không xuất trình séc giấy cho ngân hàng để thanh toán mà chuyển đổi tấm séc thông qua thiết bị đọc séc. Sau khi xử lý séc xong, người bán sẽ phải hủy séc trong 14 ngày theo quy định kể từ ngày thanh toán và chỉ được lưu bản sao hoặc hình ảnh của tấm séc trong thời gian 2 năm theo quy định của ngân hàng.

2.5.3.3 Tiền mặt tập trung hoặc giải ngân (CCD: Cash concentration or disbursement)

CCD là một giao dịch tính phí hoặc tín dụng đối với tài khoản séc kinh doanh của khách hàng. Các giao dịch CCD có thể diễn ra một lần hoặc định kỳ thường là các khoản chuyển tiền tới hoặc từ các doanh nghiệp hoặc thực thể của doanh nghiệp. Các giao dịch CCD sẽ do một doanh nghiệp/ tổ chức khởi xướng sang một tài khoản thương mại khác để hợp nhất các khoản tiền hoặc để thanh toán tín dụng cho một văn phòng chi nhánh, đối tác thương mại, nhà cung cấp.

CCD sử dụng để thực hiện thanh toán giao dịch qua mạng ACH (biên nhận đơn, thanh toán đơn….) cho doanh nghiệp/ tổ chức.

2.5.3.4. Tiền thanh toán trước và đặt cọc (PPD: Prearranged payment and deposit entry)

Các giao dịch PPD là các khoản ghi nợ và tín dụng do một tổ chức khởi xướng đối với tài khoản séc cá nhân hoặc tiết kiệm của khách hàng. Tất cả các giao dịch tín dụng cho các tài khoản ngân hàng cá nhân phải được nộp như PPD.

PPD sử dụng để thực hiện thanh toán giao dịch qua mạng ACH (biên nhận đơn, thanh toán đơn….) cho cá nhân. Các giao dịch PPD chỉ có thể bắt đầu khi các điều khoản thanh toán và ký quỹ giữa thương gia và khách hàng được sắp đặt trước và bằng văn bản, tức là có sự thỏa thuận từ trước.

2.5.3.5 Thanh toán qua điện thoại (TEL: Telephone-Initiated Entry)

TEL là giao dịch tính phí một lần hoặc định kỳ đối với tài khoản séc cá nhân hoặc tiết kiệm cá nhân của khách hàng. Các giao dịch TEL chỉ có thể bắt đầu thực hiện khi có một mối quan hệ giữa thương gia và khách hàng đã tồn tại từ trước đó (trong khoảng 2 năm trở lại). Hoặc nếu không có mối quan hệ nào tồn tại từ trước, thì khách hàng phải gọi điện thoại cho thương gia để tạo dựng "mối quan hệ kinh doanh" bằng văn bản.

2.5.3.6 Thanh toán qua WEB(Internet Initiated / Mobile Entries)

WEB là một giao dịch tính phí đối một lần hoặc định kỳ với tài khoản séc cá nhân hoặc tài khoản tiết kiệm cá nhân của khách hàng. Các giao dịch WEB có thể được bắt nguồn từ Internet hoặc một thiết bị di động trên mạng không dây.

Các thương gia có trách nhiệm ngăn ngừa các giao dịch có khả năng gian lận bằng cách đảm bảo rằng các giao dịch WEB được nhận từ các khách hàng có chứng thực được xác thực, cho dù đó là một mã PIN tại thời điểm thanh toán hoặc một số phương tiện khác theo yêu cầu của thương gia.

Để làm rõ hơn về các loại hình thanh toán của séc điện tử, bảng 2.1 dưới đây sẽ so sánh về các loại hình bao gồm: đối tượng người dùng, cách hoạt động, loại giao dịch.

Bảng 2.1 : So sánh các loại hình séc điện tử

	ARC	BOC	CCD	PPD	TEL	WEB
Đối tượng	Tài khoản séc doanh nghiệp và cá nhân	Tài khoản séc doanh nghiệp và cá nhân	Tài khoản séc doanh nghiệp	Tài khoản séc cá nhân	Tài khoản séc cá nhân	Tài khoản séc cá nhân
Cách hoạt động	Gửi séc qua thư (thư tín bưu điện) hoặc hộp thả (drop box)	Gửi séc tại quầy thanh toán	Giao dịch tự động (auto pay)	Giao dịch tự động (auto pay)	Giao dịch thông qua điện thoại (sử dụng IVR payments)	Giao dịch thông qua Internet
Loại giao dịch	Giao dịch một lần	Giao dịch một lần	Giao dịch một lần hoặc định kỳ	Giao dịch một lần hoặc định kỳ	Giao dịch một lần hoặc định kỳ	Giao dịch một lần hoặc định kỳ

2.5.4 Quy trình thanh toán bằng séc điện tử

2.5.4.1 Quy trình thanh toán séc điện tử Authorize.net

- Bước 1: Khách hàng người mua sẽ tiến hành truy cập vào website bán hàng, lựa chọn số lượng và chủng loại sản phẩm, lựa chọn hình thức thanh toán séc điện tử để tiến hành thanh toán.

- Bước 2: Khách hàng người mua sẽ được truy cập thông qua mọt kết nối an toàn đến website của nhà thanh toán điện tử Authorize.net.

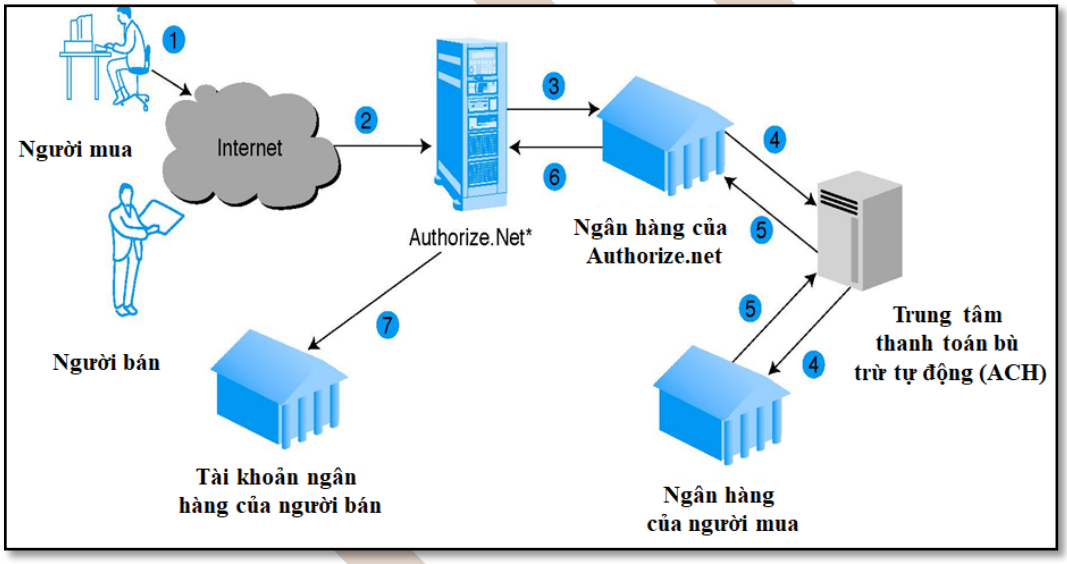
- Bước 3: Trên website của nhà cung cấp dịch vụ thanh toán séc điện tử Authorize.net, khách hàng người mua tiến hành khai báo thông tin. Máy chủ xử lý giao dịch của Authorize.net sẽ chuyển tải thông tin về tấm séc của khách hàng cùng chi tiết của quá trình giao dịch tới ngân hàng của Authorize.net.

- Bước 4: Ngân hàng của Authorize.net tiếp tục truyền thông tin về tấm séc của khách hàng tới ngân hàng của khách hàng thông qua trung tâm thanh toán bù trừ tự động.

- Bước 5: Ngân hàng của khách hàng người mua tiến hành kiểm tra thông tin trên tấm séc mà khách hàng khai báo. Sau đó xác thực thanh toán với ngân hàng của Authorize.net thông qua trung tâm thanh toán bù trừ tự động. (Ngân hàng của khách hàng tiến hành chuyển tiền từ tài khoản phát hành séc của khách hàng người mua sang tài khoản ngân hàng của Authorize.net một số tiền bằng đúng số tiền ghi trên séc thông qua trung tâm thanh toán bù trừ tự động)

- Bước 6: Ngân hàng của Authorize.net sau khi nhận được tiền thanh toán trong tài khoản sẽ lập tức gửi thông báo về phát sinh có trong tài khoản tới Authorize.net cùng với thông tin chi tiết về quá trình giao dịch.

- Bước 7: Authorize.net tiến hành chuyển tiền thanh toán từ tài khoản ngân hàng của mình sang tài khoản ngân hàng của website bán hàng.



Hình 2.16: Quy trình thanh toán séc điện tử của Authorize.net

2.5.4.2 Quy trình thanh toán séc điện tử NACHA

- Bước 1: Trên website bán hàng, người mua lựa chọn sản phẩm và tiến hành thanh toán bằng cách khai báo thông tin chi tiết thông tin về ngân hàng, tài khoản séc của mình.

- Bước 2: Máy chủ của website bán hàng gửi thông tin chi tiết về giao dịch, thông tin về tài khoản séc của người mua và thông tin về tài khoản ngân hàng của website bán hàng tới ngân hàng của người mua.

- Bước 3: Ngân hàng của người mua gửi thông báo về giao dịch và yêu cầu người mua xác thực tài khoản séc và xác nhận giao dịch.

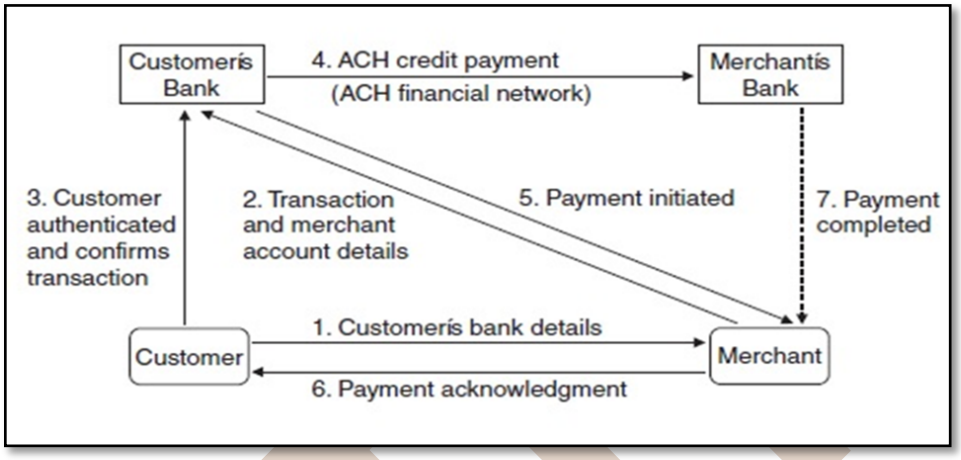
- Bước 4: Sau khi người mua xác thực tài khoản séc và xác nhận giao dịch, ngân hàng

của người mua sẽ tiến hành chuyển khoản số tiền tương ứng từ tài khoản phát hành séc của người mua sang tài khoản ngân hàng của website bán hàng (người bán) thông qua trung tâm thanh toán bù trừ tự động ACH.

- Bước 5: Ngân hàng của người mua sau khi thực hiện giao dịch sẽ thông báo "đã khởi tạo thanh toán" tới website bán hàng hoặc người bán.

- Bước 6: Ngân hàng của website bán hàng gửi thông báo đã nhận được thanh toán tới người mua.

- Bước 7: Ngân hàng của website bán hàng gửi thông báo về phát sinh có trong tài khoản tới website bán hàng.



Hình 2.17: Quy trình thanh toán séc điện tử của NACHA

2.6 Hệ thống thanh toán bằng thư tín dụng và bao thanh toán

2.6.1 Hệ thống thanh toán bằng thư tín dụng điện tử (e-L/C)

2.6.1.1 Thư tín dụng L/C

✓ **Khái niệm**

Trước khi nói đến thư tín dụng điện tử, cần nhắc lại khái niệm về thư tín dụng thông thường. Thư tín dụng còn có tên gọi là L/C – viết tắt của từ Letter of Credit là thư do ngân hàng phát hành theo yêu cầu của bên mua, cam kết thanh toán cho bên bán khoảng tiền nhất định theo hợp đồng trong một thời gian quy định nếu người bán xuất trình được bộ chứng từ thanh toán theo quy định trong L/C.

L/C là hình thức thường được sử dụng trong thanh toán quốc tế. Trong ngành thương mại quốc tế, việc mua bán giữa các nước ngày càng gia tăng, khoảng cách địa lý kéo theo mối lo ngại trong kinh doanh ra nước khác, vì vậy việc sử dụng thư tín dụng giúp cho các bên yên tâm về quyền lợi của mình hơn, góp phần phát triển ngành xuất nhập khẩu của quốc gia.

✓ **Nội dung của L/C**

- Số hiệu, địa điểm, ngày mở L/C*:* Tất cả các L/C đều phải có số hiệu riêng do ngân hàng mở L/C quy định. Ngày mở L/C: là ngày bắt đầu phát sinh cam kết của ngân hàng phát hành với người bán hàng.

- Loại L/C: L/C hủy ngang, L/C không thể hủy ngang, L/C trả chậm, L/C trả dần, L/C

dự phòng, L/C tuần hoàn, L/C chuyển nhượng, L/C giáp lưng, L/C đối ứng.

- Tên và địa chỉ các bên liên quan: Người yêu cầu mở L/C, người hưởng lợi, các ngân hàng…

- Số tiền, loại tiền

- Thời hạn hiệu lực, thời hạn trả tiền, và thời hạn giao hàng

- Điều khoản giao hàng: Điều kiện cơ sở giao hàng, nơi giao hàng…

- Nội dung về hàng hóa: Tên, số lượng, trọng lượng, bao bì…

- Những chứng từ người hưởng lợi phải xuất trình: Hối phiếu, hóa đơn thương mại, vận đơn, chứng từ bảo hiểm, chứng nhận xuất xứ…

- Cam kết của ngân hàng mở thư tín dụng

- Những nội dung khác

✓ **Đặc điểm của L/C**

- L/C là giao dịch kinh tế hai bên giữa ngân hàng phát hành và bên bán, mọi chỉ thị, yêu cầu của bên mua sẽ do ngân hàng phát hành đại diện. Cụ thể, ngân hàng phát hành là người sẽ thanh toán cho bên bán nên khi bên bán muốn ký phát hối phiếu đòi tiền thì phải gửi đến ngân hàng phát hành, không phải là bên mua.

- L/C độc lập với hợp đồng ngoại thương và hàng hóa: L/C thể hiện cam kết thanh toán của ngân hàng phát hành cho người thụ hưởng khi người này xuất trình được bộ chứng từ phù hợp, nó hình thành trên cơ sở hợp đồng nhưng sau đó lại hoàn toàn độc lập với hợp đồng này.

- L/C chỉ giao dịch bằng chứng từ và chỉ thanh toán căn cứ vào chứng từ: Ngân hàng phát hàng không dựa vào tình trạng của hàng hoá thực tế mà sẽ dựa vào bộ chứng từ thanh toán mà bên bán cung cấp có phù hợp với điều khoản trong L/C hay không nên nếu bộ chứng từ hợp lệ thì ngân hàng sẽ thanh toán cho bên bán vô điều kiện vì vậy bên mua cần lưu ý trong công tác kiểm tra hàng hoá.

- L/C yêu cầu tuân thủ chặt chẽ của bộ chứng từ: Bộ chứng từ phải tuân thủ chặt chẽ các điều khoản của L/C.

- L/C không thể huỷ ngang (theo quy định của UPC 600 – Phiên bản áp dụng mới nhất của bộ Quy tắc thực hành thống nhất về tín dụng chứng từ)

- Các bên phải thống nhất và ghi rõ phiên bản áp dụng UPC vào L/C.

- Trước khi mở L/C, bên bán và bên mua cần thống nhất với nhau về các điều khoản trong L/C như thời gian giao hàng và thanh toán…

✓ **Lợi ích của L/C**

Hình thức thanh toán qua L/C được đánh giá là an toàn được nhiều công ty sử dụng, có lợi cho bên bán, bên mua và cả ngân hàng.

- Đối với bên mua

+ Đảm bảo nhận được hàng hoá: Với L/C, chỉ khi nhận được hàng hoá từ người bán thì bên mua mới phải thanh toán cho họ.

+ Đảm bảo các quy định đã đưa ra trong L/C: Giúp cho bên mua yên tâm rằng bên bán

phải đảm bảo thực hiện các điều khoản về thời gian, quy chuẩn hàng hoá đã đưa ra trong L/C.

+ Có thể được ngân hàng phát hành cho vay để thanh toán tiền hàng cho bên bán.

- Đối với bên bán

+ Nhận được thanh toán: Khi bên bán thực hiện đúng theo quy định trong thư tín dụng thì chắc chắn sẽ nhận được thanh toán từ ngân hàng phát hành theo điều khoản thanh toán trong thư tín dụng.

+ Không phải phụ thuộc vào bên mua: Được đảm bảo quyền lợi dựa trên điều khoản của L/C, không phải phụ thuộc vào bên mua như các phương thức thanh toán khác.

- Đối với ngân hàng

+ Gia tăng doanh thu cho ngân hàng thông qua việc thu phí các dịch vụ liên quan đến thư tín dụng

+ Mở rộng quan hệ trong thương mại, tạo được uy tín và danh tiếng trong ngành xuất nhập khẩu.

2.6.1.2 Thư tín dụng điện tử (e-L/C)

Thư tín dụng điện tử thực chất cũng là một thư tín dụng, là phiên bản điện tử của thư tín dụng thông thường và cũng tuân thủ các bước trên. Tuy nhiên, sự khác biệt là các bước này được làm trực tuyến. Để làm được điều này, ngân hàng sẽ phải cung cấp một hệ thống dịch vụ mạng cho phép các bên mua hàng (nhà nhập khẩu) soạn thảo L/C từ máy tính của nhà nhập khẩu, truyền bản thảo này đến ngân hàng để kiểm tra và xử lý. L/C sẽ được phát hành chỉ trong vòng vài giờ. Dịch vụ này cũng cho phép nhận được các L/C xuất khẩu và kiểm tra chúng từ máy tính của nhà xuất khẩu. Và các chứng từ xuất trình có thể là chứng từ điện tử.

Đây là hình thức rất mới và hiện mới chỉ áp dụng ở một số ngân hàng lớn ở các nước có nền CNTT phát triển như Mỹ. Các ngân hàng Mỹ áp dụng e-L/C sẽ yêu cầu khách hàng phải sử dụng địa chỉ IP tĩnh khi sử dụng dịch vụ này của ngân hàng. Khách hàng sẽ được cài một phần mềm do ngân hàng cung cấp, phần mềm này sẽ làm nhiệm vụ thực hiện các thủ tục và giao dịch với ngân hàng. Thư tín dụng điện tử chịu sự điều chỉnh của e-UCP (quy tắc thực hành thống nhất về tín dụng chứng từ điện tử) và là hình thức thanh toán quốc tế có nhiều tiềm năng phát triển mạnh trong tương lai.

2.6.2 Bao thanh toán

Bao thanh toán (factoring), một khái niệm mới với nhiều doanh nghiệp Việt Nam nhưng lại là dịch vụ không thể thiếu với doanh nước ngoài khi bán hàng, đây cũng là một dịch vụ mà các ngân hàng, các tổ chức tài chính của Việt nam cần mở rộng trong quá trình hội nhập với nền tài chính quốc tế.

- ✓ **Khái niệm bao thanh toán**

Một cách giản đơn, bao thanh toán là việc ngân hàng, tổ chức tài chính tạm ứng trước một khoản tiền và thu nợ hộ người bán, thông qua hợp đồng bao thanh toán với một khoản phí. Các doanh nghiệp khi bán hàng trả chậm cho khách hàng (đặc biệt là bán hàng cho nước ngoài), nếu sợ rủi ro trong việc thu tiền trả chậm (trường hợp người mua không thanh toán cho người bán) thì sẽ yêu cầu ngân hàng bao thanh toán rủi ro này.

Có rất nhiều phương thức bao thanh toán:

- Bao thanh toán từng lần: Mỗi lần bao thanh toán, đơn vị bao thanh toán và khách hàng thực hiện thủ tục bao thanh toán và ký kết hợp đồng bao thanh toán.

- Bao thanh toán theo hạn mức: Đơn vị bao thanh toán xác định và thỏa thuận với khách hàng một mức nợ bao thanh toán tối đa được duy trì trong một khoảng thời gian nhất định và việc sử dụng hạn mức này. Mỗi năm ít nhất một lần, đơn vị bao thanh toán xem xét xác định lại hạn mức và thời gian duy trì hạn mức này.

- Bao thanh toán hợp vốn: Hai hay nhiều đơn vị bao thanh toán cùng thực hiện bao thanh toán đối với một hoặc một số khoản phải thu hoặc khoản phải trả của khách hàng, trong đó một đơn vị bao thanh toán làm đầu mối thực hiện việc tổ chức bao thanh toán hợp vốn.

✓ **Quy trình thực hiện bao thanh toán**

- **Quy trình thực hiện bao thanh toán trong nước**

- Bước 1: Người bán và người mua tiến hành thương lượng trên hợp đồng mua bán hàng hóa.

- Bước 2: Người bán đề nghị đơn vị bao thanh toán (ngân hàng) tài trợ với tài sản đảm bảo chính là khoản phải thu trong tương lai từ hợp đồng mua bán hàng hóa.

- Bước 3: Đơn vị bao thanh toán tiến hành thẩm định khả năng thanh toán tiền hàng của người mua.

- Bước 4: Nếu xét thấy có thể thu được tiền hàng từ người mua theo đúng hạn hợp đồng mua bán, đơn vị bao thanh toán sẽ thông báo đồng ý tài trợ cho người bán.

- Bước 5: Đơn vị bao thanh toán và người bán thỏa thuận và ký kết hợp đồng bao thanh toán.

- Bước 6: Người bán hàng giao hàng cho người mua theo đúng thỏa thuận trong hợp đồng mua bán hàng hóa.

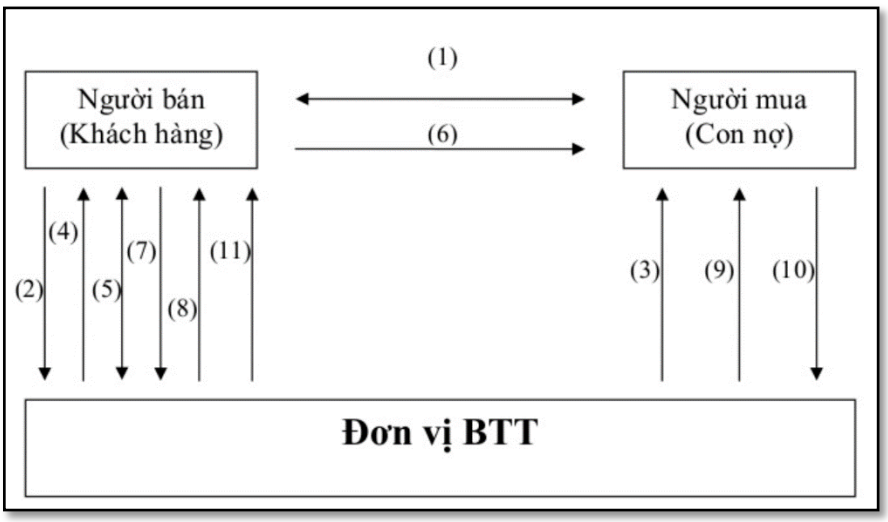
- Bước 7: Người bán chuyển nhượng hóa đơn, chứng từ bán hàng và các chứng từ khác liên quan đến các khoản phải thu cho đơn vị bao thanh toán.

