**ĐỀ CƯƠNG MÔN THƯƠNG MẠI ĐIỆN TỬ**

# Câu 1: Lịch sử phát triển TMĐT và các ứng dụng của TMĐT, phân loại TMĐT và kiến trúc TMĐT

**Lịch sử phát triển:**

Cách phân chia thứ nhất: 6 cấp độ phát triển E-Commerce

– Cấp độ 1 – hiện diện trên mạng: doanh nghiệp có website trên mạng. Ở mức độ này, website rất đơn giản, chỉ là cung cấp một thông tin về doanh nghiệp và sản phẩm mà không có các chức năng phức tạp khác.

– Cấp độ 2 – có website chuyên nghiệp: website của doanh nghiệp có cấu trúc phức tạp hơn, có nhiều chức năng tương tác với người xem, hỗ trợ người xem, người xem có thể liên lạc với doanh nghiệp một cách thuận tiện.

– Cấp độ 3 – chuẩn bị E-commerce: doanh nghiệp bắt đầu triển khai bán hàng hay dịch vụ qua mạng. Tuy nhiên, doanh nghiệp chưa có hệ thống cơ sở dữ liệu nội bộ để phục vụ các giao dịch trên mạng. Các giao dịch còn chậm và không an toàn.

– Cấp độ 4 – áp dụng E-Commerce: website của DN liên kết trực tiếp với dữ liệu trong mạng nội bộ của DN, các hoạt động truyền dữ liệu được tự động hóa, hạn chế sự can thiệp của con người và vì thế làm giảm đáng kể chi phí hoạt động và tăng hiệu quả.

– Cấp độ 5 – E-Commerce không dây: doanh nghiệp áp dụng TMĐT trên các thiết bị không dây như điện thoại di động, pocket PC (máy tính bỏ túi) v.v… sử dụng giao thức truyền không dây WAP (Wireless Application Protocal).

– Cấp độ 6 – cả thế giới trong một máy tính: chỉ với một thiết bị điện tử, người ta có thể truy cập vào một nguồn thông tin khổng lồ, mọi lúc, mọi nơi và mọi loại thông tin (hình ảnh, âm thanh, phim, v.v…) và thực hiện các loại giao dịch.

Cách phân chia thứ hai: 3 cấp độ phát triển

– Cấp độ 1 – thương mại thông tin (I-commerce) doanh nghiệp có website trên mạng để cung cấp thông tin về sản phẩm, dịch vụ… Các hoạt động mua bán vẫn thực hiện theo cách truyền thống.

– Cấp độ 2 – thương mại giao dịch (T-commerce): doanh nghiệp cho phép thực hiện giao dịch đặt hàng, mua hàng qua website trên mạng, có thể bao gồm cả thanh toán trực tuyến.

– Cấp độ 3 – thương mại tích hợp (C-business): website của doanh nghiệp liên kết trực tiếp với dữ liệu trong mạng nội bộ của doanh nghiệp, mọi hoạt động truyền dữ liệu được tự động hóa, hạn chế sự can thiệp của con người và vì thế làm giảm đáng kể chi phí hoạt động và tăng hiệu quả.

**Các ứng dụng của thương mại điện tử:**

Tài liệu tự động hóa ở chuỗi cung ứng và hậu cần

Hệ thống thanh toán trong nước và quốc tế

Quản lý nội dung doanh nghiệp

Nhóm mua

Trợ lý tự động trực tuyến

IM (Instant Messaging)

Nhóm tin

Mua sắm trực tuyến và theo dõi đặt hàng

Ngân hàng điện tử

Văn phòng trực tuyến

Phần mềm giỏ hàng

Hội thảo truyền thông trực tuyến

Vé điện tử

Nhắn tin nhanh

Mạng xã hội

Mua bán dịch vụ trực tuyến

Phân loại:Các chủ thể tham gia phần lớn vào các giao dịch điện tử là: chính phủ,  
doanh nghiệp, người tiêu dùng/khách hàng cá nhân.  
B : đóng vai trò động lực phát triển TMĐT  
C : quyết định sự thành công của TMĐT

G : đóng vai trò định hướng điều tiết và quản lý  
***Kiến trúc TMĐT***

Các thành phần bao gồm:  
• Máy chủ Web, chứa website TMĐT  
• Trung tâm xử lý thanh toán  
• Ngân hàng

• Ngoài ra, hệ thống mạng đóng vai trò truyền dữ liệu là trong  
suốt với quá trình hoạt động của hệ thống.  
Phân theo chủ sở hữu thì hệ thống TMĐT gồm 5 đối tượng:  
• Máy khách, PC của người mua  
• Máy chủ web, làm dịch vụ hosting website TMĐT. Đối tượng  
này có chủ sở hữu là nhà cung cấp dịch vụ webhosting  
• Website TMĐT có webmaster chính là công ty, bán dịch vụ,  
hàng hóa trực tuyến.  
• Trung tâm dịch vụ xử lý giao dịch, chính là đơn vị trung gian  
đứng ra thực hiện giao dịch thanh toán trực tuyến.  
• Các ngân hàng: bắt buộc phải bao gồm ngân hàng thực hiện  
giao dịch thanh toán (có tài khoản của trung tâm xử lý giao dịch  
thanh toán hoặc webmaster trang TMĐT), ngân hàng có tk  
người mua, có thể thêm một số ngân hàng trung gian trong quá  
trình chuyển tiền giữa hai ngân hàng này. Cũng có trường hợp  
một ngân hàng vừa có tài khoản người mua, vừa có tài khoản  
của trung tâm dịch vụ thanh toán.

# Câu 2: Marketing điện tử? so sánh marketing điện tử và marketing truyền thống. Quá trình phát triển của marketing điện tử

Khái niệm: marketing điện tử hay tiếp thị qua mạng, tiếp thị trực tuyến có tên tiếng anh là E – marketing, là quá trình lập kế hoạch về sản phẩm, giá, phân phối và xúc tiến đối với sản phẩm, dịch vụ và ý tưởng để đáp ứng nhu cầu của tổ chức và cá nhân dựa trên các phương tiện điện tử và Internet

So sánh:

|  |  |  |
| --- | --- | --- |