- Bước 8: Đơn vị bao thanh toán ứng trước một phần tiền cho người bán theo thỏa thuận trong hợp đồng bao thanh toán.

- Bước 9: Khi đến hạn thanh toán, đơn vị bao thanh toán tiến hành thu hồi nợ từ người mua.

- Bước 10: Người mua thanh toán tiền hàng cho đơn vị bao thanh toán.

- Bước 11: Sau khi đã thu hồi tiền hàng từ phía người mua, đơn vị bao thanh toán thanh toán nốt tiền chuyển nhượng khoản phải thu cho người bán.



Hình 2.18: Quy trình thực hiện bao thanh toán trong nước

- **Quy trình thực hiện bao thanh toán quốc tế**

- Bước 1: Nhà xuất khẩu và nhà nhập khẩu đàm phán ký kết hợp đồng xuất nhập khẩu hàng hóa.

- Bước 2: Nhà xuất khẩu đề nghị đơn vị bao thanh toán xuất khẩu cung cấp dịch vụ bao thanh toán.

- Bước 3: Đơn vị bao thanh toán xuất khẩu đề nghị đơn vị bao thanh toán nhập khẩu cùng thực hiện hợp đồng bao thanh toán.

- Bước 4: Đơn vị bao thanh toán nhập khẩu tiến hành thẩm định nhà nhập khẩu và quyết định có cung cấp dịch vụ bao thanh toán hay không.

- Bước 5: Nếu đơn vị bao thanh toán nhập khẩu đồng ý tham gia giao dịch bao thanh toán với đơn vị bao thanh toán xuất khẩu, đơn vị bao thanh toán xuất khẩu sẽ thông báo đồng ý tài trợ cho nhà xuất khẩu.

- Bước 6: Đơn vị bao thanh toán xuất khẩu và nhà nhập khẩu thỏa thuận và ký kết hợp đồng bao thanh toán.

- Bước 7: Nhà xuất khẩu giao hàng cho nhà nhập khẩu theo đúng thỏa thuận hợp đồng mua bán ngoại thương.

- Bước 8: Nhà xuất khẩu chuyển nhượng bộ chứng từ cho đơn vị bao thanh toán xuất khẩu, đồng thời đơn vị bao thanh toán xuất khẩu cũng sẽ chuyển nhượng bộ chứng từ này cho đơn vị bao thanh toán nhập khẩu.

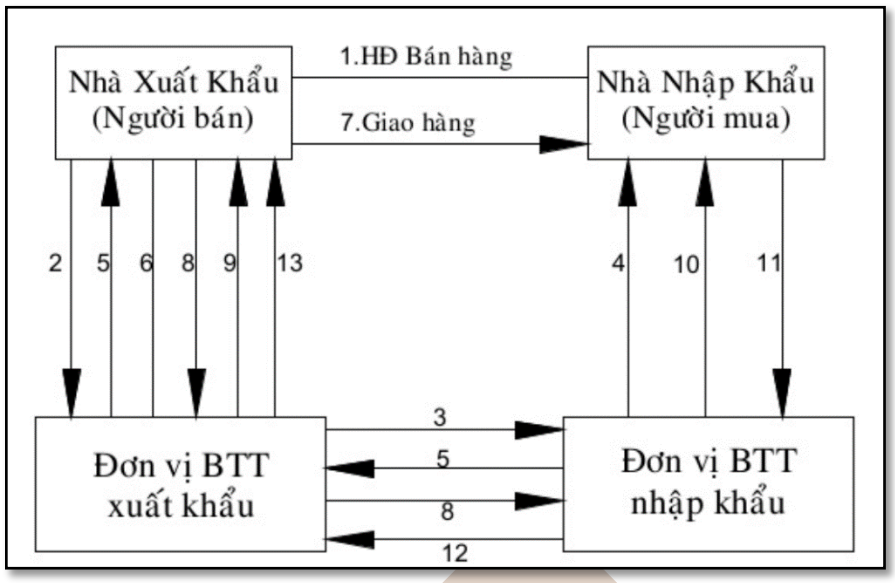
- Bước 9: Đơn vị bao thanh toán xuất khẩu ứng trước tiền cho nhà xuất khẩu theo thỏa thuận trong hợp đồng bao thanh toán.

- Bước 10: Khi đến hạn thanh toán, đơn vị bao thanh toán nhập khẩu tiến hành thu tiền từ nhà nhập khẩu.

- Bước 11: Nhà nhập khẩu thanh toán tiền cho đơn vị bao thanh toán nhập khẩu.

- Bước 12: Đơn vị bao thanh toán nhập khẩu sau khi trừ đi các khoản phí và lãi (nếu có) sẽ chuyển số tiền còn lại cho đơn vị bao thanh toán xuất khẩu.

- Bước 13: Đơn vị bao thanh toán xuất khẩu và nhà nhập khẩu quyết toán các khoản còn lại.



Hình 2.19: Quy trình thực hiện bao thanh toán quốc tế

✓ **Những tiện ích của bao thanh toán**

- **Về phía người bán hàng**

- Người bán có thể thu tiền ngay thay vì phải đợi tới kỳ hạn thanh toán theo hợp đồng.

- Tăng lợi thế cạnh tranh khi chào hàng với các điều khoản thanh toán trả chậm mà không ảnh hưởng đến nguồn vốn kinh doanh của mình.

- Được sử dụng khoản phải thu đảm bảo cho tiền ứng trước, do đó tăng được (một cách gián tiếp) nguồn vốn lưu động phục vụ sản xuất kinh doanh.

- Chủ động trong việc lập kế hoạch tài chính vì dự đoán được dòng tiền vào.

- Tiết kiệm thời gian và chi phí trong việc theo dõi thu hồi các khoản trả chậm này.

- Tiện ích của dịch vụ bao thanh toán rất quan trọng đối với nhà sản xuất, bởi hiện nay các nhà nhập khẩu qui mô, ưu thế chỉ chấp nhận hình thức trả sau và từ chối yêu cầu mở L/C của nhà xuất khẩu. Điều này sẽ khiến các doanh nghiệp dễ mất đơn hàng xuất khẩu nếu không có khả năng về vốn. Còn nếu chấp nhận hình thức trả sau, doanh nghiệp sẽ khó khăn trong việc quay vòng vốn, nhất là những đơn vị xuất khẩu các mặt hàng luôn biến động giá như cà phê, gạo, tiêu… Trong khi đó, ngân hàng cũng không dễ cho doanh nghiệp kéo dài thời gian thanh toán nếu thanh toán theo phương thức trả sau. Vì thế, dịch vụ bao thanh toán xuất khẩu ra đời sẽ giúp doanh nghiệp giải quyết được những khó khăn này.

- Đa phần các doanh nghiệp vừa và nhỏ rất thích dịch vụ bao thanh toán, bởi thông thường những doanh nghiệp này có tổng tài sản không lớn nên rất khó để ngân hàng xem xét các hạn mức tín dụng. Với bao thanh toán họ dễ dàng được cấp hạn mức tín dụng hơn.

- Các doanh nghiệp khi đã biết về dịch vụ bao thanh toán thường rất thích sử dụng vì bao thanh toán có nhiều hình thức khác nhau, rất đa dạng để phục vụ cho các doanh nghiệp. Các doanh nghiệp có thể sử dụng các hình thức như: bao thanh toán chiết khấu hóa đơn, bao

thanh toán trung gian, bao thanh toán đến hạn, bao thanh toán thu hộ, bao thanh toán truy đòi, bao thanh toán miễn truy đòi.

- Phạm vi hoạt động bao thanh toán cũng rất đa dạng: Về địa lý thì có bao thanh toán trong nước và bao thanh toán quốc tế; Trong hoạt động xuất nhập khẩu thì có bao thanh toán xuất khẩu và bao thanh toán nhập khẩu; Có bao thanh toán số lượng hóa đơn của người bán hoặc bao thanh toán toàn bộ hay bao thanh toán một phần; Có bao thanh toán kín và bao thanh toán công khai... Khách hàng có thể sử dụng bao thanh toán trực tiếp và bao thanh toán hệ hai đại lý, hay khách hàng cũng có thể sử dụng liên kết của các hợp đồng bao thanh toán với bao thanh toán giáp lưng. Phương thức bao thanh toán từng lần hoặc bao thanh toán theo hạn mức.

- **Về phía ngân hàng**

- Đa dạng hóa các loại hình dịch vụ phục vụ khách hàng.

- So với việc cấp hạn mức tín dụng, ngân hàng thích làm dịch vụ bao thanh toán hơn vì nếu cấp vốn lưu động cho doanh nghiệp, ngân hàng phải giám sát rất vất vả, trong khi với bao thanh toán các khoản phải thu rất rõ, việc sử dụng cũng đã rõ, các doanh nghiệp đã chứng minh với ngân hàng về uy tín trên thị trường khi đã bán được hàng.

- Có thể nói, bao thanh toán là loại dịch vụ cả hai bên cùng có lợi. Nhưng doanh nghiệp có lợi hơn ngân hàng. Khi cung cấp dịch vụ này ngân hàng phải gánh chịu về mình những rủi ro khi người mua mất khả năng thanh toán. Do vậy, ngân hàng phục vụ người bán, nhà xuất khẩu, nếu không chắc chắn về khả năng tài chính của người mua thường hay tư vấn cho khách hàng của mình tới ngân hàng phục vụ người mua, nhà nhập khẩu yêu cầu dịch vụ bao thanh toán. Những ngân hàng thực hiện dịch vụ bao thanh toán cần tính toán kỹ lưỡng đối với những mặt hàng nhiều rủi ro như nông sản, thực phẩm…

- **Về phía doanh nghiệp mua**

- Được áp dụng hình thức trả chậm.

- Từ đó cũng làm tăng nguồn vốn lưu động kinh doanh của doanh nghiệp.

2.7. Hệ thống thanh toán EDI

2.7.1 Khái niệm

Trao đổi dữ liệu điện tử (EDI:electronic data interchangeb) là công nghệ cho phép trao đổi trực tiếp dữ liệu có cấu trúc giữa các máy tính thông qua phương tiện điện tử.

Hiểu một cách đơn giản hơn, EDI chính là việc trao đổi dữ liệu dưới dạng *có cấu trúc* (structured form), nghĩa là các thông tin được trao đổi giữa các đối tác thoả thuận với nhau tuân thủ theo một khuôn dạng nào đó từ máy tính điện tử này sang máy tính điện tử khác, giữa các doanh nghiệp hoặc các đơn vị đã thỏa thuận với nhau, theo cách này sẽ tự động hóa hoàn toàn không cần có sự can thiệp của con người.

EDI bao hàm những qui trình đảm bảo cho hình thức truyền thông này an toàn hơn. Ngoài khả năng nhận dạng, kỹ thuật này còn có thể hỗ trợ phát hiện và sửa lỗi. Chứng thực theo hướng xác nhận nội dung dữ liệu có thể được thực hiện và tính cá nhân có thể trong EDI bởi một số phương tiện tích hợp trong hệ thống. Chứng thực người được quyền gửi thông điệp cũng được đảm bảo.

EDI có thể được sử dụng để truyền theo đường điện tử các tài liệu như hoá đơn, phiếu đặt hàng, giấy biên nhận, các tài liệu vận chuyển và các thư từ trao đổi nghiệp vụ chuẩn khác giữa các tổ chức và các đối tác kinh doanh. EDI cũng có thể được sử dụng để truyền thông tin tài chính và thanh toán dưới dạng điện tử, thường được gọi là *chuyển tiền điện tử* (EFT-Electronique funds transfer). Do đó, các chức năng của EDI ngày nay càng trở nên có ý nghĩa hơn, đặc biệt với sự phát triển của TMĐT trên thế giới.

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…). EDI chủ yếu được thực hiện thông qua *mạng ngoài* (extranet) với nhau và thường được gọi là *mạng thương mại* (net-commerce). Cũng có khi có *EDI hỗn hợp* (hybird EDI) dùng cho trường hợp chỉ có một bên đối tác dùng EDI, còn bên kia thì vẫn dùng các phương thức thông thường (như fax, thư tín qua bưu điện…).

Để sử dụng rộng rãi EDI, người ta phải tìm cách áp dụng EDI vào Internet. Khái niệm EDI mở được đưa ra để phù hợp với môi trường mạng Internet. Doanh nghiệp có thể dùng các EDI trong tất cả các khâu của quá trình kinh doanh.

2.7.2 Đặc điểm của EDI

- Cho phép doanh nghiệp gửi và nhận một lượng lớn giao dịch thông tin thông thường nhanh hơn trên phạm vi toàn cầu.

- Rất ít lỗi trong việc truyền dữ liệu vì được truyền qua mạng máy tính.

- Thông tin được truyền giữa một vài đối tác kinh doanh thống nhất.

- Công ty có thể truy cập cơ sở dữ liệu của đối tác kinh doanh để lấy và lưu giữ giao dịch chuẩn.

- EDI thúc đẩy mối quan hệ hợp tác chiến lược vì nó liên quan đến việc cam kết với đầu tư trong dài hạn và sự tinh lọc lại hệ thống

- EDI tạo ra một môi trường giao dịch không giấy tờ, vì vậy rất tiết kiệm chi phí và tăng tính hiệu quả.

- Thanh toán được rút ngắn lại.

- Dữ liệu có thể được nhập khi không cần kết nối Internet

- Khi nhận được tài liệu được truyền bằng EDI, dữ liệu có thể được sử dụng ngay.

- Thông tin về bán hàng được thông báo tới nhà sản xuất, bộ phận vận chuyển và bộ phận kho kịp thời.

- EDI có thể giúp doanh nghiệp tiết kiệm được một khoản chi phí đáng kể

2.7.3 Quy trình hoạt động của EDI

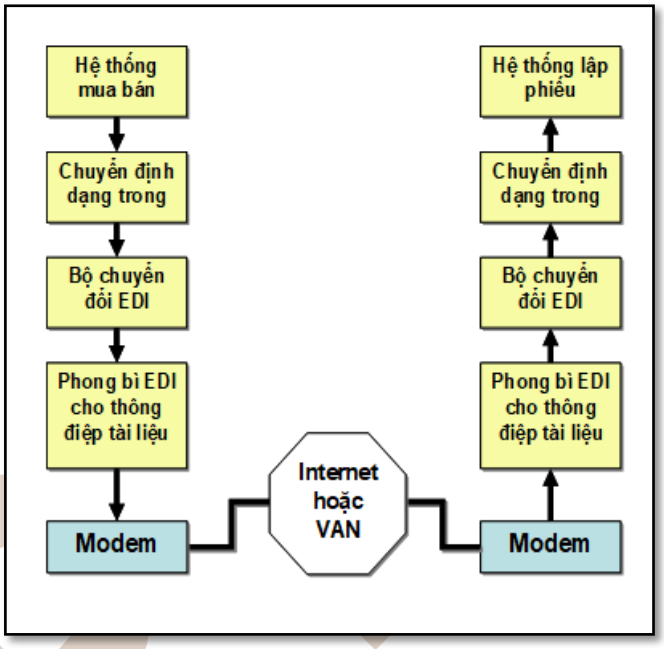
- Bước 1 - Chuẩn bị tài liệu điện tử*:* Bước đầu tiên trong trình tự của EDI là tập hợp thông tin và dữ liệu. Cách thu thập thông tin cần thiết cũng giống như trong hệ thống truyền thống. Tuy nhiên, thay vì in dữ liệu ra giấy, hệ thống phải xây dựng một cơ sở dữ liệu để lưu các dữ liệu này. Khi đã có tệp dữ liệu hoặc cơ sở dữ liệu rồi, có thể chuyển sang bước sau.

- Bước 2 - Dịch dữ liệu để chuyển đi: Bước tiếp theo là dịch tệp tài liệu hoặc cơ sở dữ liệu sang định dạng tiêu chuẩn theo đặc tả của tài liệu tương ứng. Tệp dữ liệu kết quả phải chứa một chuỗi giao dịch có liên quan đến, chẳng hạn như phiếu mua hàng.

- Bước 3 - Truyền thông: Máy tính sẽ nối và chuyển tự động các tệp dữ liệu đó đến lên mạng Internet hoặc một mạng giá trị gia tăng (VAN) đã thu xếp trước. Internet hoặc mạng VAN sẽ xử lý từng tệp dữ liệu và chuyển tới hộp thư điện tử tương ứng với các địa chỉ nơi nhận đã được ghi trong tệp

- Bước 4 - Dịch dữ liệu đến: Công ty nhận dữ liệu định kỳ lấy tệp dữ liệu từ hộp thư của họ và dịch ngược tệp dữ liệu đó từ dạng tiêu chuẩn sang dạng đặc thù theo yêu cầu của phần mềm ứng dụng của công ty.

- Bước 5 - Xử lý tài liệu điện tử: Đến đây thì hệ thống tài liệu nội bộ của công ty đã có thể xử lý tài liệu nhận được. Mọi tài liệu là kết quả xử lý tương ứng với giao dịch nhận được cũng phải dùng những qui trình hoặc những bước như vậy để chuyển lại cho nơi khởi động giao dịch. Khi đó, có thể kết thúc vòng thực hiện trao đổi dữ liệu điện tử.



Hình 2.20: Hoạt động của EDI

2.7.4 Thanh toán qua EDI

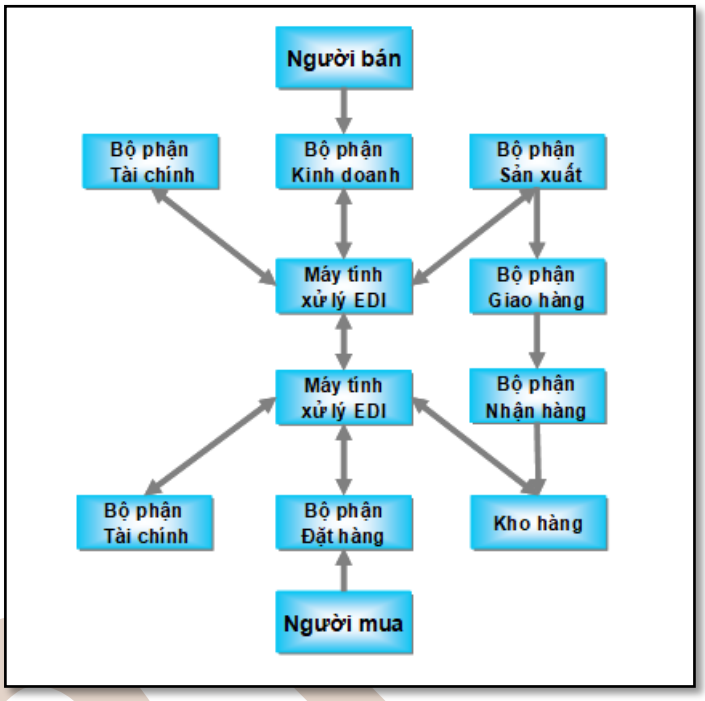
Thanh toán qua EDI đã được các hãng lớn sử dụng từ lâu, trên mạng riêng gọi là mạng giá trị gia tăng (VAN). Hệ thống này đảm bảo độ an toàn và tin cậy cao. VAN là một hệ thống kết nối chặt chẽ, thủ tục trao đổi được kiểm soát gắt gao, chi phí thanh toán trên VAN rất cao, không thích hợp với doanh nghiệp vừa và nhỏ.

Doanh nghiệp có thể dùng các EDI trong tất cả các khâu của quá trình kinh doanh. Thuận lợi này trước hết tạo điều kiện cho các doanh nghiệp sử dụng EDI giảm bớt nhu cầu về phần cứng và phần mềm phải duy trì trên các hệ thống máy tính, đồng thời làm tăng tính linh hoạt và mềm dẻo của dịch vụ EDI, tạo ra cơ hội để nhiều doanh nghiệp (đặc biệt là doanh nghiệp quy mô vừa và nhỏ) có thể dễ dàng ứng dụng EDI, tận dụng các lợi thế của nó phục vụ hoạt động kinh doanh của mình.

Một giao dịch EDI trong lĩnh vực thanh toán được gọi là giao dịch EDI tài chính. EDI tài chính thường được thiết lập giữa doanh nghiệp và ngân hàng trong việc thanh toán giao dịch B2B. Ngân hàng khi nhận EDI coi như đã nhận được ủy nhiệm chi của người mua và

thanh toán cho người bán. Việc sử dụng EDI trên internet sẽ mở ra khả năng thanh toán trên mạng tăng vì có chi phí rất thấp và linh hoạt hơn nhiều so với việc sử dụng mạng VAN. Hình 2.21 trình bày luồng thanh toán qua EDI trong TMĐT.

Các phương án thanh toán trên mạng có một vị trí quan trọng trong tiến trình phát triển TMĐT. Các phương án trên là những phương án khả thi, chủ yếu mô phỏng phương pháp truyền thống. Thực tế cũng còn rất nhiều việc phải tiếp tục nghiên cứu và hoàn thiện để đi đến một sự chấp nhận chung mang tầm quốc tế. Vấn đề quan trọng nhất đó chính là vấn đề an ninh trong TMĐT.



Hình 2.21: Thanh toán EDI trong TMĐT

CÂU HỎI CHƯƠNG 2

[1]. Trình bày khái thẻ thanh toán?

[2]. Trình bày cấu tạo thẻ thanh toán?

[3]. Trình bày về các loại thẻ thanh toán?

[4]. Mô tả quy trình thanh toán thẻ trực tuyến?

[5]. Phân tích các rủi ro thường gặp trong thanh toán thẻ? Cho ví dụ minh họa?

[6]. Trình bày về hệ thống thanh toán bằng ví điện tử?

[7]. Nêu khái niệm, đặc điểm, phân loại ví điện tử?

[8]. Trình bày quy trình thanh toán bằng ví điện tử?

[9]. Trình bày khái quát về hệ thống vi thanh toán điện tử?

[10]. Trình bày về hệ thống thanh toán bằng chuyển khoản điện tử?

[11]. Trình bày về hệ thống thanh toán séc điện tử?

[12]. Trình bày về hệ thống thanh toán bằng thư tín dụng và bao thanh toán?

[13]. Trình bày về hệ thống thanh toán EDI?

TÀI LIỆU THAM KHẢO CHƯƠNG 2

[9]. Nguyễn Văn Hồng và Nguyễn Văn Thoan, Giáo trình TMĐT căn bản, NXB Bách Khoa – Hà Nội, 2013

[10]. Nguyễn Văn Hùng (chủ biên), TMĐT - cẩm nang, NXB Kinh tế TP Hồ Chí Minh 2013

[11]. Lê Quân & Hoàng Văn Hải, Giáo trình quản trị tác nghiệp doanh nghiệp thương mại, NXB Thống Kê, 2010

[12]. Thái Thanh Sơn và Thái Thanh Tùng, TMĐT trong thời đại số, NXB Thông tin và Truyền thông, 2017

[13]. Andreas Meier & Henrik Stormer, eBusiness & eCommerce - Managing the Digital Value Chain, Springer, 2009

[14]. Dave Chaffey, E-business and E-commerce Management: Strategy, Implementation and Practice – 6th, Pearson Education, 2015

[15]. Arch G. Woodside & Peter J. LaPlaca, Handbook of Strategic e-Business Management, Springer-Verlag Berlin Heidelberg, 2014.

[16]. Kenneth C. Laudon & Carol Guercio Traver: E-commerce Business, Technology, Society: 13th edition: Pearson Publishing House, 2017.

CHƯƠNG 3: BẢO MẬT TRONG THANH TOÁN ĐIỆN TỬ

3.1 Vấn đề bảo mật trong thanh toán điện tử

Thanh toán điện tử là một hoạt động then chốt đảm bảo thực thi và hoàn thiện hoạt động TMĐT được xuyên suốt, vì thế bảo mật trong thanh toán điện tử là vấn đề vô cùng quan trọng và cần thiết. Việc đảm bảo an toàn trong thanh toán điện tử sẽ giúp cho các bên tham gia người mua, người bán, tổ chức thanh toán tin tưởng và gia tăng hiệu quả trong thanh toán.

An toàn trong thanh toán điện tử được hiểu là an toàn thông tin trao đổi giữa các chủ thể khi tham gia giao dịch thanh toán, an toàn cho các hệ thống (hệ thống máy chủ thương mại và các thiết bị đầu cuối, đường truyền…) không bị xâm hại từ bên ngoài hoặc có khả năng chống lại những tai hoạ, lỗi và sự tấn công từ bên ngoài.

- ✓ **Dưới góc độ người dùng**

Được sử dụng đúng website của những công ty hợp pháp, được đảm bảo về độ an toàn và tin cậy

Kể cả trong môi trường TMĐT, doanh nghiệp bán hàng trên website không bán hàng trực tiếp thì doanh nghiệp vẫn luôn phải đăng ký kinh doanh và có địa điểm vật lý rõ ràng, vì thế người dùng phải kiểm tra tính pháp lý rõ ràng của doanh nghiệp.

Không được chứa đựng virus và các đoạn mã nguy hiểm trong các website

Khi đã truy cập đúng vào website rồi, thì người dùng băn khoăn là website này có chứa đựng những đoạn mã nguy hiểm hay không? website có bị lây nhiễm những phần mềm spyware hay trojan horse hay không? Khi truy cập vào có bị nguy hại gì đến máy tính hay các thiết bị hay không. Chính vì thế vấn đề thứ hai là website đó phải đảm bảo độ an toàn cho người dùng, làm cho người dùng có cảm giác tin cậy.

Hoặc là người dùng phải tự bảo vệ mình bằng những biện pháp cơ bản: ví dụ trên hệ thống thiết bị của người dùng luôn có phương thức để đảm bảo an toàn cho máy móc như cài chương trình phần mềm diệt virus trên máy tính, hoặc thường xuyên cập nhật phiên bản mới của hệ điều hành.

Được bảo mật các thông tin về thanh toán: mã thanh toán, mật khẩu, số tài khoản…

Khi tham gia giao dịch trên web, vấn đề thứ ba rất đáng lo ngại xuất phát từ phía người dùng, là liệu thông tin liên quan đến thanh toán có được bảo vệ hay không? Thông tin về mã PIN, mật khẩu, mã xác thực thẻ thanh toán CVV, ngày có hiệu lựu của thẻ thanh toán… .

- ✓ **Dưới góc độ doanh nghiệp**

Đứng dưới góc độ doanh nghiệp, họ có một số yêu cầu:

Có khả năng bảo vệ website, bảo vệ hệ thống trước những cuộc tấn công bên ngoài

Từ năm 2000 trở lại đây, tình trạng tội phạm mạng ngày càng tăng cao, có nhiều cuộc tấn công vào website TMĐT: tấn công thay đổi giao diện, DoS, DDoS. Chính vì thế, bản thân doanh nghiệp có khả năng bảo vệ website trước những cuộc tấn công bên ngoài.

Bảo vệ người tiêu dùng khi tham gia các giao dịch thanh toán

Đặt lợi ích của người tiêu dùng lên trên hết. Tức là website lại phải được đảm bảo, an toàn, tạo độ tin cậy. Thông qua một số giao thức SET, SSL.

✓ **Dưới góc độ hệ thống**

Tính bí mật của thông tin

+ Đảm bảo thông tin trao đổi giữa các bên tham gia không bị tiết lộ ra bên ngoài.

+ Sử dụng phương pháp mã hóa thông tin để đảm bảo tính bí mật của thông tin.

Tính toàn vẹn của thông tin

+ Đảm bảo cho thông tin trao đổi 2 chiều không bị biến đổi trong quá trình truyền tin. Bất kỳ 1 sự sửa đổi hay thay thế nào về mặt nội dung dù là nhỏ nhất cũng dễ dàng bị phát hiện.

+ Sử dụng hàm băm để đảm bảo được tính toàn vẹn của thông tin.

Tính sẵn sàng của thông tin

+ Đảm bảo thông tin luôn luôn sẵn sàng, đáp ứng yêu cầu truy cập dịch vụ khi cần thiết

+ Nếu muốn đảm bảo được yêu cầu này mà lại phải chống lại tất cả các cuộc tấn công từ bên ngoài cho nên rất khó.

- Tính chống từ chối phủ định

+ Đảm bảo tính chống lại từ chối hoặc phủ định các giao dịch thanh toán đã thực hiện thông qua việc cung cấp bằng chứng cụ thể.

+ Để đảm bảo được yêu cầu này, hệ thống thông tin bảo vệ được người dùng chứng thực giao dịch đã xảy ra để đảm bảo quyền lợi cho người tiêu dùng.

Tính xác thực

+ Xác thực là xác định xem những ai tham gia vào quy trình giao dịch, trao đổi thông tin về phương tiện thanh toán. Xác thực thông tin cần làm rõ: chủ thể tham gia giao dịch là ai, phương tiện thanh toán của chủ thể là gì?

+ Sử dụng chữ ký điện tử để xác thực người dùng, đối tượng tham gia giao dịch.

Quyền cấp phép

+ Xác định những ai có quyền truy cập vào tài nguyên hệ thống, những loại tài nguyên nào thì đượp phép sử dụng thông qua việc cung cấp nhưng bằng chứng cụ thể.

Thực chất của quá trình cấp phép là ngăn ngừa những dữ liệu không hợp pháp, những người không hợp pháp can thiệp vào người dùng.

+ Cơ chế cấp phép là cơ chế so sánh về cá nhân hay chương trình với các thông tin kiểm soát truy cập liên kết với các nguồn lực được truy cập.

Quyền kiểm soát

+ Mục đích: Theo dõi lưu vết người dùng

+ Cung cấp các bằng chứng chứng minh đã có giao dịch xảy ra, để sau này có phát sinh khiếu nại sẽ có bằng chứng chống lại từ chối dịch vụ.

3.2 Các loại hình tấn công

3.2.1 Phishing

- ✓ **Khái niệm**

Tấn công giả mạo trong lĩnh vực bảo mật máy tính, là một hành vi giả mạo ác ý nhằm lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thể tin cậy trong một giao dịch điện tử. Các giao dịch thường dùng để đánh lừa những người dùng ít đa nghi là các giao dịch có vẻ xuất phát từ các website xã hội phổ biến, các trung tâm chi trả trực tuyến hoặc các quản trị mạng.

Phishing là loại hình gian lận (thương mại) trên Internet, một thành phần của Social Engineering – "kỹ nghệ lừa đảo" trên mạng. Nguyên tắc của phishing là bằng cách nào đó "lừa" người dùng gửi thông tin nhạy cảm như tên, địa chỉ, mật khẩu, số thẻ tín dụng, mã thẻ ATM, số an sinh xã hội,… đến kẻ lừa đảo (scammer). Cách thực hiện chủ yếu là mô phỏng lại giao diện trang web đăng nhập (login page) của các website có thật, kẻ lừa đảo sẽ dẫn dụ nạn nhân (victim) điền các thông tin vào trang "dỏm" đó rồi truyền tải đến anh ta (thay vì đến server hợp pháp) thực hiện hành vi đánh cắp thông tin bất hợp pháp mà người sử dụng không hay biết.

Tấn công giả mạo thường được thực hiện qua thư điện tử hoặc tin nhắn nhanh, và hay yêu cầu người dùng nhập thông tin vào một website giả mạo gần như giống hệt với website thật. Ngay cả khi có sử dụng chứng thực máy chủ, có khi vẫn phải cần vài kĩ năng phức tạp mới xác định được website là giả mạo. Tấn công giả mạo là một đơn cử của những kĩ thuật lừa đảo qua mạng (social engineering) nhằm đánh lừa người dùng, và khai thác sự bất tiện hiện nay của công nghệ bảo mật web. Để chống lại hình thức tấn công lừa đảo ngày càng tăng, người ta đã nỗ lực hoàn chỉnh hành lang pháp lý, huấn luyện cho người dùng, cảnh báo công chúng, và tăng cường an ninh kĩ thuật.

- ✓ **Nguồn gốc và tên gọi**

Nguồn gốc từ Phishing là kết hợp giữa 2 từ Fish - Fishing và Phreaking. Fishing nghĩa gốc là "câu cá" nhưng được hiểu là "câu" các thông tin mật khẩu, tài chính của người dùng. Mặt khác, do tính chất của nó cũng gần giống kiểu tấn công Phreaking (Chữ "Ph" được các hacker thay thế cho chữ "F" để tạo thành phishing do cách phát âm gần giống) - được biết đến lần đầu tiên bởi hacker John Draper (biệt danh aka Captain Crunch) khi sử dụng "Blue Box" để tấn công hệ thống điện thoại ở Mỹ nhằm thực hiện các cuộc gọi đường dài miễn phí hoặc sử dụng đường điện thoại của người khác thực hiện các cuộc gọi bất hợp pháp,… vào đầu thập niên 1970, tên gọi khác là Phone Phreaking.

Phishing xuất hiện cũng khá lâu, lần đầu được biết vào khoảng năm 1996 khi được các hacker sử dụng để đánh cắp các tài khoản các khách hàng của công ty AOL (American Online) – các tài khoản bị đánh cắp thường được gọi là "phish". Cũng vào năm 1996, kỹ thuật phishing được thảo luận thường xuyên trên các Nhóm tin (NewsGroup) của nhóm hacker "2600" nổi tiếng. Tuy nhiên, kỹ thuật này có thể được sử dụng nhiều năm trước đó, nhưng không phổ biến. Theo thời gian, những cuộc tấn công phishing không còn chỉ nhằm vào các tài khoản internet của AOL mà đã mở rộng đến nhiều mục tiêu, đặc biệt là các ngân hàng trực tuyến, các dịch vụ TMĐT, thanh toán trên mạng, và hầu hết các ngân hàng lớn ở Mỹ, Anh, Úc đều bị tấn công bởi phishing. Vì nhằm vào đánh cắp credit card nên nó còn được gọi là

Carding.

✓ **Cách thức tấn công**

Trước đây, hacker thường dùng trojan (gián điệp) đến máy nạn nhân để chương trình này gửi mật khẩu hay thông tin đến kẻ tấn công. Sau này cách dùng mánh lới lừa đảo lấy thông tin được sử dụng nhiều hơn. Lừa đảo thì có rất nhiều cách, phổ biến và dễ thực hiện vẫn là phishing. Nếu ai đã từng nghe qua kỹ thuật "Fake Login Email" sẽ thấy phishing cũng dựa theo nguyên tắc này. Để thực hiện phishing cần hai bước chính:

(1) Tìm cách dụ nạn nhân mở địa chỉ trang web đăng nhập giả. Cách làm chính là thông qua đường liên kết của email.

(2) Tạo một web lấy thông tin giả giống ý như thật.

Không chỉ có vậy, hacker còn kết hợp nhiều xảo thuật khác như tạo những email (giả) cả địa chỉ lẫn nội dung sao cho có sức thu hút, mã hóa đường link (URL) trên thanh addres bar, tạo IP server giả.

✓ **Cách phòng chống**

Phòng chống phishing không khó, quan trọng là người dùng phải cẩn thận khi nhận được các trang đăng nhập có yêu cầu điền thông tin nhạy cảm. Như đã nói trên, tấn công phishing qua hai giai đoạn thì phòng chống cũng qua hai giai đoạn.

- Với email giả: Chúng ta thử lấy một ví dụ một email giả mạo danh ngân hàng Citibank gửi đến khách hàng.

QUOTE
Received: from host70-72.pool80117.interbusiness.it ([80.117.72.70]) by mailserver with SMTP id <20030929021659s1200646q1e > ; Mon, 29 Sep 2003 02:17:00 +0000

Received: from sharif.edu [83.104.131.38] by host70-72.pool80117.interbusiness.it

Postfix) with ESMTP id EAC74E21484B for; Mon, 29 Sep 2003 11:15:38 +0000
Date: Mon, 29 Sep 2003 11:15:38 +0000

From: Verify

Subject: Citibank E-mail Verification: e-response@sécurescience.net
To: E-Response
References:
In-Reply-To:
Message-ID:
Reply-To: Verify
Sender: Verify
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Dear Citibank Member,

This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection -t- becaurse some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL)K, copy and paste the link into the address bar of your web browser.
http://www.citibank.com:ac=piUq3027qcHw003...X6CMW2I2uPOVQW/
y----------
Thank you for using Citibank!
C----------
This automatic email sent to: e-response@sécurescience.net
Do not reply to this email.
R_CODE: ulG1115mkdC54cbJT469

Nếu quan sát kỹ, chúng ta sẽ thấy một số điểm "thú vị" của email này:

+ Về nội dung thư:

Rõ là câu cú, ngữ pháp lộn xộn và có những từ sai chính tả, ví dụ becaurse, this automatic. Và ai cũng rõ là điều này rất khó xảy ra đối với một ngân hàng vì các email đều được "chuẩn hóa" thành những biểu mẫu thống nhất.

Có chứa những ký tự hash-busters – là những ký tự đặc biệt để vượt qua các chương trình lọc thư rác (spam) - dựa vào kỹ thuật hash-based spam như "-t-", "K" ở phần chính thư và "y", "C" ở cuối thư. Người nhận khác nhau sẽ nhận những spam với những hash-busters khác nhau. Một email thật, có nguồn gốc rõ ràng thì đâu cần phải dùng đến các "tiểu xảo" đó.

Phần header của email không phải xuất phát từ mail server của Citibank. Thay vì mango2-a.citicorp.com (mail server chính của Citybank ở Los Angeles) thì nó lại đến từ Italia với địa chỉ host70-72.pool80117.interbusiness.it (80.117.72.70) vốn không thuộc quyền kiểm soát của CityBank. Lưu ý, mặc định Yahoo Mail hay các POP Mail Client không bật tính năng xem header, các người sử dụng nên bật vì sẽ có nhiều điều hữu ích.

+ Với liên kết ở dưới:

Nhìn thoáng quá thì có vẻ là xuất phát từ Citibank, nhưng thực tế hãy xem đoạn phía sau chữ @ (xem link). Đó mới là địa chỉ thật và sd96V.pIsEm.Net là một địa chỉ giả từ Mạc Tư Khoa, Nga – hoàn toàn chẳng có liên quan gì đến Citibank. Kẻ tấn công đã lợi dụng lỗ hổng của trình duyệt web để thực thi liên kết giả. Có 2 khả năng:

Sử dụng ký tự @. Trong liên kết, nếu có chứa ký tự @ thì trình duyệt web (web browser) hiểu thành phần đứng trước ký tự này chỉ là chú thích, nó chỉ thực thi các thành phần đứng sau chữ @. Ví dụ như link trên thì đường dẫn thực sự là sd96V.pIsEm.NeT/3/?3X6CMW2I2uPOVQW.

Sử dụng ký tự %01. Trình duyệt sẽ không hiển thị những thông tin nằm phía sau ký tự này. Ví dụ Tên liên kết . Lúc đó khi đưa trỏ chuột vào Tên liên kết thì trên thanh trạng thái chỉ hiển thị thông tin ở phía trước ký tự %01.

- Với web giả

Nếu nhấn vào liên kết ở email đó nó đưa người sử dụng đến một trang đăng nhập (giả). Dù bên ngoài nó giống hệt trang thật, ngay cả địa chỉ hay thanh trạng thái nhìn cũng có

vẻ thật. Nhưng nếu người sử dụng xem kỹ liên kết trên thanh address bar thì sẽ thấy ở phía sau chữ @ mới là địa chỉ thật. Nếu điền thông tin vào thì sẽ mắc bẫy ngay. Chắc ăn nhất là xem mã nguồn (view source) của trang thì rõ là form thông tin không phải truyền đến citibank mà là đến một nơi khác.

Với cách tiếp cận theo kiểu "biết cách tấn công để phòng thủ" trên, chúng ta sẽ thấy rõ hơn bản chất của một cuộc tấn công phishing – tấn công đơn giản, nhưng hiệu quả thì rất cao. Một khi hiểu được cách thức tấn công thì chắc rằng người dùng cũng sẽ có cách đối phó thích hợp.

- Tóm lại:

+ Cẩn thận với những emal lạ, đặc biệt là những email yêu cầu cung cấp thông tin.

+ Xem kỹ nội dung có chính xác, có giống với những biểu mẫu thường gặp không. Nếu sai chính tả như trên thì phải lưu ý.

+ Nếu có yêu cầu xác nhận thì xem kỹ liên kết, nếu có ký tự là như @ hay %01 thì là giả mạo.

+ Nếu muốn mở một link thì nên tô khối và copy rồi dán vào trình duyệt, và đồng thời phải xem kỹ trên thanh địa chỉ xem liên kết có biến đổi thêm các ký tự lạ như @ hay không.

+ Khi được yêu cầu cung cấp thông tin quan trọng, tốt hơn hết là nên trực tiếp vào website của phía yêu cầu để cung cấp thông tin chứ không đi theo đường liên kết được gửi đến. Cẩn thận hơn thì nên email lại (không reply email đã nhận) với phía đối tác để xác nhận hoặc liên hệ với phía đối tác bằng phone hỏi xem có kêu mình gửi thông tin không cho an toàn.

+ Với các trang xác nhận thông tin quan trọng, họ luôn dùng giao thức http sécure (có s sau http) nên địa chỉ có dạng https://.... chứ không phải là http:// thường. Ngân hàng yêu cầu xác nhận lại hà tiện dùng http:// "thường" thì đó chỉ là mạo danh.

+ Để phân tán rủi ro, mỗi tài khoản nên đặt mật khẩu khác nhau, và nên thay đổi thường xuyên.

+ Nên thường xuyên cập nhật các miếng vá lỗ hổng bảo mật cho trình duyệt (web browser). Cài thêm chương trình phòng chống virus, diệt worm, trojan và tường lửa là không bao giờ thừa.

+ Cuối cùng, và cũng là quan trọng nhất là đừng quên kiểm tra thường xuyên thông tin thẻ ATM, Credit Card, Tài khoản ngân hàng,… xem sự dịch chuyển của luồng tiền vào ra thế nào.

3.2.2. Sniffer

- ✓ **Khái niệm**

Sniffer là một hình thức nghe lén trên hệ thống mạng. Dựa trên những điểm yếu của cơ chế TCP/IP. Hiện nay, khi người dùng sử dụng các dịch vụ web yêu cầu phải đăng nhập ID như mail, tài khoản diễn đàn…v.v. Trong hệ thống mạng LAN hay wirelessLAN, việc bị kẻ xấu sử dụng các chương trình như cain&Abel, wireShark hay Ethereal để capture, thì việc bị lộ ID là điều làm nhiều người đau đầu.

Khởi đầu Sniffer là tên một sản phẩm của Network Associates có tên là Sniffer Network Analyzer. Đơn giản chỉ cần gõ vào từ khoá Sniffer trên bất cứ công cụ tìm kiếm nào,

ta cũng sẽ có những thông tin về các Sniffer thông dụng hiện nay. Sniffer được hiểu đơn giản như là một chương trình cố gắng nghe ngóng các lưu lượng thông tin trên (trong một hệ thống mạng). Tương tự như là thiết bị cho phép nghe lén trên đường dây điện thoại. Chỉ khác nhau ở môi trường là các chương trình Sniffer thực hiện nghe nén trong môi trường mạng máy tính.

Tuy nhiên những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân (binary). Bởi vậy để nghe lén và hiểu được những dữ liệu ở dạng nhị phân này, các chương trình Sniffer phải có tính năng được biết như là sự phân tích các nghi thức (protocol analysis), cũng như tính năng giải mã (decode) các dữ liệu ở dạng nhị phân để hiểu được chúng. Trong một hệ thống mạng sử dụng những giao thức kết nối chung và đồng bộ. Người sử dụng có thể sử dụng Sniffer ở bất cứ Host nào trong hệ thống mạng của người sử dụng. Chế độ này được gọi là chế độ hỗn tạp (promiscuous mode).

Sniffer có hai hình thức: Active - chủ động (switch) và Passive - thụ động (hub.

Các hình thức Sniffer bằng kỹ thuật máy tính nhằm khai thác thông tin riêng tư: Bị nhìn trộm khi gõ Password, bị nghe lén điện thoại, bị đọc trộm thư hay E-mail, bị nhìn trộm nội dung chat.

- ✓ **Sử dụng Sniffer**

Sniffer thường được sử dụng vào hai mục đích khác biệt nhau. Theo hướng tích cự, nó có thể là một công cụ giúp cho các quản trị mạng theo dõi và bảo trì hệ thống mạng của mình. Cũng như theo hướng tiêu cực nó có thể là một chương trình được cài vài một hệ thống mạng máy tính với mục đích đánh hơi, nghe lén các thông tin trên đoạn mạng này... Dưới đây là một số tính năng của Sniffer được sử dụng theo cả hướng tích cực và tiêu cực:

- Tự động chụp các tên người sử dụng (username) và mật khẩu không được mã hoá (clear text password). Tính năng này thường được các hacker sử dụng để tấn công hệ thống.

- Chuyển đổi dữ liệu trên đường truyền để những quản trị viên có thể đọc và hiểu được ý nghĩa của những dữ liệu đó.

- Bằng cách nhìn vào lưu lượng của hệ thống cho phép các quản trị viên có thể phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng. Ví dụ, tại sao gói tin từ máy A không thể gửi được sang máy B.

- Một số Sniffer tiên tiến còn có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng mà nó đang hoạt động (intrusion detecte service).

- Ghi lại thông tin về các gói dữ liệu, các phiên truyền…. Tương tự như hộp đen của máy bay, giúp các quản trị viên có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau sự cố…. phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.

- ✓ **Hoạt động của Sniffer**

Công nghệ Ethernet được xây dựng trên một nguyên lý chia sẻ. Theo một khái niệm này thì tất cả các máy tính trên một hệ thống mạng cục bộ đều có thể chia sẻ đường truyền của hệ thống mạng đó. Hiểu một cách khác tất cả các máy tính đó đều có khả năng nhìn thấy lưu lượng dữ liệu được truyền trên đường truyền chung đó. Như vậy phần cứng Ethernet được xây dựng với tính năng lọc và bỏ qua tất cả những dữ liệu không thuộc đường truyền chung với nó.

Sniffer hoạt động chủ yếu dựa trên phương thức tấn công ARP. Nó thực hiện được điều này trên nguyên lý bỏ qua tất cả những Frame có địa chỉ MAC không hợp lệ đối với nó. Khi Sniffer được tắt tính năng lọc này và sử dụng chế độ hỗn tạp (promiscuous mode). Nó có thể nhìn thấy tất cả lưu lượng thông tin từ máy B đến máy C, hay bất cứ lưu lượng thông tin giữa bất kỳ máy nào trên hệ thống mạng. Miễn là chúng cùng nằm trên một hệ thống mạng.

Quá trình "đầu độc" ARP được diễn ra như sau:

+ Host A và Host B là 2 Máy tính đang "nói chuyện" với nhau

+ Host C là "kẻ Sniffer"

+ Ở Host A trên bảng ARP có lưu địa chỉ IP và MAC tương ứng của Host B

+ Ở Host B trên bảng ARP có lưu địa chỉ IP và MAC tương ứng của Host A

+ Host C thực hiện quá trình nghe lén:

+ Host C gửi các ARP packet tới cả Host A và Host B có nội dung sau: " tôi là A, B, MAC và IP của tôi là XX, YY"

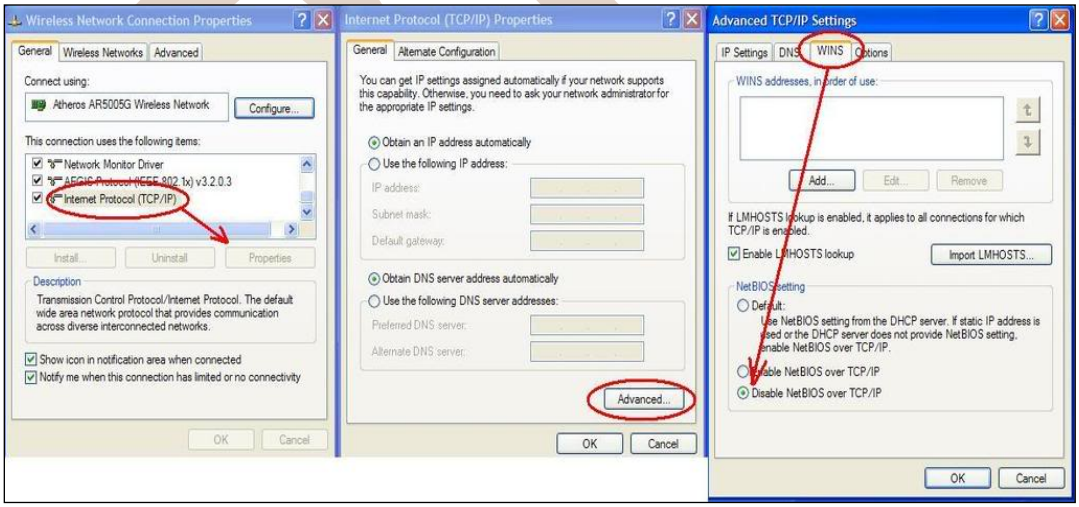
+ Host A nhận lầm Host C là Host B

+ Host B nhận lầm Host C là Host A

= > Quá trình "nói chuyện" giữa Host A và Host B, tất cả thông tin đều bị Host C "nghe thấy".

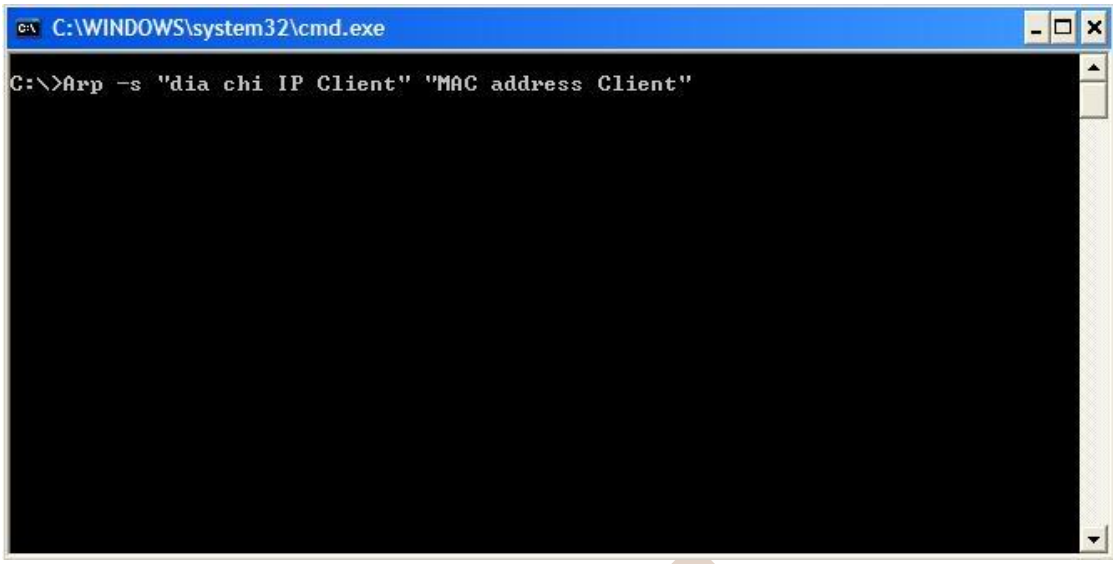
✓ **Cách phòng chống Sniffer**

Thứ nhất: các chương trình thuộc dạng này ban đầu phải quét các địa chỉ IP trong mạng, khi đã có IP rồi thì hacker mới tiến hành sniffer, do đó cách đầu tiên là vô hiệu hóa Netbios name nhằm ngăn cản sự dò tìm IP của các chương trình này (Hình 3.1).

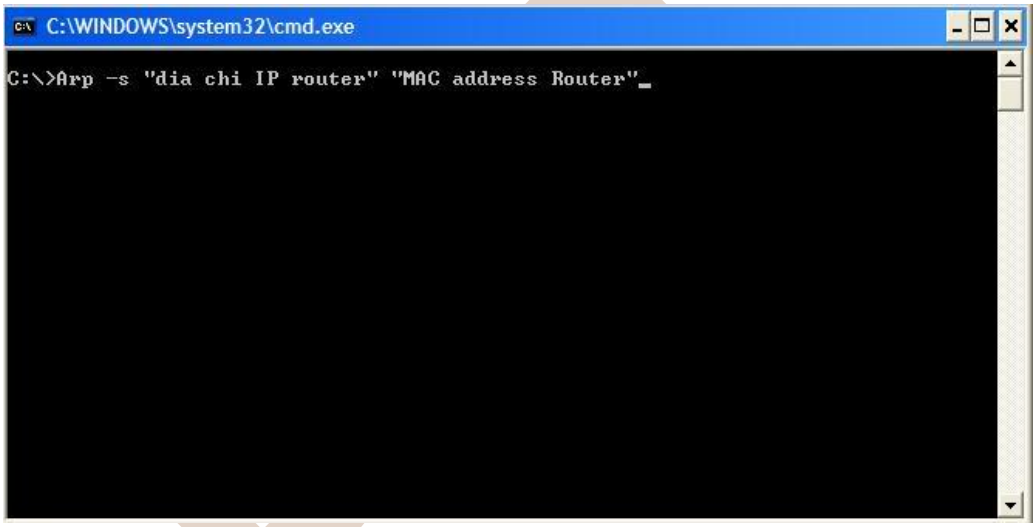


Hình 3.1: Bước 1

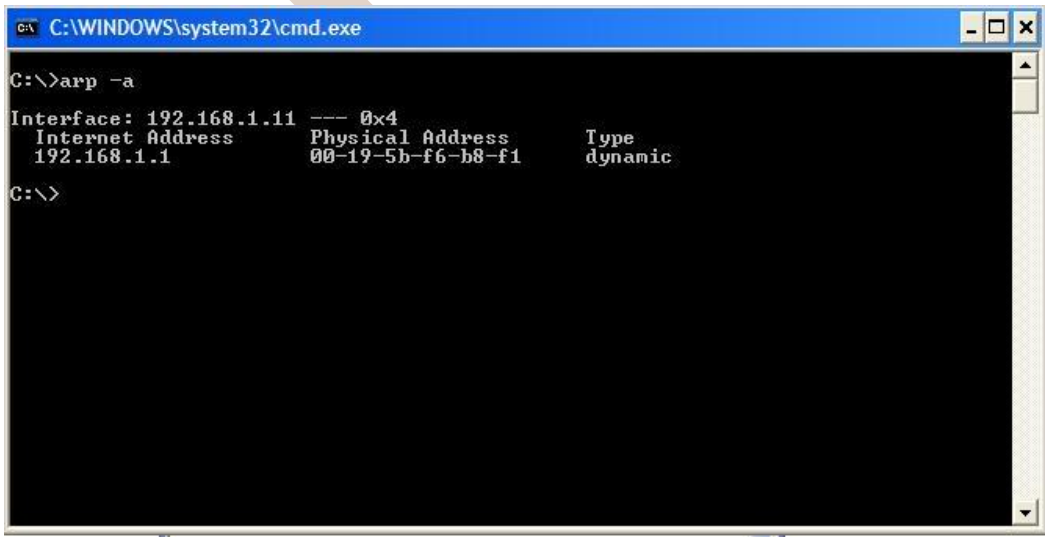
Thứ hai: về mặt cơ cấu thì các chương trình này làm việc dựa trên phương thức thay đổi bảng ARP và tấn công theo kiểu "Man in the midle". Cách khắc phục: khóa cứng bảng ARP và chọn dạng ARP startic, có thể làm việc này trên từng Client, hay có thể config trực tiếp trên Router! để tự bảo vệ mình thì có thể khóa cứng ARP trên máy để tránh bị sniffer.



Hình 3.2: Gõ câu lệnh 1

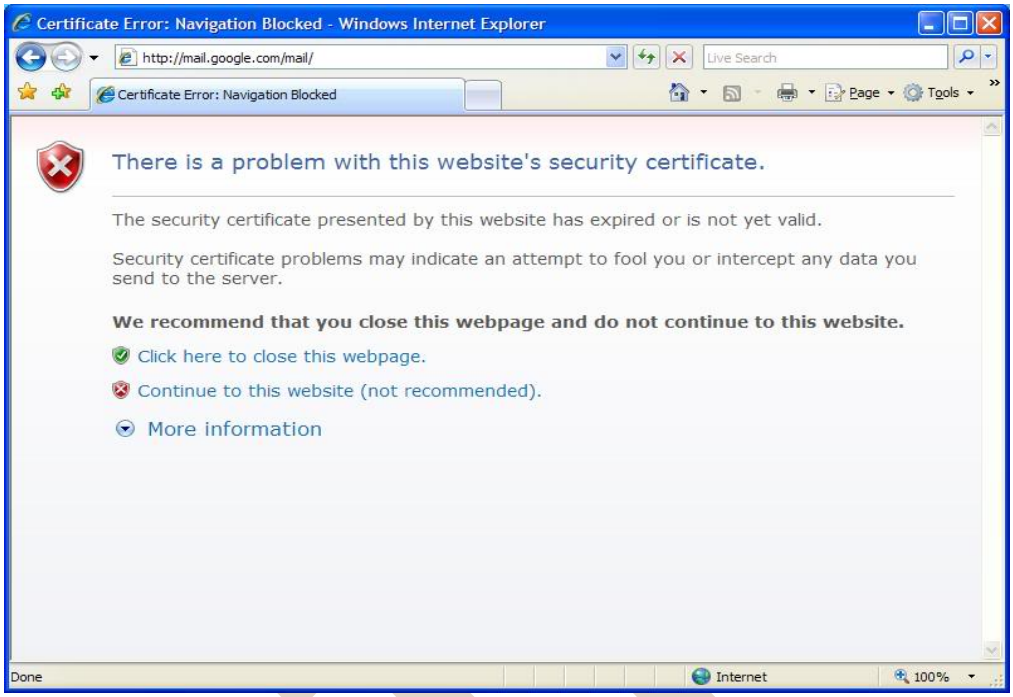


Hình 3.3: Gõ câu lệnh 2



Hình 3.4: Gõ câu lệnh 3

Và đây là dấu hiệu cảnh báo của trình duyệt khi có kẻ nào đó cố tình dùng cain&Abel trong mạng. Cain&Abel thay đổi hay làm giả mạo các CA để phát tới các Victim của nó. Thế nhưng khi các CA này được so sánh với CA mặc định của Windows thì ngay lập tức Windows phát hiện ra sự sai lệch của CA mà nó nhận từ Cain&Abel, Và phát ra thông điệp cảnh báo ngay trên trình duyệt IE khi ta login vào một site sử dụng giao thức https/ (Hình 3.5).



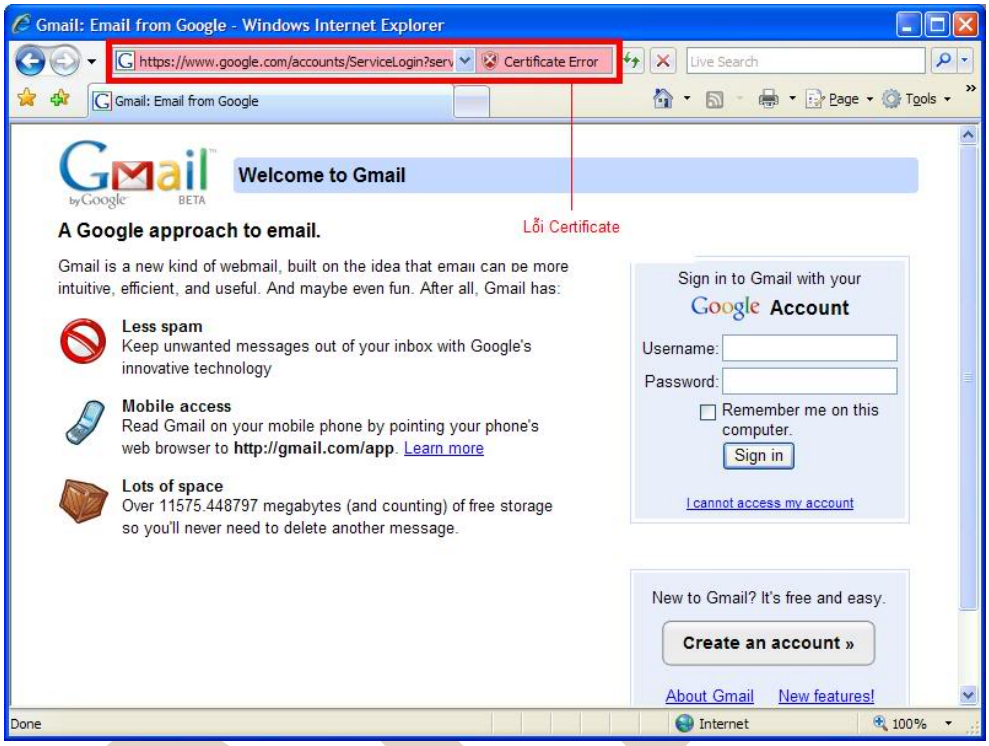
Hình 3.5: Trang web hiển thị

Đây là một thông điệp cảnh báo hết sức rỏ ràng, tuy nhiên người dùng bình thường thì lại không để ý đến cảnh báo bất thường này, và tất nhiên là vẫn vô tư click vào dòng "Continue to this website". Thế nhưng IE lại phát ra một thông điệp khác và thông báo trên ô Address và yêu cầu người dùng kiểm tra CA bằng cách xem lại nó một lần nữa trước khi gõ username và password. Nếu người dùng vẫn vô tư bỏ qua và gõ username, password vào thì coi như cho không cho hacker (Hình 3.6).

Qua một số ví dụ trên, chúng ta nhận thấy các thông tin quan trọng và những tập tin riêng tư có thể bị đánh cắp khá dễ dàng. Để phòng ngừa các trường hợp như vậy, chúng ta không nên tiến hành các hình thức chứng thực username và password dưới dạng văn bản đơn thuần (không mã hóa) mà nên mã hóa chúng bằng IPSéc hay SSL.

Tuy nhiên, không phải lúc nào chúng ta cũng có thể thực hiện được các giải pháp này và cũng không phải lúc nào các giải pháp đó cũng mang lại hiệu quả tốt nhất (vẫn có thể bị các chương trình như dsniff hay ettercap bẻ khoá). Do đó, trong vai trò quản trị mạng, cách tốt nhất là thường xuyên giám sát các hành động bất thường trong hệ thống của mình để đưa ra hành động thích hợp. Như trong trường hợp ở trên, hệ thống bị tấn công do cơ chế giả danh ARP (hay còn gọi bằng thuật ngữ “spoofing arp”) - một giao thức dùng để phân giải địa chỉ vật lý MAC của máy tính. Ta có thể dùng arpwatch giám sát các thông tin arp trong hệ thống để phát hiện khi bị tấn công bằng các phương pháp spoofing arp hay sniffer. Hoặc người sử dụng tiến hành cài đặt các hệ thống IDS như Snort, GFI để phát hiện các hành động bất thường trên mạng.

Thực tế, người sử dụng có thể dùng chính etteracp để dò tìm ra chính nó cũng như các chương trình sniffer khác trên mạng theo phương pháp "dĩ độc trị độc". Ettercap có hai plug-in rất hữu ích, một dùng để tìm kiếm các máy tính chạy chương trình ettercap khác trên mạng và plug-in còn lại dùng để phát hiện các chương trình sniffer khả nghi khác. Ví dụ, nếu nghi ngờ có ai đó đang "nghe lén" trên mạng, người sử dụng khởi động Ettercap và nhấn phím P sau đó chọn plug-in đầu tiên sẽ tìm ra các máy đang chạy Ettercap.



Hình 3.6: Trang web hiển thị hiện trạng

Còn khi đối phương sử dụng các chương trình khác như dSniff, ta có thể dò tìm thông qua plug-in thứ 15 là arpcop, lúc đó một cửa sổ mới sẽ hiển thị những máy tính đang chạy các chương trình spoofing arp trên mạng. Khi xác nhận được đối tượng, ta có thể tiến hành cô lập máy tính này khỏi mạng ngay lập tức bằng cách chọn P và chọn plug-in thứ 23 tên là leech và sau đó chọn Yes, nhấn Enter. Một số người quản trị hệ thống còn dùng ettercap để phát hiện các máy bị nhiễm virus đang phát tán trên mạng rồi cô lập chúng bằng leech sau đó diệt bằng các chương trình chống virus rất hiệu quả.

Tóm lại, cách tốt nhất để giữ an toàn cho hệ thống mạng của mình là nên thường xuyên giám sát hệ thống cũng như có các chính sách để ngăn ngừa các trường hợp gây hại vô tình hay cố ý của người sử dụng. Thông qua việc thực hiện các chính sách hợp lý, chúng ta có thể quy định những chương trình không nên sử dụng cũng như các hành động bị nghiêm cấm, như tiến hành thao tác phân tích gói tin, trừ khi phục vụ cho mục đích đặc biệt để xử lý sự cố mạng.

3.2.3 Keylogger

- ✓ **Khái niệm**

Keylogger hay "trình theo dõi thao tác bàn phím" theo cách dịch ra tiếng Việt là một chương trình máy tính ban đầu được viết nhằm mục đích theo dõi và ghi lại mọi thao tác thực hiện trên bàn phím vào một tập tin nhật ký (*log*) để cho người cài đặt nó sử dụng. Vì chức

năng mang tính vi phạm vào riêng tư của người khác này nên các trình keylogger được xếp vào nhóm các phần mềm gián điệp.

Về sau, khi keylogger phát triển cao hơn nó không những ghi lại thao tác bàn phím mà còn ghi lại cả các hình ảnh hiển thị trên màn hình (screen) bằng cách chụp (screen-shot) hoặc quay phim (screen-capture) thậm chí còn ghi nhận cách con trỏ chuột trên máy tính di chuyển.

✓ **Phân loại keylogger**

Keylogger bao gồm hai loại, một loại keylogger phần cứng và một loại là phần mềm. Phần này đề cập đến loại phần mềm. Theo những người lập trình, keylogger viết ra với chỉ có một loại duy nhất là giúp giám sát con cái, người thân xem họ làm gì với PC, với internet, khi chat với người lạ. Nhưng cách sử dụng và chức năng của keylogger hiện tại trên thế giới khiến người ta thường hay phân loại keylogger theo mức độ nguy hiểm bằng các câu hỏi:

- Nhiễm vào máy không qua cài đặt/Cài đặt vào máy cực nhanh (quick install)?

- Có thuộc tính ẩn/giấu trên trình quản lí tiến trình (process manager) và trình cài đặt và dỡ bỏ chương trình (Add or Remove Program)?

- Theo dõi không thông báo/PC bị nhiễm khó tự phát hiện?

- Có thêm chức năng Capturescreen hoặc ghi lại thao tác chuột?

- Khó tháo gỡ?

- Có khả năng lây nhiễm, chống tắt (kill process)?

Cứ mỗi câu trả lời "có", cho một điểm. Điểm càng cao, keylogger càng vượt khỏi mục đích giám sát (monitoring) đến với mục đích do thám (spying) và tính nguy hiểm nó càng cao. Keylogger có thể được phân loại theo số điểm:

- Loại số 1- Không điểm: keylogger loại bình thường; chạy công khai, có thông báo cho người bị theo dõi, đúng với mục đích giám sát.

- Loại số 2 - Một đến hai điểm: keylogger nguy hiểm; chạy ngầm, hướng đến mục đích do thám nhiều hơn là giám sát (nguy hại đến các thông tin cá nhân như là tài khoản cá nhân, mật khẩu, thẻ tín dụng vì người dùng không biết).

- Loại số 3 - Ba đến năm điểm: keylogger loại rất nguy hiểm; ẩn dấu hoàn toàn theo dõi trên một phạm vi rộng, mục đích do thám rõ ràng.

- Loại số 4 - Sáu điểm: keylogger nguy hiểm nghiêm trọng, thường được mang theo bởi các trojan-virus cực kỳ khó tháo gỡ, là loại keylogger nguy hiểm nhất. Chính vì vậy (và cũng do đồng thời là "đồng bọn" của trojan-virus) nó thường hay bị các chương trình chống virus tìm thấy và tiêu diệt.

✓ **Thành phần của Keylogger**

Thông thường, một chương trình keylogger sẽ gồm có ba phần chính:

- Chương trình điều khiển (Control Program): dùng để theo điều phối hoạt động, tinh chỉnh các thiết lập, xem các tập tin nhật ký cho Keylogger. Phần này là phần được giấu kỹ nhất của keylogger, thông thường chỉ có thể gọi ra bằng một tổ hợp phím tắt đặt biệt.

- Tập tin hook, hoặc là một chương trình monitor dùng để ghi nhận lại các thao tác bàn phím, capture screen (đây là phần quan trọng nhất).

- Tập tin nhật ký (log), nơi chứa đựng/ghi lại toàn bộ những gì hook ghi nhận được.

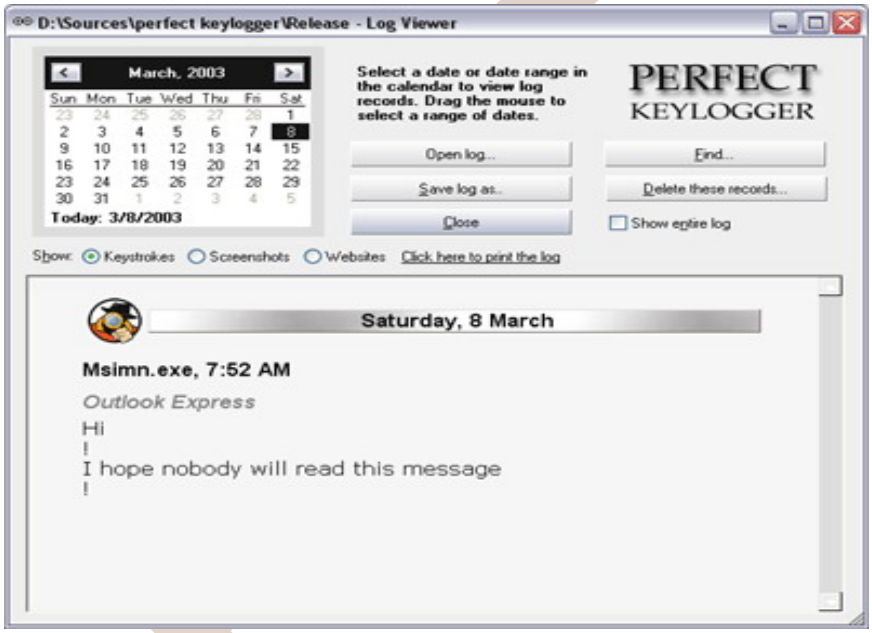
Ngoài ra, tùy theo loại có thể có thêm phần chương trình bảo vệ (guard, protect), chương trình thông báo (report)…

✓ **Cách thức cài đặt vào máy**

Các loại keylogger từ loại 1 - 3 thông thường khi cài đặt vào máy cũng giống như mọi chương trình máy tính khác, đều phải qua bước cài đặt. Đầu tiên nó sẽ cài đặt các tập tin dùng để hoạt động vào một thư mục đặc biệt (rất phức tạp), sau đó đăng ký cách thức hoạt động rồi đợi người dùng thiết lập thêm các ứng dụng. Sau đó nó bắt đầu hoạt động.

Loại keylogger số 4 có thể vào thẳng máy của người dùng bỏ qua bước cài đặt, dùng tính năng autorun để cùng chạy với hệ thống. Một số loại tự thả (drop) mình vào các chương trình khác, để khi người dùng sử dụng các chương trình này keylogger sẽ tự động chạy theo.

Chương trình Perfect Keylogger là một chương trình keylog rất mạnh, hỗ trợ việc theo dõi bàn phím, clipboard, chụp ảnh màn hình và gửi mail tất cả những thứ nó ghi nhận được đến địa chỉ e-mail được chỉ ra (Hình 3.7).



Hình 3.7: Chương trình Perfect Keylogger

✓ **Cách hoạt động**

Trong một hệ thống (Windows, Linux, Mac…), khi bấm một phím trên bàn phím, bàn phím sẽ chuyển nó thành tín hiệu chuyển vào CPU. CPU sẽ chuyển nó tới hệ điều hành để hệ điều hành dịch thành chữ hoặc số cho chính nó hoặc các chương trình khác sử dụng.

Nhưng khi trong hệ thống đó có keylogger, không những chỉ có hệ điều hành theo dõi mà cả hook file/monitor program của keylogger theo dõi nó sẽ ghi nhận và dịch lại các tính hiệu ghi vào tập tin nhật ký. Đồng thời nó còn có thể theo dõi cả màn hình và thao tác chuột.

✓ **Phòng, tránh và chống keylogger**

- Cách phòng ngừa keylogger

Keylogger thường thâm nhập vào máy qua hai con đường chính: được cài đặt hoặc bị cài đặt.

+ Phòng ngừa "được cài đặt":

Phương pháp sau chỉ có tác dụng với chủ máy (người nắm quyền root / administrator) cách tốt nhất là không cho ai sử dụng chung máy tính. Bảo mật máy bằng cách khóa lại bằng các chương trình bảo vệ, hoặc mật khẩu khi đi đâu đó. Nếu phải dùng chung nên thiết lập quyền của người dùng chung đó thật thấp (guest đối với Windows XP, user đối với Linux) để kiểm soát việc cài đặt chương trình của họ.

+ Phòng ngừa "bị cài đặt":

Bị cài đặt là cách để nói đến các trường hợp keylogger vào máy không do người nào đó trực tiếp đưa vào trên máy đó mà do trojan, virus, spyware cài đặt vào máy nạn nhân mà nạn nhân không hề hay biết. Các biện pháp phòng ngừa:

Không tùy tiện mở các tập tin lạ, không rõ nguồn gốc (đặc biệt chú ý các tập tin có đuôi *.exe, *.com, *.bat, *.scr, *.swf, *.zip, *.rar, *.js, *.gif…). Tốt nhất là nên xóa đi, hoặc kiểm tra (scan) bằng một chương trình antivirus và một chương trình antispyware, vì nhiều chương trình antivirus chỉ có thể tìm thấy virus, không thể nhận biết spyware.

Không vào các trang web lạ, đặc biệt là web "tươi mát" vì có thể các trang web này ẩn chứa một loại worm, virus, hoặc là mã độc nào đó có thể âm thầm cài đặt.

Không click vào các đường link lạ do ai đó cho người sử dụng.

Không cài đặt các chương trình lạ (vì nó có thể chứa virus, trojan)

Không download chương trình từ các nguồn không tin cậy. Nếu người sử dụng có thể, xem xét chữ ký điện tử, để chắc chắn chương trình không bị sửa đổi.

Hạn chế download và sử dụng cracked-program.

Luôn luôn tự bảo vệ mình bằng các chương chình chuyên dùng chống virus, chống spyware (antivirus, antispyware) và dựng tường lửa (firewall) khi ở trong Internet.

Thường xuyên cập nhật đầy đủ các bản cập nhật bảo mật của hệ điều hành.

Hoặc chúng ta có thể download một số phần mềm chống keylog về để bảo vệ

- Các tránh keylogger

Khi nghi ngờ nó có keylogger mà không có điều kiện kiểm tra. Thì người dùng có một vài cách sau:

+ Diệt tập tin hook, chương trình theo dõi: Sử dụng một chương trình task manager (có thể gọi ra bằng tổ hợp phím tắt Ctrl+Alt+Del trên Windows) xem các chương trình đang chạy. Nếu người sử dụng thấy process nào lạ (đặc biệt đối với Windows XP là các tập tin được chạy dưới User name không phải là System) chưa thấy bao giờ hãy tắt (end, kill) nó đi. Lưu ý, cách này có thể làm treo hệ thống nếu đó là một tập tin cần cho nó; vì vậy người dùng cần có kinh nghiệm.

+ Che mắt keylogger: Keylogger hoạt động trên nguyên tắc theo dõi bàn phím (monitoring keyboard) chỉ có rất ít có khả năng theo dõi chuột (dù có theo dõi được cũng không chính xác lắm) và có khả năng capture clipboard. Vì vậy dù hệ thống có keylogger (trừ các keylogger có khả năng quay phim) có thể được vượt qua bằng cách sử dụng On-Screen Keyboard (bàn phím trên màn hình) (trong windows gọi ra bằng Start/Run/osk) để nhập cách dữ liệu nhạy cảm (mật khẩu, thẻ tín dụng) bằng cách click chuột. Vì đây là cách nhập liệu nằm ngoài vùng theo dõi của các tập tin hook (vì không qua bàn phím) nên keylogger sẽ không ghi nhận được thông tin gì. Cách này dễ dùng nhưng người khác có thể trông thấy

thông tin được nhập vào (tiếng lóng thường dùng là đá pass) từ đó người sử dụng mất password.

- Cách chống lại keylogger

+ Phương pháp đơn giản: Nhanh hiệu quả nhất là diệt trừ toàn bộ các chương trình đang theo dõi bàn phím đi. Một số chương trình như là Keylogger Killer của Totto quét các process tìm các chương trình theo dõi cùng lúc quá nhiều ứng dụng (keylogger dùng cách này thường bằng một tập tin *.dll) rồi đề nghị người sử dụng tắt nó đi. Thế nhưng một số chương trình tốt (như các chương trình giúp gõ bàn phím Unikey, Vietkey) cũng dùng cách này nên có thể gây diệt lầm.

+ Phương pháp nâng cao: Sử dụng một chương trình chống spyware chuyên dùng. Các chương trình này sẽ tự động quét, phân tích các chương trình đang chạy cũng như trên máy để từ đó nhận biết các chương trình keylogger và tự động diệt. Một số chương trình còn có chế độ bảo vệ thời gian thực (Real-Time Protection) giúp bảo vệ chống ngay khi spyware chuẩn bị cài vào máy.

Điểm gây khó khăn nhất của cách dùng này là đa số các chương trình sử dụng tốt đều phải trả tiền (ví dụ như Spyware Doctor của Pctools, McAfee Antispyware của McAfee, Bitdefender…). Tuy thế vẫn có một số chương trình miễn phí và khá tốt như Ad-Aware SE, Spybot S&D, Spyblaster tuy rằng nó lâu lâu vẫn bắt hụt một số chương trình đặc biệt, nhưng nếu dùng kết hợp (cùng lúc cả hai hoặc cả ba) thi hiệu quả hầu như là hoàn toàn.

Trong một số trường hợp, người dùng chọn cách chống Keylogger theo cách "sống chung với lũ". Lấy ví dụ về Keyscrambler là một trong số những phần mềm bảo vệ máy tính theo phương pháp này. Mọi dữ liệu về phím bấm được truyền đến Hệ điều hành và được Keyscrambler mã hóa trước (do keyscrambler tác động trực tiếp từ phần lõi Kennel), sau đó mới đến các phần mềm khác (bao gồm cả keylogger) và cuối cùng được giải mã lại cho đúng với các phím được gõ. Phương pháp này có thể vô hiệu hóa đa số các loại keylogger hiện tại, không yêu cầu người dùng cập nhật các trình anti-keylogger thường xuyên. Tuy nhiên, nó cũng có những điểm yếu riêng. Nếu keylogger được viết để ghi lại các phím sau khi chúng được giải mã (ví dụ: cài keylogger như là một addon của trình duyệt...) thì xem như đã vô hiệu hóa được keyscrambler, và nó cũng chỉ hỗ trợ một số phần mềm nhất định. Khi dùng chung với các phần mềm gõ tiếng Việt, người dùng sẽ phải tắt KeyScramble đi, đây là một sự phiền phức lớn dù nó minh chứng cho khả năng bảo mật của phần mềm này.

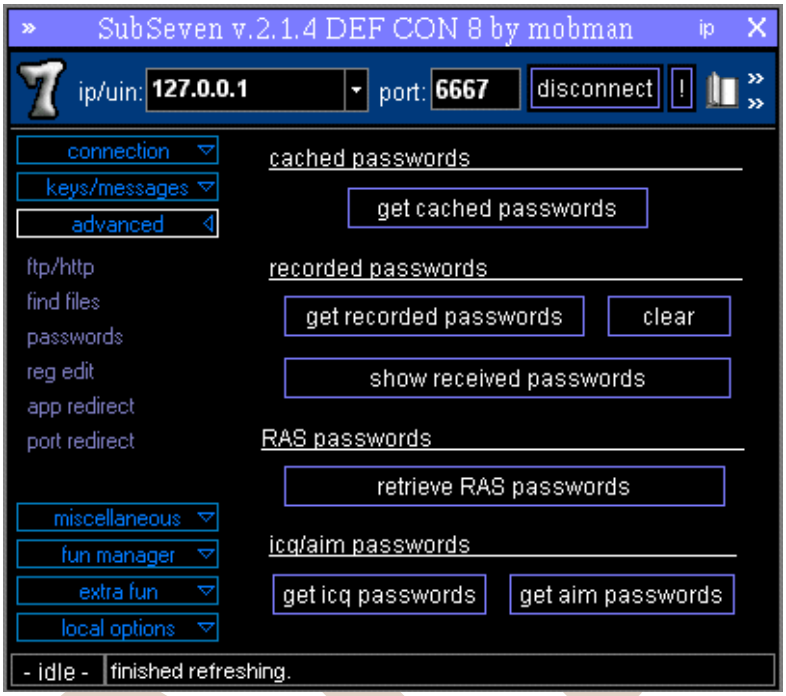
3.2.4. Trojan horse

- ✓ **Khái niệm**

Con ngựa thành Tơ-roa (Trojan horse), nó xuất hiện vào cuối năm 1989, được ngụy trang dưới những thông tin về AIDS. Hơn 10.000 bản sao trên đĩa máy tính, từ một địa chỉ ở Luân Đôn đã được gửi cho những công ty, các hãng bảo hiểm, và các chuyên gia bảo vệ sức khỏe trên khắp châu Âu và Bắc Mỹ. Những người nhận đã nạp đĩa vào máy tính, ngay sau đó họ phát hiện ra đó là một "con ngựa thành Tơ-roa" ác hiểm, đã xóa sạch các dữ liệu trên đĩa cứng của họ. Những con ngựa thành Tơ-roa cũng có thể giả dạng các chương trình trò chơi, nhưng thực chất giấu bên trong một đoạn chương trình có khả năng đánh cắp mật khẩu thư điện tử của một người và gửi nó cho một người khác.

Có rất nhiều cách để lây nhiễm Trojan vào máy người dùng, hacker thường gửi

chương trình Trojan đến các thuê bao cần tấn công thông qua thư điện tử (e-mail) dưới dạng dữ liệu đính kèm (File Attachment). Chỉ cần khi người dùng vô tình mở file này, lập tức Trojan được kích hoạt và tự động sao chép lại tất cả các thông số về mật khẩu của người dùng, không chỉ là mật khẩu truy cập Intemet mà ngay cả đến mật khẩu của hòm thư điện tử cũng dễ dàng bị đánh cắp. Ngay sau khi người dùng kết nối Internet, Trojan sẽ bí mật sinh ra một e- mail và gửi mật khẩu đánh cắp về cho "tin tặc". Và sau đó mỗi lần thay đổi mật khẩu Trojan sẽ tiếp tục lặng lẽ "tuồn" của ăn cắp tới một địa chỉ mà hacker đã định sẵn.



Hình 3.8: Thông tin bị hack

Để đánh lừa "nạn nhân", "tin tặc" luôn tìm cách giăng ra những loại bẫy hết sức tinh vi đến nỗi không ít người dùng dù rất 'kỹ tính" nhưng vẫn cứ "sập" bẫy như thường. Phổ biến nhất là hacker đội lốt những tổ chức hay công ty có uy tín để đánh lừa người dùng bằng chương trình phần mềm thư ma Ghostmail. "Tin tặc" dễ dàng thảo ra những e-mail mạo danh với nội dung: *"Hiện giờ tình trạng đánh cắp mật khẩu thuê bao đang rất phổ biến, nhằm để phòng tránh, chúng tôi xin được gửi tới quý khách chương trình phần mềm Tr-Protect (Trojan sau khi đã đổi tên)".*

Có khi chúng lại "đội lốt" chuyên gia lập trình chương trình diệt virus số một Việt Nam - Nguyễn Tử Quảng: *"Để phòng chống virus Chernobyl 26- 4, chúng tôi hân hạnh gởi tới quý ngài chương trình BKAV 383. Mong quý vị dùng thử Mọi ý kiến đóng góp xin gửi về địa chỉ sau quangnt@it-hut.edu.vn".* Khi nhận được những tin kiểu như vậy, có không ít thuê bao dễ dàng "cắn câu" và cứ "tự nhiên" cho chạy chương trình Trojan mà không hề nhận thức được rằng họ đang "tự nguyện" hiến mình thành nạn nhân của bọn "tin tặc".

Như vậy, khi Trojan được kích hoạt trên máy tính và khi truy cập Internet thì Trojan có thể lấy mật khẩu truy cập mạng, lấy danh sách thư điện tử và thậm chí cả cấu hình máy tính của người sử dụng để gửi cho một địa chỉ thư điện tử của tên tin tặc. Nhưng nguy hiểm hơn, Trojan còn gửi cả địa chỉ mạng IP, là địa chỉ mà nhà cung cấp dịch vụ mạng (ISP) gán cho người sử dụng lúc truy cập; tên tin tặc sẽ sử dụng địa chỉ IP của người sử dụng để thiết lập kết nối từ máy tính của hắn tới máy tính của người sử dụng qua mạng Internet. Trojan sẽ

lấy thông tin, xóa thông tin....v.v.

Các kiểu gây hại:

- Xoá hay viết lại các dữ liệu trên máy tính
- Làm hỏng chức năng của các tệp
- Lây nhiễm các phần mềm ác tính khác như là virus
- Cài đặt mạng để máy có thể bị điều khiển bởi máy khác hay dùng máy nhiễm để gửi thư nhũng lạm
- Đọc lén các thông tin cần thiết và gửi báo cáo đến nơi khác (xem thêm phần mềm gián điệp)
- Ăn cắp thông tin như là mật khẩu và số thẻ tín dụng
- Đọc các chi tiết tài khoản ngân hàng và dùng vào các mục tiêu phạm tội
- Cài đặt lén các phần mềm chưa được cho phép

✓ **Cách thức thực hiện (các thủ đoạn của Hacker)**

- Giả danh nhà cung cấp dịch vụ: Hacker lấy danh nghĩa nhà cung cấp dịch vụ Internet (ISP) gọi điện thoại hoặc gửi e-mail yêu cầu người sử dụng cung cấp password hoặc đổi password theo họ gợi ý. Hacker mail cho người sử dụng một Attached File (tập tin .exe) cho biết là file hỗ trợ sử dụng Internet nhưng thực chất đây là file ăn cắp password.

- Lợi dụng sự tin tưởng khi mượn hoặc sửa chữa máy tính của người sử dụng họ sẽ dễ dàng lấy mật khẩu vì đa số người sử dụng đều thường xuyên Save Password vào máy.

- Cài "gián điệp" (spy) vào máy tính của người sử dụng: Đây là phương thức cổ điển nhưng lại là cách ăn cắp password thông dụng và hiệu quả nhất mà không tốn công sức, thường là file Trojan horse được gởi qua e-mail với những lời mời chào hết sức hấp dẫn, kích thích tò mò. Nếu người sử dụng mở file này thì ngay lập tức máy người sử dụng đã bị nhiễm vi rút và từ đó trở đi, password của người sử dụng được thường xuyên gởi về cho Hacker ngay cả khi người sử dụng thay password mới.

✓ **Cách phòng, chống Trojan**

Để tìm và diệt Trojan, người sử dụng cần tiến hành theo các bước sau:

- Không nên tải và chạy thử những tập tin gắn kèm thư điện tử gửi cho người sử dụng từ những địa chỉ thư điện tử mà người sử dụng không rõ. Cũng vì lý do này mà tác giả của chương trình diệt vi rút thông dụng BKAV đã cảnh báo có nhiều kẻ mạo danh gửi cho người sử dụng chương trình diệt virus mà thực chất là Trojan.

- Sử dụng chương trình phát hiện và diệt Trojan, người sử dụng có thể tìm kiếm trên mạng Internet với từ khóa "Detect and destroy Trojan". Nếu người sử dụng không có sẵn trong tay những chương trình phát hiện và diệt Trojan thì người sử dụng có thể kiểm tra Registry của Window: HKEY - LOCAL - MACHINE\Software\Microsoft\Windows\Current Version\Run.

Nếu thấy có đường dẫn tới một chương trình mà người sử dụng biết là không phải của Window hoặc của các chương trình tiện ích, người sử dụng hãy thoát Window về chế độ DOS và xóa tập tin theo đường dẫn của Registry, vào lại Window và xóa dòng đã ghi trong Registry. Người sử dụng cũng có thể kiểm tra cả tập tin Win.ini, System.ini trong thư mục

C:\Windows sau mục Run hoặc Load.

- Cách phòng chống hữu hiệu nhất là đừng bao giờ mở các đính kèm được gửi đến một cách bất ngờ. Khi các đính kèm không được mở ra thì Trojan horse cũng không thể hoạt động. Cẩn thận với ngay cả các thư điện tử gửi từ các địa chỉ quen biết. Trong trường hợp biết chắc là có đính kèm từ nơi gửi quen biết thì vẫn cần phải thử lại bằng các chương trình chống virus trước khi mở nó. Các tệp tải về từ các dịch vụ chia sẻ tệp như là Kazaa hay Gnutella rất đáng nghi ngờ, vì các dịch vụ này thường bị dùng như là chỗ để lan truyền Trojan horse.

3.2.5. Trộm Cokkies

- ✓ **Khái niệm**

Cookies là những phần tử dữ liệu nhỏ có cấu trúc được chia sẻ giữa website và trình duyệt của người dùng. Cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (size dưới 4KB). Chúng được các site tạo ra để lưu trữ, truy tìm, nhận biết các thông tin về người dùng đã ghé thăm site và những vùng mà họ đi qua trong site. Những thông tin này có thể bao gồm tên, định danh người dùng, mật khẩu, sở thích, thói quen,…v.v.

Cookies được Browser của người dùng chấp nhận lưu trên đĩa cứng của máy tính, không phải Browser nào cũng hỗ trợ cookies. Sau một lần truy cập vào web site, những thông tin về người dùng sẽ được lưu trữ trong cookies. Ở những lần truy cập sau đến site đó, web site có thể dùng lại những thông tin trong cookies (như thông tin liên quan đến việc đăng nhập vào 1 forum …) mà người dùng không phải thực hiện lại thao tác đăng nhập hay phải nhập lại các thông tin khác.

Như vậy, vấn đề đặt ra là có nhiều site quản lý việc dùng lại các thông tin lưu trong cookies không chính xác, kiểm tra không đầy đủ hoặc mã hóa các thông tin trong cookies còn sơ hở giúp hacker khai thác để vượt qua cánh cửa đăng nhập, chiếm quyền điều khiển site. Sau khi đã được lưu lại trên đĩa cứng, cookies không bị mất đi khi người dùng rời khỏi trang web đó hoặc tắt máy tính.

Nescape là trình duyệt đầu tiên sử dụng cookies, tiếp đến là Internet Explorer (IE) của Microsoft. Cookies của trình duyệt IE được đặt trong *Document and Settings\Username\Cookies\username@sitename.txt*. Việc lưu trữ và dùng lại các thông tin đăng nhập được lưu trong Cookies giúp người dùng tiết kiệm được thời gian trong việc duyệt các site. Tuy nhiên, Cookies là một trong những nguyên nhân gây tiết lộ thông tin riêng tư của người dùng.

Ví dụ: Một hacker làm việc ở một ngân hàng, có thể anh ta tìm cách xem thông tin cookies của khách hàng và sử dụng thông tin này truy cập vào tài khoản của khách hàng đó hoặc một hacker có thể tìm cách trộm cookies của một admin của một website. Từ đó, có toàn quyền truy cập và điều khiển website. Ngoài ra những người tấn công cũng có thể hack một vài forum bằng cách khai thác thông tin trong cookies. Những Browser hiện nay cho phép người dùng khóa cookies lại và thiết lập chế độ hỏi lại họ trước khi lưu lại cookies trên hệ thống. Bên cạnh đó còn có một số phần mềm giúp người dùng quản lý cookies, chúng giúp ngăn chặn hoặc cảnh báo những nguy cơ có thể gây hại cho hệ thống.

Cookies nói chung là lưu trong máy hết, với IE thì lưu trong thư mục Temporary Internet Files. Xem COOKIES: *Chọn Tool > Internet Options > Tab General nhấn chọn Settings > View files.*

✓ **Cách phòng chống**

- Không nên đánh dấu vào trước dòng chữ *Remember my ID on this computer* để không lưu dấu tích của người sử dụng trong Cookie.

- Khi rời khỏi máy tính nên xoá Cookie đi bằng cách: Mở IE, kích chuột vào *Tools, Internet Options, Gerneral, Delete Cookie.* Và cuối cùng, người sử dụng kích chuột vào OK.

3.3 Các biện pháp bảo mật trong thanh toán điện tử

3.3.1 Kiểm soát truy cập và xác thực

3.3.1.1 Khái niệm

- Kiểm soát truy cập xác định ai (người hoặc máy) được sử dụng hợp pháp các tài nguyên mạng và những tài nguyên nào họ được sử dụng. Còn tài nguyên có thể là bất kỳ cái gì: các trang Web, các file văn bản, cơ sở dữ liệu, các ứng dụng, các máy chủ, máy in, hoặc các nguồn thông tin, các thành phần mạng khác.

- Xác thực là quá trình kiểm tra xem người dùng có đúng là người xưng danh hay không. Việc kiểm tra thường dựa trên một hoặc nhiều đặc điểm phân biệt người đó với những người khác.

3.3.1.2 Các phương pháp kiểm soát truy cập và xác thực

✓ **Mật khẩu**

Mật khẩu là việc sử dụng các ký tự trên bàn phím để thiết lập quyền truy cập.

✓ **Thẻ (Token)**

Token (thẻ) được hiểu là một thiết bị để lưu trữ thông tin. Mức độ bảo mật cao hơn mật khẩu, đạt được dựa trên việc kết hợp một cái gì đó mà chỉ một người biết với một cái gì đó mà người đó có. Kỹ thuật đó được biết đến như xác thực hai yếu tố.

- Token bị động

Thẻ bị động là một thiết bị lưu trữ có chứa mã bí mật. Phần lớn thẻ bị động là thẻ nhựa có gắn dải từ. Người dùng cà thẻ bị động vào một đầu đặt gắn kết với máy tính hoặc trạm công tác, sau đó nhập mật khẩu và nhận được quyền truy cập vào mạng.

- Token chủ động

Là một thiết bị điện tử nhỏ độc lập có khả năng sinh ra mật khẩu một lần và người dùng sử dụng mật khẩu này để truy cập.

Token hoạt động theo phương thức tự tạo các dãy mã số một cách ngẫu nhiên (gồm 06 chữ số hiện ra trên màn hình phía trên Token) và thay đổi liên tục trong một khoảng thời gian nhất định (30 giây hoặc 60 giây). Cơ chế bảo mật của mỗi Token chính là mã số được tạo ra liên tục, duy nhất, đồng bộ hoá và xác thực bởi máy chủ.

✓ **Hệ thống sinh trắc trong xác thực**

- Quét dấu vân tay

Dựa trên sự đo đạc các đường không liên tục trong vân tay của một người. Xác suất trùng dấu vân tay là khoảng 1 phần tỷ. Hiện các thiết bị quét dẫu vân tay gắn với máy tính được cung cấp với giá không cao.

- Quét mống mắt

Mống mắt là phần có màu của mắt bao quanh đồng tử. Mống mắt có một số vết đặc biệt có thể được camera nghi nhận ở khoảng cách 3-10 inches so với mắt. Các vết đặc biệt đó có thể tạo nên một mẫu dạng sinh trăc học dùng để so sánh khi nhận dạng.

- Ghi giọng nói

Mỗi người có những đặc điểm khác nhau trong giọng nói như cường độ, tần số, nhịp điệu…, và các đặc điểm này qua một quy trình nhất định, được số hóa và tạo thành các mẫu dạng lưu trữ trong cơ sở dữ liệu và sử dụng để so sánh khi thiết bị scan giọng nói của đối tượng. Trong phần lớn các hệ thống nhận dạng giọng nói, người dùng nói vào microphone hoặc telephone. Lời nói thường là số nhận dạng (ID) hoặc mật khẩu của người dùng. Lần sau, khi người dùng muốn truy cập hệ thống, sẽ nhắc lại những lời đã nghi âm. Thiết bị để ghi giọng nói khá phổ biến và rẻ.

- Kiểm tra qua thao tác gõ bàn phím

Kiểm tra qua thao tác gõ bàn phím dựa trên giả thiết rằng cách thức mà người dùng gõ các từ trên bàn phím (áp lực, tốc độ, nhịp độ) là khác nhau giữa người này so với người khác, được ghi nhận và qua một quy trình nhất định, được số hóa và tạo thành các mẫu dạng lưu trữ trong cơ sở dữ liệu và sử dụng để so sánh. Cũng tương tự như trường hợp trước, từ được nhập thường là số nhận dạng (ID) hoặc mật khẩu của người dùng. Trở ngại chủ yếu khi sử dụng phương pháp này là cách thức mà người dùng gõ các từ trên bàn phím không ổn định trong các lần gõ khác nhau.

3.3.2 Mã hóa

Mã hoá thông tin là quá trình chuyển các văn bản hay các tài liệu gốc thành các văn bản dưới dạng mật mã để bất cứ ai, ngoài người gửi và người nhận, đều không thể đọc được.

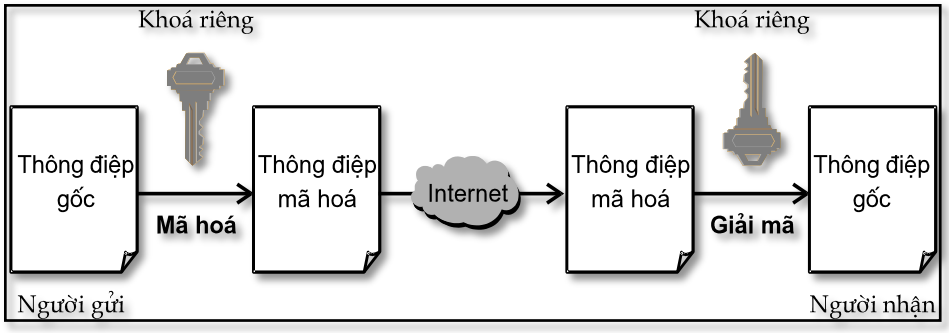
Mục đích của mã hóa thông tin là: Đảm bảo tính toàn vẹn của thông điệp, khả năng chống phủ định, đảm bảo tính xác thực, đảm bảo tính bí mật của thông tin. Hai kỹ thuật mã hóa cơ bản được dùng là: mã hóa khóa đối xứng (mã hóa khóa đơn) và mã hóa khóa bất đối xứng (mã hóa khóa công khai).

3.3.2.1 Mã hóa đối xứng

✓ **Khái niệm**

Mã hoá khoá bí mật, còn gọi là mã hoá đối xứng hay mã hoá khoá riêng, là sử dụng một khoá cho cả quá trình mã hoá (được thực hiện bởi người gửi thông tin) và quá trình giải mã (được thực hiện bởi người nhận).

✓ **Quá trình mã hóa**



Hình 3.9 : Quy trình mã hóa khóa đối xứng

Ví dụ Bob (người gửi) gửi cho Alice (người nhận) một đơn hàng và chỉ muốn Alice đọc được vì thế Bob đã mã hóa đơn hàng bằng một mã khóa và gửi đơn hàng đã mã hóa đó cho Alice. Và Alice khi nhận được đơn hàng thì sẽ giải mã bằng chính mã khóa đó. Điều đáng chú ý là trong kỹ thuật mã hoá khoá bí mật, khoá để mã hoá thông điệp và khoá để giải mã thông điệp giống như nhau

✓ **Ưu điểm**

- Đơn giản, dễ sử dụng
- Quá trình mã hóa và giải mã nhanh chóng
- Sử dụng để mã hoá những dữ liệu lớn (hàng loạt)

✓ **Nhược điểm**

- Dễ bị phá (bị tấn công) do dùng chung một khóa

Vì dùng chung 1 khóa cho quá trình mã hóa và giải mã đơn giản, vì vậy rất dễ bị phá trong quá trình truyền tin. Rõ ràng khi hệ thống đã ko thể truyền tin trên một kênh truyền an toàn thì ko thể đảm bảo được việc truyền khóa bí mật từ người gửi đến người nhận là an toàn.

- Không dùng cho mục đích xác thực, hay chống phủ nhận được

Vì chỉ có 1 khóa, thuật toán như nhau, nên không xác định được người gửi và nhận.

- Chi phí tốn kém

Rất khó có thể thực hiện việc phân phối an toàn các mã khoá bí mật với hàng ngàn khách hàng trực tuyến của mình trên những mạng thông tin rộng lớn. Và doanh nghiệp sẽ phải bỏ ra những chi phí không nhỏ cho việc tạo một mã khoá riêng và chuyển mã khoá đó tới một khách hàng bất kỳ trên Internet khi họ có nhu cầu giao dịch với doanh nghiệp.

- Khó khăn trong vấn đề tạo lập, phân phối, lưu trữ và quản lý khóa

Trong mô hình mã hóa đối xứng, việc bảo mật và phân phối khóa là công việc khó khăn, phức tạp nhất. Như vậy tính bảo mật của phương pháp mã hóa này sẽ phụ thuộc vào việc giữ bí mật của khóa. Nhưng khóa thường được truyền trong môi trường truyền tin nên rất dễ bị bẻ khóa.

Các bên tham gia trong quá trình mã hoá cần phải tin tưởng nhau và phải chắc chắn rằng bản sao của mã hoá đang được các đối tác bảo vệ cẩn mật. Thêm vào đó, nếu người gửi và người nhận thông điệp ở hai nơi khác nhau, họ phải đảm bảo rằng, khi họ gặp mặt hoặc sử dụng một phương tiện thông tin liên tác chung (hệ thống điện thoại, dịch vụ bưu chính...) để trao mã khoá cho nhau không bị người khác nghe trộm hay bị lộ mã khoá, bởi vì nếu như vậy, những người này sau đó có thể sử dụng mã khoá để đọc lén các thông điệp mà các bên gửi cho nhau.

Để có thể dễ dàng đảm bảo an toàn cho các giao dịch trên Internet cần có những kỹ thuật mã hoá khác thuận tiện và hiệu quả hơn, nhằm khắc phục những nhược điểm của mã hóa khóa bí mật và kỹ thuật mã hoá khoá công khai đã ra đời.

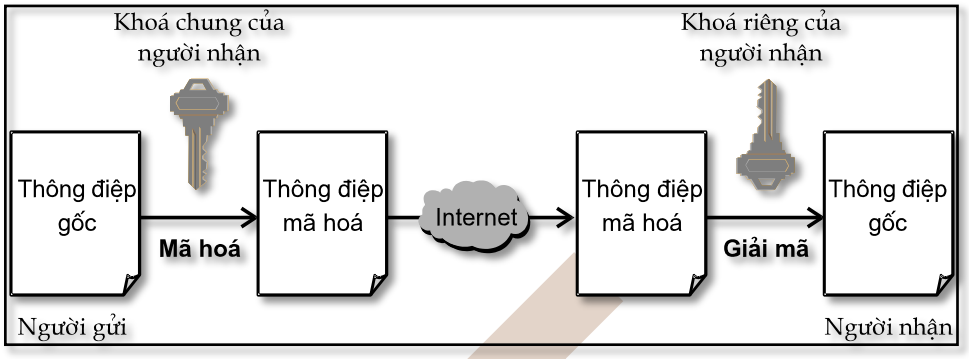
3.3.2.2 Mã hóa bất đối xứng

✓ **Khái niệm**

Khác với khoá bí mật, mã hoá khoá công khai (còn gọi là mã hoá bất đối xứng) sử dụng hai mã khoá trong quá trình mã hoá: một mã khoá dùng để mã hoá thông điệp và một mã khoá khác dùng để giải mã. Hai mã khoá này có quan hệ với nhau về mặt thuật toán sao cho dữ liệu được mã hoá bằng khoá này sẽ được giải mã bằng khoá kia.

✓ **Quá trình mã hóa**

Như vậy thực chất, phương pháp mã hoá này dùng một cặp mã khoá cho quá trình mã hoá: một mã khoá gọi là mã khoá công cộng (khóa chung) và một là mã khoá riêng. Mã khoá công cộng là mã khoá có thể công khai cho nhiều người biết, còn mã khoá riêng được giữ bí mật và chỉ mình chủ nhân của nó được biết. Tất nhiên, cả hai mã khoá này đều được bảo vệ tránh bị đánh cắp hoặc thay đổi.



Hình 3.10 : Quy trình mã hóa khóa bất đối xứng

Ví dụ: Bob (người gửi) muốn gửi thư cho Anne (người nhận) thì đầu tiên Bob phải tìm khóa công khai của Anne, và Bob sử dụng khóa công khai này để mã hóa bức thư mà Bob muốn gửi cho Anne. Anne sau khi nhận được thư của Bob thì sử dụng khóa riêng (khóa bí mật) của mình để giải mã và mở được thư của Bob gửi.

✓ **Ưu điểm**

- Đảm bảo tính toàn vẹn thông tin (Mã hóa khóa công khai giúp đảm bảo tính toàn vẹn thông điệp vì cho dù nó bị những kẻ tội phạm chặn lại trên đường truyền, chúng cũng không thể đọc được nội dung thông điệp vì không có mã khoá riêng do chủ nhân đích thực của cặp khoá cất giữ.)

- Độ an toàn và tin cậy cao.

- Không cần phải phân phối khóa giải mã (khóa cá nhân) của mình như trong mã hóa đối xứng.

Đơn giản trong việc lưu chuyển khóa vì chỉ cần đăng ký 1 khóa công khai và mọi người sẽ lấy khóa này về để trao đổi thông tin với tất cả mọi người.

- Gửi thông tin mật trên đường truyền không an toàn mà không cần thỏa thuận khóa từ trước.

- Tạo và cho phép nhận dạng chữ ký số và do đó được dùng để xác thực (authentication) hay chống phủ nhận (non repudiation).

✓ **Nhược điểm**

- Tốc độ mã hóa và giải mã chậm.

- Sử dụng đối với những ứng dụng có nhu cầu mã hoá nhỏ hơn như mã hoá các tài liệu nhỏ hoặc để ký các thông điệp

3.3.2.3 Hạ tầng khóa công khai PKI

✓ **Khái niệm PKI và mục đích**

Nền tảng cho mọi phương thức truyền thông là một cơ chế tin cậy mặc dù truyền

thông dựa vào phương thức vật lý hay là điện tử. Đối với việc truyền thông vật lý thì việc xây dựng cơ chế tin cậy là dễ dàng hơn khi bạn có thể phân biệt mọi người với nhau thông qua khuôn mặt hoặc các giấy tờ khác nhau như chữ ký, chứng minh nhân dân. Tuy nhiên, đối với việc truyền thông điện tử, xây dựng cơ chế tin cậy là công việc khá khó khăn khi phải định danh những thực thể không xác định. Do vậy, các nhà khoa học đã xây dựng một cơ chế tin cậy là hạ tầng khóa công khai – Public Key Infrastructure (PKI).

Ở phần trên khi bàn về mã hóa khóa công khai, còn 1 số vấn đề cần giải quyết:

- Khi người gửi sử dụng khóa công khai của người nhận để mã hóa và gửi thông tin, mặc dù người nhận có thể sử dụng khóa bí mật của họ để mở và đọc thông tin nhưng người nhận hoàn toàn không thể chắc chắn người gửi là ai?

- Khi người gửi "ký" vào bản tin bằng khóa bí mật của mình, sau đó người nhận giải mã bản tin bằng khóa công khai của người gửi, khi đó người nhận đọc được thông tin nhưng người nhận không thể chắc chắn được rằng khóa công khai đang sử dụng thực sự là của ai vì không ai xác nhận rằng đối tượng khóa công khai này là của đối tương nào.

Cơ sở hạ tầng khóa công khai PKI sẽ giải quyết vấn đề này. Theo X.509 PKIX15 định nghĩa: *"PKI là một hệ thống bao gồm phần cứng, phần mềm, dịch vụ, chuẩn định dạng, giao thức, quy trình, chính sách để giúp đảm bảo an toàn, tin cậy cho các phiên truyền thông"*. PKI đáp ứng các yêu cầu về xác thực, bảo mật, toàn vẹn, chống chối từ cho các thông điệp được trao đổi.

Trong mật mã học, hạ tầng khóa công khai (tiếng Anh: public key infrastructure, viết tắt PKI) là một cơ chế để cho một bên thứ 3 (thường là nhà cung cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa công khai/khóa bí mật. Các quá trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm phối hợp khác tại các địa điểm của người dùng. Khóa công khai thường được phân phối trong chứng thực khóa công khai.

✓ **Vai trò, chức năng**

PKI cho phép những người tham gia xác thực lẫn nhau. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa và định danh người dùng. Nhờ vậy người dùng có thể sử dụng trong một só ứng dụng như:

- Mã hóa, giải mã văn bản

- Xác thực người dùng ứng dụng

- Mã hóa email hoặc xác thực

- Tạo chữ ký số trên văn bản điện tử

Một PKI phải đảm bảo được các tính chất sau trong một hệ thống trao đổi thông tin: Tính bí mật, tính toàn vẹn, tính xác thực, tính chống từ chối

✓ **Thành phần cơ bản của PKI**

Dưới góc độ các hoạt động quản lý hệ thống PKI, những đối tượng tham gia vào hệ thống PKI bao gồm: các đối tượng sử dụng (EE), các đối tượng quản lý thẻ xác nhận (CA) và các đối tượng quản lý đăng ký (RA) và các hệ thống lưu trữ.

- Thực thể cuối – Đối tượng sử dụng (EE – End Entity)

Là đối tượng sử dụng chứng nhận (chứng thư số): có thể là một tổ chức, một người cụ thể hay một dịch vụ máy chủ.

- Tổ chức chứng nhận CA (Certificate Authority)

Là cơ quan chuyên cung cấp và xác thực chứng chỉ số. CA có chức năng:

+ Có nhiệm vụ phát hành, quản lý và hủy bỏ các chứng thư số

+ Là thực thể quan trọng trong một PKI và được thực thể cuối tin cậy

+ Gồm tập hợp các con người và các hệ thống máy tính có độ an toàn cao.

- Tổ chức đăng ký chứng nhận RA (Registration Authority)

Là một cơ quan thẩm tra trên mạng máy tính, xác minh các yêu cầu của người dùng muốn sử dụng hoặc xác thực một chứng chỉ số và sau đó yêu cầu CA đưa ra kết quả. Mục đích chính của RA là để giảm tải công việc của CA. Chức năng thực hiện của một RA cụ thể sẽ khác nhau tùy theo nhu cầu triển khai PKI nhưng chủ yếu bao gồm các chức năng sau:

+ Được ủy quyền và có quyền thực hiện công việc mà CA cho phép

+ Tiếp nhận thông tin đăng ký chứng nhận

+ Gắn kết giữa khóa công khai và định danh của người giữ chứng nhận

+ Xác thực cá nhân, chủ thể đăng ký chứng thư số.

+ Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.

+ Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số được yêu cầu.

+ Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không, điều này thường được đề cập đến như sự chứng minh sở hữu.

+ Tạo cặp khóa bí mật, công khai.

+ Phân phối bí mật được chia sẻ đến thực thể cuối (ví dụ khóa công khai của CA).

+ Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.

+ Lưu trữ khóa riêng.

+ Khởi sinh quá trình khôi phục khóa.

+ Phân phối thẻ bài vật lý (thẻ thông minh).

- Hệ thống lưu trữ chứng nhận CR (Certificate Repository)

Hệ thống lưu trữ chứng nhận CR có chức năng:

+ Hệ thống (có thể tập trung hoặc phân tán) lưu trữ chứng thư và danh sách các chứng thư bị thu hồi.

+ Cung cấp cơ chế phân phối chứng thư và danh sách thu hồi chứng thư (CRLs – Certificate Revocatio Lists).

- Chứng chỉ số

Chứng chỉ số là một tệp tin điện tử được sử dụng để nhận diện một cá nhân, một máy chủ, một công ty…trên Internet. Giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ nhận diện cá nhân thông thường khác, chứng chỉ số cung cấp bằng chứng cho sự nhận diện của một đối tượng.

Để có chứng minh thư, bạn 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 bạn là chính xác, được gọi là Nhà cung cấp chứng thực số (Certificate 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 mình cấp.

- Ủy quyền xác nhận hợp lệ - Validation Authority (VA)

Validation Authority (VA) – Ủy quyền xác nhận hợp lệ: Xác nhận tính hợp lệ thẻ chứng thực số của một đối tác trao đổi thông tin. Hoặc VA là một thực thể cung cấp dịch vụ được sử dụng để xác minh tính hợp lệ của chứng chỉ kỹ thuật số theo các cơ chế được mô tả trong tiêu chuẩn X.509 và RFC 5280

3.3.3 Chữ ký điện tử

3.3.3.1 Khái niệm

Trong giao dịch điện tử hiện nay trên thế giới, chữ ký số là hình thức chữ ký điện tử phổ dụng nhất. Tại Việt Nam xu hướng phát triển và ứng dụng chữ ký số đang ngày càng trở nên phổ biến.

Chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách lô gíc với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.

Chữ ký số không phải là hình ảnh số hóa của chữ ký tay, cũng ko phải là một nhận dạng cá nhân hay một mật khẩu mà là một dữ liệu đính kèm vào một thông điệp điện tử. Dữ liệu này được tạo lập bằng cách sử dụng phương thức mã hóa khóa công khai.

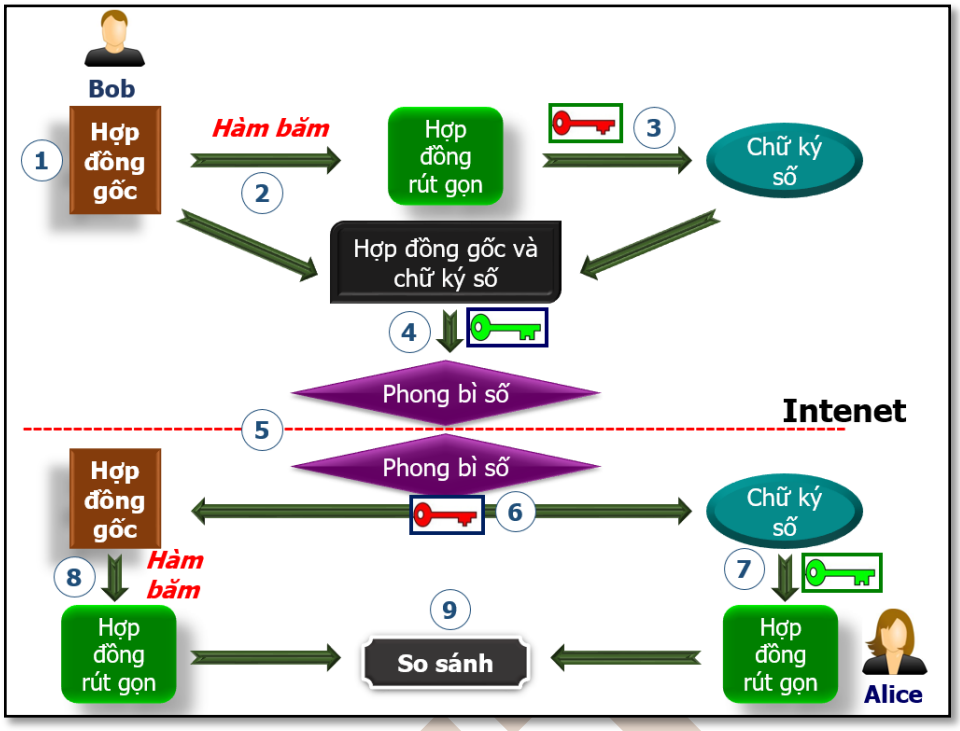
Theo Điều 3, Khoản 4, NĐ 26/2007/NĐ-CP, *"Chữ ký số là một dạng chữ ký điện tử được tạo lập bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: Việc biến đổi nêu trên được tạo ra bằng đúng khó bí mật tương tứng với khóa công khai trong cùng cặp khóa và sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện biến đổi nêu trên."*

Ứng dụng chữ ký số sẽ đảm bảo được 2 vấn đề: tính xác thực của người ký, đảm bảo tính toán vẹn của thông tin.

Chữ ký số về bản chất là một thông điệp dữ liệu (file text, tập hợp các ký tự hoặc một loại thông điệp dữ liệu nhất định do phần mềm ký số sinh ra dựa trên các thuật toán nhất định). Công thức để sinh ra chữ ký số phụ thuộc vào ba yếu tố đầu vào: (i) bản thân văn bản điện tử cần ký (ii) khóa bí mật (private key) và (iii) phần mềm để ký số. Khóa bí mật đơn giản có thể là một mật khẩu (password) hoặc một thông điệp dữ liệu. Phần mềm ký số là phần mềm có chức năng tạo ra các chữ ký số từ hai yếu tố là văn bản cần ký và khóa bí mật và gắn chữ ký số được tạo ra vào thông điệp gốc. Trong các quy trình ký số hiện nay, quy trình phổ biến nhất là sử dụng công nghệ khóa công khai (PKI).

3.3.3.2 Quy trình gửi thông điệp và sử dụng chữ ký số

Dưới đây là quy trình gửi thông điệp và sử dụng chữ ký số. Trong quy trình, phong bì số là kỹ thuật kết hợp giữa mã hóa khóa công khai và chữ ký số. Trong thực tế để đảm bảo độ tin cậy về nội dung thông tin và nguồn gốc trong các giao dịch điện tử, người ta sẽ sử dụng kỹ thuật phong bì số (Hình 3.11).



Hình 3.11: Quy trình gửi thông điệp và sử dụng chữ ký số

- Bước 1: Tạo một hợp đồng gốc.

- Bước 2: Sử dụng hàm băm (thuật toán Hash) để chuyển từ hợp đồng gốc sang hợp đồng rút gọn.

- Bước 3: Người gửi sử dụng khóa riêng để mã hóa hợp đồng rút gọn. Hợp đồng rút gọn sau khi được mã hóa gọi là chữ ký số.

- Bước 4: Người gửi mã hóa cả hợp đồng gốc và chữ ký số sử dụng khóa công khai của người nhận. Hợp đồng gốc và chữ ký số sau khi được mã hóa gọi là phong bì số.

- Bước 5: Người gửi gửi phong bì số hóa cho người nhận

- Bước 6: Khi nhận được phong bì số hóa, người nhận sử dụng khóa riêng của mình để giải mã phong bì số và nhận được hợp đồng gốc và chữ ký số của người gửi.

- Bước 7: Người nhận sử dụng khóa công khai của người gửi để nhận dạng chữ ký số của người gửi (là thông điệp đã được mã hóa bằng hàm Hash).

- Bước 8: Người nhận sử dụng thuật toán băm để chuyển hợp đồng gốc thành hợp đồng rút gọn số như ở bước 2 mà người gửi đã làm.

- Bước 9: Người nhận so sánh thông điệp số vừa tạo ra ở bước 8 với thông điệp số nhận được ở bước 6 (nhận được sau khi giải mã phong bì số).

3.3.4 Các giao thức đảm bảo an toàn

3.3.4.1 SSL (Sécure Sockets Layer)

Trong TMĐT, các giao dịch được thực hiện chủ yếu thông qua mạng Internet, một mạng truyền thông mở, vì vậy, thông tin thương mại giữa các bên rất dễ bị kẻ xấu lấy trộm và sử dụng vào những mục đích bất chính. Giải pháp cơ bản giải quyết vấn đề này là sử dụng giao thức lớp ổ cắm an toàn (SSL - Sécure Sockets Layer).

Lớp ổ cắm an toàn là một chương trình an toàn cho việc truyền thông trên web, được

hãng Netscape Communication phát triển năm 1994 như là một phương pháp bảo đảm sự an toàn của kết nối khách (client) – chủ (server) trên môi trường Internet. Ngày nay giao thức Sécure Socket Layer (SSL) đã được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hoá thông tin.

✓ **Khái niệm**

SSL là công nghệ để mã hóa việc truyền dữ liệu giữa trình duyệt web và máy chủ web giúp cho việc truyền thông tin qua mạng được thực hiện một cách an toàn và bảo mật. Công nghệ này được sử dụng thường xuyên bởi các trang web ngân hàng trực tuyến và trang web TMĐT.

✓ **Đặc điểm**

- SSL được tích hợp sẵn vào các Web browser và Web server, cho phép người sử dụng làm việc với các trang Web ở chế độ an toàn với 3 nhiệm vụ chính: xác thực server, xác thực client, mã hóa kết nối.

- Địa chỉ web được bảo mật bằng SSL bắt đầu với https: thay vì http: với biểu tượng ổ khóa màu xanh lá cây.

- Để bảo vệ những thông tin mật trên mạng Internet hay bất kỳ mạng TCP/IP nào, SSL đã kết hợp những yếu tố sau để thiết lập được một giao dịch an toàn:

+ Xác thực: đảm bảo tính xác thực của trang web mà bạn sẽ làm việc ở đầu kia của kết nối. Cũng như vậy, các trang Web cũng cần phải kiểm tra tính xác thực của người sử dụng.

+ Mã hoá: đảm bảo thông tin không thể bị truy cập bởi đối tượng thứ ba. Để loại trừ việc nghe trộm những thông tin "nhạy cảm" khi nó được truyền qua Internet, dữ liệu phải được mã hoá để không thể bị đọc được bởi những người khác ngoài người gửi và người nhận.

+ Toàn vẹn dữ liệu: đảm bảo thông tin không bị sai lệch và nó phải thể hiện chính xác thông tin gốc gửi đến.

- Với việc sử dụng SSL, các Web site có thể cung cấp khả năng bảo mật thông tin, xác thực và toàn vẹn dữ liệu đến người dùng. SSL được tích hợp sẵn vào các browser và Web server, cho phép người sử dụng làm việc với các trang Web ở chế độ an toàn. Khi Web browser sử dụng kết nối SSL tới server, biểu tượng ổ khóa sẽ xuất hiện trên thanh trạng thái của cửa sổ browser và dòng "http" trong hộp nhập địa chỉ URL sẽ đổi thành "https". Một phiên giao dịch HTTPS sử dụng cổng 443 thay vì sử dụng cổng 80 như dùng cho HTTP.

- SSL sử dụng phương pháp mã hóa khóa công khai với thuật toán RSA dùng để mã hóa. SSL cho phép:

+ Client và server nhận dạng lẫn nhau.

+ Sử dụng chứng thực số để chứng thực tính toàn vẹn.

+ Mã hóa toàn bộ thông tin để đảm bảo tính bí mật.

➢ **Hoạt động của SSL**

Khi trình duyệt của một máy khách đến một Website bí mật của một máy chủ, máy chủ gửi một lời chào tới trình duyệt. Trình duyệt đáp lại bằng một lời chào. Việc tiến hành trao đổi lời chào, hoặc bắt tay cho phép 2 máy tính quyết định các chuẩn mã hoá và nén (mà chúng cùng hỗ trợ). Trình duyệt máy khách yêu cầu máy chủ đưa ra một chứng chỉ số. Máy

chủ gửi cho trình duyệt một chứng chỉ đã được công nhận bởi CA. Trình duyệt kiểm tra chữ ký số có trên chứng chỉ của máy chủ, dựa vào khoá công khai của CA, khoá này được lưu giữ trong trình duyệt. Hoạt động này xác thực máy chủ thương mại.

Máy khách và máy chủ thoả thuận rằng mọi trao đổi phải được giữ bí mật, bởi vì những thông tin này là quan trọng. Để thực hiện bí mật, SSL sử dụng mã hoá khoá công khai (không đối xứng) và mã hoá khoá riêng (đối xứng). Thoạt đầu, trình duyệt sinh ra một khoá riêng dùng chung cho cả hai. Sau đó, trình duyệt mã hoá khoá riêng bằng khoá công khai của máy chủ. Khoá công khai của máy chủ được lưu giữ trong chứng chỉ số, máy chủ gửi chứng chỉ này cho trình duyệt trong quá trình xác thực. Một khi khoá được mã hoá, trình duyệt gửi nó cho máy chủ. Ngược lại, máy chủ giải mã thông báo bằng khoá riêng của nó và tìm ra khoá riêng dùng chung. Tất cả các thông báo giữa máy khách và máy chủ được mã hoá bằng khoá riêng dùng chung (cũng được biết đến như là một khoá phiên). Sau khi kết thúc phiên giao dịch, khoá phiên bị huỷ bỏ. Một kết nối mới lại bắt đầu tương tự

3.3.4.2 SET (Sécure Electronic Transaction)

Giao thức SSL có khả năng mã hoá thông tin (như số thẻ tín dụng của khách hàng) và đảm bảo an toàn khi gửi nó từ trình duyệt của người mua tới website của người bán hàng. Tuy nhiên, các giao dịch mua bán trên web không chỉ đơn thuần như vậy. Số thẻ tín dụng này cần phải được ngân hàng của người mua kiểm tra để khẳng định tính hợp lệ và giá trị của thẻ tín dụng tiếp đó các giao dịch mua bán phải được thực hiện. SSL không giải quyết được các vấn đề này.

Một giao thức được thiết kế để hoàn tất các bước tiếp theo của một giao dịch mua bán trên Internet đó là giao thức giao dịch điện tử an toàn (SET - Sécure Electronic Transaction). Giao dịch điện tử an toàn (SET), do Visa International, MasterCard, Netscape và Microsoft phát triển vào năm 1996, được thiết kế đặc biệt để bảo vệ các giao dịch thanh toán trong TMĐT.

- ✓ **Khái niệm**

SET (Sécure Electronic Transaction) là một giao thức giao dịch điện tử an toàn, sử dụng mật mã để cung cấp tính bảo mật cho thông tin, đảm bảo tính toàn vẹn trong thanh toán, và cho phép xác thực các thực thể với nhau.

- ✓ **Đặc điểm**

- SET sử dụng các chứng thực điện tử để xác thực mỗi bên tham gia trong một giao dịch TMĐT bao gồm người mua, người bán và ngân hàng của người bán. Kỹ thuật mã hoá khoá công cộng được sử dụng trong việc đảm bảo an toàn các thông tin khi chuyển nó trên Web.

+ Khác với giao thức SSL có 3 thực thể là người chủ sở hữu thẻ, người kinh doanh và cơ quan chứng thực (CA), SET có thêm một thực thể là cổng thanh toán. Đây là cổng kết nối Internet với các mạng độc quyền của các ngân hàng. Mỗi thực thể tham gia cần chứng thực riêng.

- Để tiến hành các giao dịch, người bán hàng cần phải có một chứng thực điện tử và một phần mềm SET đặc biệt. Người mua cũng cần phải có chứng thực điện tử và một phần mềm ví tiền số hoá.

- Trong giao thức SET toàn bộ quá trình giao dịch là bí mật:

+ Doanh nghiệp/ Người bán không được biết thông tin về thanh toán

+ Tổ chức tài chính không được biết thông tin đơn hàng

✓ **Quy trình giao dịch của SET**

- Bước 1: Người mua truy cập vào ví điện tử, ví điện tử sẽ tự động lựa chọn tài khoản thẻ được lưu trữ trong ví và tiến hành khai báo các thông tin một cách tự động

- Bước 2: Thông tin thanh toán đó sẽ được truyền tải tự động về máy chủ của website bán hàng

- Bước 3: Máy chủ của website bán hàng sẽ gửi yêu cầu xác thực các thông tin này tới ngân hàng của website thông qua cổng thanh toán

- Bước 4: Ngân hàng của website bán hàng gửi tiếp yêu cầu xác thực về ngân hàng phát hành thẻ

- Bước 5: Ngân hàng phát hành thẻ kiểm tra các thông tin, tiến hành thanh toán sau đó gửi kết quả về ngân hàng của website bán hàng

- Bước 6: Ngân hàng của website bán hàng gửi tiếp kết quả thông báo về máy chủ của website bán hàng

- Bước 7: Website bán hàng tiến hành giao hàng cho người mua

✓ **Hạn chế của SET**

Yêu cầu phần mềm, phần cứng chuyên dụng với chi phí cao, độ trễ khi giao dịch do tính phức tạp của các thuật toán mã hóa công khai và thường xuyên tiến hành giao dịch với các ngân hàng trung gian, hệ thống cổng kênh và quá trình giao dịch chậm, các tổ chức tài chính phải trả thêm phí cài đặt và duy trì PKI cho CA, các giao dịch dựa trên tài khoản như: séc điện tử không hỗ trợ trong SET.

CÂU HỎI CHƯƠNG 3

1 Trình bày về vấn đề bảo mật trong thanh toán điện tử? Phân tích sự cần thiết phải bảo mật trong thanh toán điện tử?

2 Mô tả các loại hình tấn công sau đây: (1) Phishing; (2) Sniffer; (3) Keylogger.

3 Mô tả các loại hình tấn công sau đây: (1) Trojan horse; (2) Trộm Cokkies?

4 Nêu các biện pháp bảo mật trong thanh toán điện tử?

5 Trình bày phương pháp kiểm soát truy cập và xác thực?

6 Trình bày tầm quan trọng của chữ ký điện tử trong các giao dịch TMĐT

7 Trình bàt các giao thức đảm bảo an toàn cho TMĐT.

TÀI LIỆU THAM KHẢO

[17]. Nguyễn Văn Hùng (chủ biên), TMĐT - cẩm nang, NXB Kinh tế TP Hồ Chí Minh 2013

[18]. Thái Thanh Sơn và Thái Thanh Tùng, TMĐT trong thời đại số, NXB Thông tin và

Truyền thông, 2017

[19]. Đàm Gia Mạnh, Giáo trình An toàn dữ liệu trong TMĐT, NXB Thống Kê, 2009

[20]. Đàm Gia Mạnh, Giáo trình Hệ thống thông tin quản lý, NXB Thống Kê, 2017

[21]. Hoàng Đăng Hải, Quản lý An toàn thông tin, NXB Khoa học và Kỹ thuật, 2018

[22]. Bernd W. Wirtz, Digital Business Models, Concepts, Models, and the Alphabet Case Study, Springer, 2019

[23]. Kenneth C. Laudon Carol Guercio Traver, E-commerce - business. technology. society, 10th, PEASON 2014

[24]. Andreas Meier & Henrik Stormer, eBusiness & eCommerce - Managing the Digital Value Chain, Springer, 2009

[25]. Dave Chaffey, E-business and E-commerce Management: Strategy, Implementation and Practice – 6th, Pearson Education, 2015

[26]. Arch G. Woodside & Peter J. LaPlaca, Handbook of Strategic e-Business Management, Springer-Verlag Berlin Heidelberg, 2014.

[27]. Kenneth C. Laudon & Carol Guercio Traver: E-commerce Business, Technology, Society: 13th edition: Pearson Publishing House, 2017.

CHƯƠNG 4: LỰA CHỌN GIẢI PHÁP TRONG THANH TOÁN ĐIỆN TỬ

4.1 Cổng thanh toán điện tử

Thuật ngữ cổng thanh toán (payment gateway) hay cổng thanh toán điện tử là một thuật ngữ có khá nhiều cách hiểu và tiếp cận.

Quan điểm đầu tiên, cổng thanh toán trước đây được hiểu là một hệ thống thanh toán được cung cấp bởi một tổ chức, doanh nghiệp chuyên xử lý những giao dịch liên quan đến thẻ thanh toán cho các website TMĐT. Với quan điểm như trên, ở Việt Nam trước đây có một vài cổng thanh toán thuần túy: Onepay, Smartlink.

Ở góc độ tiếp cận hẹp hơn, cổng thanh toán được hiểu đơn giản là một hệ thống phần mềm được phát triển bởi các đơn vị, nhà cung cấp nhất định với mục đích hỗ trợ các website bán hàng, website TMĐT liên kết được với các ngân hàng, giúp cho các giao dịch của người mua và người bán trên các kênh này trở nên thuận tiện và nhanh chóng hơn khi họ có thể thực hiện các giao dịch chuyển tiền trực tuyến ngay trên website của người bán.

Với phạm vi nghiên cứu của học phần, chúng ta tiếp cận cổng thanh toán điện tử một cách tổng quát nhất. Về bản chất, cổng thanh toán là dịch vụ cho phép khách hàng thực hiện thanh toán trực tuyến tại các website TMĐT. Cổng thanh toán cung cấp hệ thống kết nối an toàn giữa tài khoản thanh toán của khách hàng (tài khoản thẻ, ví điện tử) với tài khoản của website bán hàng, cho phép các cá nhân và doanh nghiệp thanh toán và nhận tiền trên internet một cách nhanh chóng, tiện lợi và được bảo vệ an toàn. Tất cả những đơn vị cung cấp dịch vụ cổng thanh toán (PSP: Payment Service Provider). Các đơn vị, chủ quản lý website TMĐT thay vì phải duy trì kết nối với từng đơn vị thanh toán riêng lẻ (ngân hàng) chỉ cần sử dụng dịch vụ mà các PSP này cung cấp. PSP sẽ xử lý được đa dạng các phương tiện thanh toán mà khách hàng sử dụng. PSP đảm nhận việc kết nối, chấp nhận thanh toán qua các ngân hàng và các phương tiện mà khách hàng sử dụng.

Về cơ bản thì cổng thanh toán điện tử có những chức năng sau đây:

- Nhận thông tin giao dịch trực tuyến tại website bán hàng trực tuyến
- Xử lý thông tin trên Cổng thanh toán trực tuyến
- Xử lý giao dịch trừ tiền tại ngân hàng kết nối thanh toán
- Thông báo kết quả giao dịch tại website bán hàng trực tuyến.

4.2 Tiêu chí lựa chọn cổng thanh toán điện tử

Hiện nay trên thị trường có rất nhiều cổng thanh toán điện tử khác nhau, mỗi một cổng thanh toán sẽ có những ưu điểm và quy trình hoạt động riêng. Do đó khi làm website, doanh nghiệp có cơ hội lựa chọn cổng thanh toán tốt và phù hợp. Để lựa chọn được cổng thanh toán trực tuyến phù hợp, doanh nghiệp cần cân nhắc những tiêu chí sau đây:

(1) Danh tiếng (Uy tín): Lựa chọn cổng thanh toán của một công ty danh tiếng, có thương hiệu và uy tín không chỉ giúp doanh nghiệp cảm thấy an tâm mà còn gia tăng niềm tin với người tiêu dùng của họ. Chính vì thế, website bán hàng nên lựa chọn những cổng thanh toán uy tín lâu năm trên thị trường hoặc được công nhận và có thương hiệu về lĩnh vực giải pháp thanh toán.

(2) Khả năng tương thích hệ thống: Lựa chọn cổng thanh toán nên cân nhắc tới yếu

tố thứ hai đó là tính tương thích với hệ thống website hiện có. Website bán hàng nên kiểm tra lại các thông tin về Hosting của mình, cho dù dịch vụ Website Hosting của doanh nghiệp có thể tích hợp các cổng thanh toán hay không thì các cổng thanh toán này đều cần dễ dàng tích hợp với phần mềm mua hàng trực tuyến của website.

Một cách tổng quát hơn xem xét cổng thanh toán sẽ tích hợp tốt như thế nào với nền tảng hiện tại của website bán hàng – cả về kỹ thuật và thiết kế. Nếu cần quá nhiều thủ thuật lộn xộn và phức tạp để kết hợp nhuần nhuyễn vào cấu trúc website hiện tại thì doanh nghiệp nên suy nghĩ lại về lựa chọn của mình. Hiện tại có rất nhiều cổng thanh toán trực tuyến, hãy loại bỏ những lựa chọn không tương thích với hệ thống mà doanh nghiệp đang sử dụng.

(3) Bảo mật: Vấn đề quan tâm rất lớn khi lựa chọn cổng thanh toán đó là vấn đề bảo mật. Chính vì cổng thanh toán điện tử là thanh toán trung gian giữa người mua - người bán – đơn vị thanh toán, do đó đòi hỏi phải có khả năng bảo mật cao để bảo mật được thông tin khách hàng và doanh nghiệp. Doanh nghiệp lựa chọn một cổng thanh toán an toàn và bảo mật chính là việc doanh nghiệp đã xây dựng được niềm tin vào danh tiếng cho chính mình. Bản thân doanh nghiệp phải hiểu cơ chế phát hiện và ngăn chặn gian lận – được tích hợp vào cổng thanh toán để tránh các vấn đề rủi ro và tránh việc mua hàng giả mạo.

Các website bán hàng có thể lựa chọn những cổng thanh toán đạt chứng chỉ PCI DSS, cấp độ Service Provider (cấp độ Nhà cung cấp dịch vụ loại 1) để sử dụng dịch vụ, vì bản thân những cổng thanh toán đạt được chứng chỉ này là bằng chứng cho việc họ đã đạt mức an toàn tối đa.

Đồng thời nhấn mạnh vào các biện pháp an ninh được xây dựng như Tokenization – các dữ liệu thẻ tín dụng được lưu trữ dưới dạng mã với một số mặt nạ riêng như **********1111 (dấu * không đại diện cho bất cứ điều gì, nó đơn giản là toàn bộ số thẻ tín dụng với 16 chữ số không được lưu trữ trên mạng của doanh nghiệp). Điều này cho phép bạn thay thế dữ liệu thẻ trên hệ thống kinh doanh nội bộ bằng một ID duy nhất.

Ngoài ra doanh nghiệp cũng nên cân nhắc lựa chọn loại hình của cổng thanh toán. *Cổng thanh toán có lưu trữ* (hosted payment gateway) chuyển hướng khách hàng của bạn sang trang thanh toán được lưu trữ an toàn. Sau khi thanh toán, khách hàng được đưa trở lại website của bạn. Đơn hàng được xác nhận và quá trình hoàn tất. *Cổng thanh toán không lưu trữ* (non-hosted payment gateway) cho phép khách hàng của bạn nhập thông tin chi tiết trực tiếp trên website của bạn.

Tham khảo thêm: Chứng chỉ PCI DSS

Chuẩn bảo mật PCI DSS được đưa ra bởi PCI Sécurity Standards Council (bao gồm các thành viên là các tổ chức thẻ quốc tế: Visa Inc, MasterCard Worldwide, American Express, Discover Financial Services, JCB International). Mục đích của PCI DSS bảo đảm an toàn cho dữ liệu thẻ khi được xử lý và lưu trữ tại các ngân hàng hoặc doanh nghiệp thanh toán. PCI DSS giúp đưa ra những chuẩn mực về bảo mật thông tin thẻ và được áp dụng trên toàn cầu.

Theo đó, tất cả mọi tổ chức có liên quan đến việc truyền tải, xử lý và lưu trữ dữ liệu thẻ thanh toán (được gọi là "Cardholder Data") đều phải tuân thủ theo tiêu chuẩn PCI DSS.

PCI DSS là là một hệ thống các yêu cầu để đáp ứng các chuẩn mực về an ninh, chính sách, quy trình, cấu trúc mạng, hệ thống phần mềm và một số yếu tố khác. Tập hợp các chuẩn mực này định hướng cho các ngân hàng hoặc doanh nghiệp về thanh toán đảm bảo an ninh cho dữ liệu của thẻ thanh toán.

Về cơ bản PCI DSS là một tập hợp những nguyên tắc và yêu cầu liên quan tới những vấn đề sau:

Xây dựng và duy trì hệ thống mạng bảo mật

- Yêu cầu 1: Xây dựng và duy trì hệ thống tường lửa để bảo vệ dữ liệu thẻ.
- Yêu cầu 2: Không sử dụng các tham số hoặc mật khẩu có sẵn từ các nhà cung cấp hệ thống.

Bảo vệ dữ liệu thẻ thanh toán

- Yêu cầu 3: Bảo vệ dữ liệu thẻ thanh toán khi lưu trên hệ thống
- Yêu cầu 4: Mã hóa thông tin thẻ trên đường truyền khi giao dịch.

Xây dựng và duy trì an ninh mạng

- Yêu cầu 5: Sử dụng và cập nhật thường xuyên phần mềm diệt Virus
- Yêu cầu 6: Xây dựng và duy trì hệ thống và ứng dụng đảm bảo an ninh mạng.

Xây dựng hệ thống kiểm soát xâm nhập

- Yêu cầu 7: Hạn chế tiếp cận với dữ liệu thẻ thanh toán
- Yêu cầu 8: Cấp và theo dõi các tài khoản truy nhập hệ thống của nhân viên
- Yêu cầu 9: Giới hạn các phương pháp tiếp cận vật lý với dữ liệu thẻ

Theo dõi và đánh giá hệ thống thường xuyên

- Yêu cầu 10: Kiểm tra và lưu tất cả các truy nhập vào hệ thống và dữ liệu thẻ
- Yêu cầu 11: Thường xuyên đánh giá và thử nghiệm lại quy trình an ninh hệ thống

Chính sách bảo vệ thông tin

- Yêu cầu 12: Xây dựng chính sách bảo vệ thông tin.

(4) Phương thức thanh toán được chấp nhận: Một cổng thanh toán càng cung cấp linh hoạt và đa dạng các loại hình thanh toán thì khả năng thành công của đơn hàng càng cao. Chính vì vậy lựa chọn cổng thanh toán với nhiều phương thức thanh toán đa dạng, khác nhau cho người dùng sẽ làm gia tăng khả năng mua hàng của khách hàng.

Website bán hàng phải xác định khách hàng của mình là đối tượng nào, bán hàng cho doanh nghiệp/ tổ chức là chủ yếu hay cho cá nhân là chủ yếu; bán hàng cho khách nước ngoài là chủ yếu hay khách trong nước là chủ yếu, từ đó sẽ xem xét và cân nhắc xem những phương tiện thanh toán nào là phù hợp với từng loại đối tượng khách hàng; cân nhắc xem cổng thanh toán trong nước hay nước ngoài sẽ phù hợp hơn, từ đó là cơ sở để đưa ra quyết định là nên lựa chọn cổng thanh toán nào.

Hiện tại thì hầu hết cổng thanh toán đều chấp nhận thanh toán với thẻ Visa, MasterCard, American Express và thẻ nội địa, nhiều cổng thanh toán còn tích hợp cho phép thanh toán cả ví điện tử, chính vì thế sẽ có đa dạng và linh hoạt loại cổng thanh toán cho website bán hàng lựa chọn mà không phải băn khoăn quá nhiều.

(5) Phí dịch vụ thanh toán: Chi phí cho dịch vụ thanh toán mà website phải chi trả cho cổng thanh toán là một trong những vấn đề rất quan trọng. Giống như hầu hết mọi dịch vụ, khi sử dụng dịch vụ của bên thứ ba đó là cổng thanh toán, chắc chắn sẽ có các khoản phí liên quan, lựa chọn cổng thanh toán phù hợp với ngân sách và quy mô của doanh nghiệp là điều cần thiết. Website bán hàng cần cân nhắc một số khoản phí sau, trước khi lựa chọn cổng thanh toán:

- Phí đăng ký dịch vụ/ chi phí thiết lập: thông thường sẽ trả một lần duy nhất khi đăng ký.

- Phí duy trì tài khoản hàng tháng/ phí quản trị: phí nay thanh toán hàng tháng, hầu như các cổng thanh toán đều thu phí này.

- Phí xử lý giao dịch: phí này sẽ trả cố định trên từng giao dịch phát sinh (tùy loại cổng thanh toán mà thu phí khác nhau).

- Phí thanh toán thẻ: phí này trả theo tỉ lệ dựa trên giá trị giao dịch, phí này giao động từ 1,5% đến 4% giá trị giao dịch.

Bên cạnh đó còn có một số loại phí bổ sung của cổng thanh toán mà website bán hàng cần cân nhắc:

- Phí xác minh địa chỉ: kiểm tra địa chỉ thanh toán đã khớp với địa chỉ thanh toán trong hồ sơ với nhà cung cấp chưa.

- Phí hủy bỏ: Nếu bạn dừng sử dụng tài khoản của mình sớm hơn trong hợp đồng, bạn sẽ phải trả một khoản phạt.

- Phí bồi hoàn: Bạn phải trả phí nếu khách hàng của bạn không chấp nhận thanh toán.

- Phí tối thiểu hàng tháng: Có thể có phí tối thiểu hàng tháng cho dù bạn có giao dịch hay không

- Phí phát hành: Phí đưa ra cho việc tạo các giấy tờ cho tài khoản của bạn

Vì vậy, tốt nhất là hiểu tất cả các loại phí và từng mức phí trước khi đưa ra quyết định rõ ràng.

(6) Yếu tố khác: Ngoài ra còn một vài những tiêu chí khác mà website bán hàng có thể cân nhắc:

- Tốc độ xử lý giao dịch: nhanh hay chậm, ở mức độ nào, có thể chấp nhận hay không?

- Quy trình thanh toán: quy trình đơn giản hay phức tạp, gồm bao nhiêu bước?

- Thời gian lưu trữ tiền của khách hàng: mỗi nhà cung cấp cổng thanh toán có lịch trình thanh toán khác nhau. Một số lưu giữ tiền của khách hàng trong vòng 30 ngày. Một số có thể chuyển tiền cho bạn ngay sau giao dịch. Một số khác có thể có một ngày quy định để chuyển tiền, số còn lại chuyển tiền theo ngày.

4.3 Một số cổng thanh toán điện tử

4.3.1 Cổng thanh toán điện tử trong nước

4.3.1.1 Cổng thanh toán Napas (Napas.com.vn)

Công ty Cổ phần Thanh toán Quốc gia Việt Nam (NAPAS) được thành lập vào năm

2004, đổi tên từ Công ty Cổ phần Chuyển mạch Tài chính Quốc gia Việt Nam (Banknetvn) kể từ ngày 04/02/2016, trên cơ sở sáp nhập với Công ty CP Dịch vụ thẻ Smartlink để xây dựng Trung tâm chuyển mạch thẻ thống nhất theo chỉ đạo của Thủ tướng Chính phủ và Ngân hàng Nhà nước Việt Nam. Là đơn vị xây dựng và hoàn thiện hạ tầng thanh toán bán lẻ quốc gia, NAPAS được Ngân hàng Nhà nước cấp phép cung ứng dịch vụ chuyển mạch tài chính và dịch vụ bù trừ điện tử tại Việt Nam. Cổ đông lớn nhất của NAPAS là Ngân hàng Nhà nước, chiếm 49% vốn điều lệ của công ty.

NAPAS hiện đang quản trị và vận hành hệ thống chuyển mạch kết nối liên thông hơn 17.000 máy ATM, 270.000 máy POS, 300 doanh nghiệp thanh toán điện tử trong các lĩnh vực hàng không, viễn thông, khách sạn, du lịch; phục vụ hơn 100 triệu chủ thẻ của 46 ngân hàng thương mại trong nước và quốc tế đang hoạt động tại Việt Nam.

Các sản phẩm dịch vụ chính được NAPAS cung cấp bao gồm: Dịch vụ chuyển mạch thẻ nội địa, Dịch vụ Cổng Thanh toán, Dịch vụ chuyển mạch thẻ quốc tế, Dịch vụ hỗ trợ Thu hộ, Chi hộ điện tử, Dịch vụ thanh toán và bù trừ điện tử, Dịch vụ chuyển tiền nhanh 24/7.

Dịch vụ Cổng thanh toán trực tuyến (Ecommerce) là dịch vụ NAPAS cung cấp cho doanh nghiệp / nhà cung cấp dịch vụ, hỗ trợ doanh nghiệp thu phí hàng hóa, dịch vụ của khách hàng có thẻ và tài khoản mở tại các ngân hàng / tổ chức liên kết với NAPAS bằng hình thức nhập thông tin thẻ nội địa và quốc tế trên các kênh bán hàng trực tuyến của doanh nghiệp như website, ứng dụng trên điện thoại di động, khác.

Hình 4.1 : Giải pháp của Napas

Cổng thanh toán Napas có một số đặc điểm :

- Hỗ trợ thanh toán đối với thẻ nội địa của gần 40 ngân hàng trong nước và thẻ quốc tế mang thương hiệu Visa, MasterCard, American Express, JCB, Diners Club, Unionpay, được phát hành trên khắp thế giới.

- Giải pháp hỗ trợ đa thiết bị (PC, tablet, smartphone) và đa đồng tiền thanh toán (191 đồng tiền) với các tính năng ưu việt như tokenization, thu tiền tự động định kỳ, quản lý rủi ro tiến tiến.

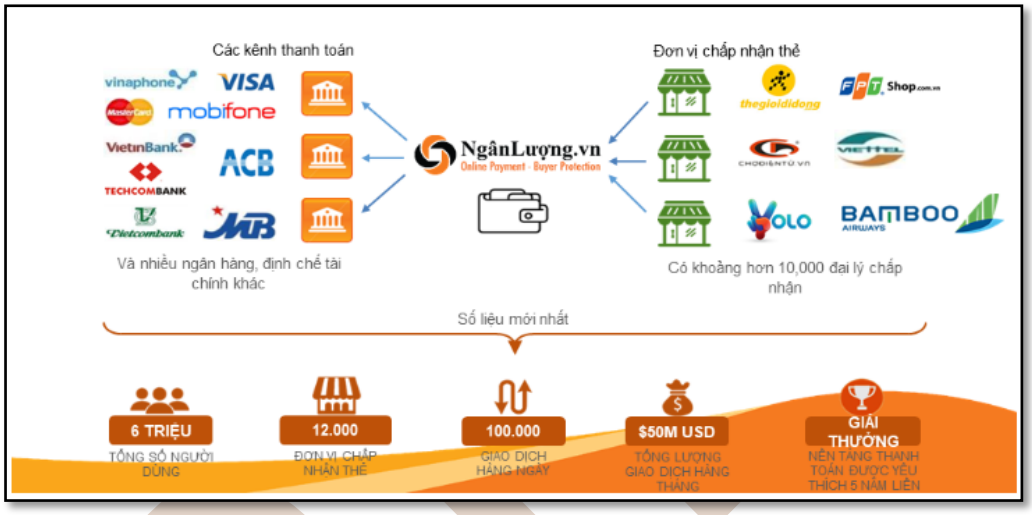
- Áp dụng các tiêu chuẩn công nghệ bảo mật, quản lý rủi ro hàng đầu trong ngành Tài chính Ngân hàng.

- Giải pháp mã hóa Tokenization cho thẻ quốc tế và nội địa cho phép khách hàng lưu lại thông tin thẻ dưới dạng mã hóa để phục vụ những lần thanh toán kế tiếp mà không cần nhập lại thông tin thẻ.

4.3.1.2 Cổng thanh toán Ngân lượng (Nganluong.vn)

NgânLượng.vn là Ví điện tử và cổng thanh toán trực tuyến tiên phong và uy tín hàng đầu tại Việt Nam, cả về sản phẩm dịch vụ, độ phủ thị trường và lưu lượng thanh toán. Được phát triển bởi Nexttech Group (tiền thân là PeaceSoft Group) từ năm 2009, Ngân Lượng cho phép các cá nhân và doanh nghiệp gửi và nhận tiền thanh toán trên Internet một cách nhanh chóng, an toàn, tiện lợi.

Ngân Lượng.vn hoạt động theo mô hình ví điện tử, theo đó người dùng có thể đăng kí tài khoản cá nhân hoặc doanh nghiệp với ba chức năng chính: Nạp tiền, Thanh toán và Chuyển tiền. Tất cả các giao dịch đều được thực hiện trực tuyến thông qua Thẻ ATM nội địa, Thẻ quốc tế (Visa, Master, JCB, Amex), Internet Banking, QR-Pay...và các hình thức tiện dụng khác.



Hình 4.2: Mô hình thanh toán của Nganluong.vn

Ngân Lượng.vn đã xây dựng hệ thống tiên tiến liên kết trực tiếp với gần 40 tổ chức tài chính và viễn thông tại Việt Nam và Quốc tế, bao gồm: Paypal, Visa/Master, CyberSource, Sacombank, VPBank, Shinhan Bank (ANZ), Eximbank, Maritime Bank, VIB, HSBC, CitiBank, Techcombank, Seabank, Standard Chartered, TP Bank, SCB (NH TMCP Sài Gòn), NAB (Nam Á Bank), OCB (NH Phương Đông), KLB (Kiên Long Bank), SHB(NH Sài Gòn – Hà Nội), BIDV, FE CREDIT, VinaPhone, MobiFone, Viettel… qua đó mang lại một giải pháp thanh toán trực tuyến toàn diện cung cấp đầy đủ và đa dạng các kênh thanh toán cho khách hàng.

4.3.1.3 Nhà cung cấp dịch vụ thanh toán Payoo (Payoo.vn)

Công ty CP Dịch vụ Trực tuyến Cộng Đồng Việt (VietUnion) được thành lập vào ngày 14/01/2008 với mục tiêu trở thành đơn vị dẫn đầu trong lĩnh vực thanh toán điện tử tại Việt Nam**.** Dịch vụ thanh toán Payoo được Thống đốc Ngân hàng Nhà nước cấp phép hoạt động trong lĩnh vực trung gian thanh toán vào ngày 18/02/2009, nhằm giúp cho người dùng có thể thanh toán một cách dễ dàng, nhanh chóng và tiện lợi hơn.

Sử dụng hệ thống thanh toán của Payoo, mang lại một số giá trị như:

- Tiện lợi: Khách hàng không phải mất nhiều thời gian cho việc tìm kiếm một địa điểm để thanh toán hóa đơn, mua mã thẻ điện thoại cũng như các dịch vụ tiện ích khác. Khách hàng có thể chủ động thanh toán hóa đơn của mình tại bất kì thời điểm nào trong ngày, bằng bất cứ

hình thức nào.

- An toàn: Tại Payoo, an ninh tài chính của khách hàng là ưu tiên cao nhất. Với công nghệ bảo mật và nền tảng kỹ thuật hoàn chỉnh, đạt chứng nhận bảo mật quốc tế PCI – DSS và chuẩn ISO 27001, Payoo đã triển khai xây dựng và kết nối các dịch vụ ứng dụng thanh toán trực tuyến đảm bảo uy tín.

- Đa dạng: Thông qua Payoo, khách hàng có thể thanh toán mọi hóa đơn như tiền điện, nước, điện thoại, truyền hình, internet, tài chính… bằng nhiều hình thức khác nhau.

Bên cạnh đó, với sự hoàn thiện hạ tầng công nghệ, Payoo đã được các đối tác tin tưởng chọn làm cổng thanh toán. Mọi giao dịch thanh toán qua cổng đều được mã hóa bằng SSL, các kết nối với đối tác đều được chứng thực bằng chữ ký điện tử và tuân thủ các quy trình theo chuẩn ISO 27001:2013 về an toàn thông tin và chuẩn PCI-DSS về an toàn thông tin và bảo mật quốc tế.

Hình 4.3: Cổng thanh toán điện tử Payoo.vn

4.3.2 Cổng thanh toán điện tử trên thế giới

4.3.2.1 Cổng thanh toán điện tử Authorize.net

Authorize.net là tổ chức cung cấp dịch vụ thanh toán được thành lập vào năm 1996. Authorize.net là cổng thanh toán hiển thị 24/7 để xử lý những giao dịch thanh toán. Kết nối 1 website với một mạng lưới xử lý thanh toán là một điều đặc biệt khó khăn và thường vượt quá khả năng chuyên môn và kỹ thuật của hầu hết các thương gia trực tuyến. Thay vì thế, người bán có thể dễ dàng kết nối với cổng thanh toán Authorize.net nơi mà cung cấp một cấu trúc rất phức tạp và an ninh cần thiết để đảm bảo việc truyền dữ liệu giao dịch nhanh, tin cậy và an toàn.

Authorize.net cung cấp hầu hết các dịch vụ thanh toán trực tuyến bao gồm: thanh toán di động, thanh toán thẻ, thanh toán hóa đơn điện tử, thanh toán qua điện thoại, và một trong những dịch vụ phổ biến nhất đó là thanh toán séc điện tử eCheck.net. Authorize.net cho phép người bán chấp nhận và xử lý thanh toán từ tài khoản ngân hàng trực tuyến thông qua trang web hoặc cũng có thể lựa chọn thanh toán séc điện tử mà ko cần thẻ tín dụng hoặc thanh toán séc điện tử với mức phí rất hợp lý chỉ 0.75$/ giao dịch. Authorize.net là cửa ngõ thanh toán hàng đầu, Authorize.Net được hơn 430.000 người bán tin cậy, xử lý hơn 1 tỷ giao dịch và 149 tỷ USD thanh toán hàng năm. Authorize.net cho phép tích hợp thanh toán séc điện tử từ thanh

toán từ tài khoản ngân hàng thông qua website hoặc Virtual Terminal.

4.3.2.2 Cổng thanh toán điện tử Paypal

Paypal là một công ty hoạt động trong lĩnh vực TMĐT, chuyên cung cấp các dịch vụ thanh toán và chuyển tiền qua mạng Internet. Paypal cung cấp đa dạng các loại hình cho khách hàng người mua và người bán. Paypal cho phép người dùng có thể thanh toán qua ví điện tử, thẻ thanh toán, séc điện tử. Paypal thu phí thông qua thực hiện việc xử lý thanh toán cho các doanh nghiệp hoạt động trực tuyến, các trang đấu giá, và các khách hàng doanh nghiệp khác.

Trước đây, PayPal là một công ty chuyên cung cấp phần mềm cho các giao dịch tài chính an toàn trên các thiết bị cá nhân tiền thân. Tiền thân của Paypal là Confinity Inc. được thành lập bởi Ken Howery, Luke Nosek, Max Levchin và Peter Thiel vào năm 1998. Vào năm 1999, công ty được tài trợ bởi John Malloy từ BlueRun Ventures. Trong tháng 3 năm 2000, Elon Musk đã tiến hành sáp nhập Confinity vào X.com (công ty ngân hàng trực tuyến của Elon Musk). Nhận thấy việc Confinity tạo ra nhiều lợi nhuận hơn so với X.com, Elon Musk tiếp tục tập trung nhiều hơn vào các hoạt động chuyển tiền của Confinity. Vào 10/2000, Elon Musk quyết định chấm dứt các hoạt động ngân hàng trên internet của X.com và chỉ tập trung vào các dịch vụ chuyển tiền của Paypal. Công ty X.com sau đó được đổi tên thành PayPal vào năm 2001, và mở rộng nhanh chóng trong suốt cả năm cho đến khi giám đốc điều hành công ty quyết định đưa PayPal ra sử dụng công cộng vào năm 2002. Vào tháng 7/2002, tập đoàn eBay mua lại PayPal với giá 1,5 tỷ USD. Kể từ đó PayPal trở thành lựa chọn hàng đầu của người sử dụng eBay cho các giao dịch. Paypal càng phát triển mạnh hơn nữa sau khi được mua lại bởi eBay và bước vào một kỉ nguyên phát triển vượt bậc và mở rộng phạm vi hoạt động ra toàn thế giới.

Hiện nay, PayPal đã có mặt tại 202 quốc gia trên toàn thế giới, với 277 triệu người dùng và 16 triệu tài khoản thương vào 2018 và lưu lượng giao dịch gần 150 tỉ USD. Kể từ khi ra đời, hệ thống này đã thực hiện 1,7 tỷ giao dịch với trung bình 32 giao dịch thanh toán trên mỗi tài khoản. Trang web PayPal.com đứng thứ 73 trên toàn thế giới bởi lượng người truy cập, 768.745 trang web trên toàn thế giới sử dụng PayPal.

CÂU HỎI CHƯƠNG 4

1 Trình bày khái niệm bổng thanh toán điện tử?
2 Trình bày tiêu chí lựa chọn cổng thanh toán điện tử?
3 Phân tích thuận lợi và khó khăn đối với phát triển thanh toán điện tử ở Việt Nam?
4 Mô tả và phân tích các yếu tố hạ tầng cho thanh toán điện tử tại Việt Nam hiện nay?
5 Trình bày các chức năng của cổng thang toán điện tử?

TÀI LIỆU THAM KHẢO CHƯƠNG 4

[28]. Nguyễn Văn Hồng và Nguyễn Văn Thoan, Giáo trình TMĐT căn bản, NXB Bách Khoa – Hà Nội, 2013

[29]. Nguyễn Văn Hùng (chủ biên), TMĐT - cẩm nang, NXB Kinh tế TP Hồ Chí Minh 2013

[30]. Lê Quân & Hoàng Văn Hải, Giáo trình quản trị tác nghiệp doanh nghiệp thương mại, NXB Thống Kê, 2010

[31]. Nguyễn Văn Thanh, Giáo trình Thanh toán trong TMĐT, NXB Thống Kê, 2011

[32]. Andreas Meier & Henrik Stormer, eBusiness & eCommerce - Managing the Digital Value Chain, Springer, 2009

[33]. Dave Chaffey, E-business and E-commerce Management: Strategy, Implementation and Practice – 6th, Pearson Education, 2015

[34]. Arch G. Woodside & Peter J. LaPlaca, Handbook of Strategic e-Business Management, Springer-Verlag Berlin Heidelberg, 2014.

[35]. Kenneth C. Laudon & Carol Guercio Traver: E-commerce Business, Technology, Society: 13th edition: Pearson Publishing House, 2017.

TÀI LIỆU THAM KHẢO

TIẾNG VIỆT

[36]. Nguyễn Văn Hồng và Nguyễn Văn Thoan, Giáo trình TMĐT căn bản, NXB Bách Khoa – Hà Nội, 2013

[37]. Nguyễn Văn Hùng (chủ biên), TMĐT - cẩm nang, NXB Kinh tế TP Hồ Chí Minh 2013

[38]. Lê Quân & Hoàng Văn Hải, Giáo trình quản trị tác nghiệp doanh nghiệp thương mại, NXB Thống Kê, 2010

[39]. Thái Thanh Sơn và Thái Thanh Tùng, TMĐT trong thời đại số, NXB Thông tin và Truyền thông, 2017

[40]. Đàm Gia Mạnh, Giáo trình An toàn dữ liệu trong TMĐT, NXB Thống Kê, 2009

[41]. Đàm Gia Mạnh, Giáo trình Hệ thống thông tin quản lý, NXB Thống Kê, 2017

[42]. Nguyễn Văn Thanh, Giáo trình Thanh toán trong TMĐT, NXB Thống Kê, 2011

[43]. Thân Danh Phúc, Giáo trình Quản lý nhà nước về thương mại, NXB Thống Kê, 2015

[44]. Hoàng Đăng Hải, Quản lý An toàn thông tin, NXB Khoa học và Kỹ thuật, 2018

TIẾNG NƯỚC NGOÀI

[45]. Sunil Gupta, Driving Digital Strategy: A Guide to Reimagining Your Business, arvard Business Review Press, 2018

[46]. Bernd W. Wirtz, Digital Business Models, Concepts, Models, and the Alphabet Case Study, Springer, 2019

[47]. Kenneth C. Laudon Carol Guercio Traver, E-commerce - business. technology. society, 10th, PEASON 2014

[48]. Andreas Meier & Henrik Stormer, eBusiness & eCommerce - Managing the Digital Value Chain, Springer, 2009

[49]. Dave Chaffey, E-business and E-commerce Management: Strategy, Implementation and Practice – 6th, Pearson Education, 2015

[50]. Damian Ryan, Understanding Digital Marketing - Marketing strategies for engaging the digital Generation - Third edition, Kogan Page Limited, 2014

[51]. Arch G. Woodside & Peter J. LaPlaca, Handbook of Strategic e-Business Management, Springer-Verlag Berlin Heidelberg, 2014.

[52]. Kenneth C. Laudon & Carol Guercio Traver: E-commerce Business, Technology, Society: 13th edition: Pearson Publishing House, 2017.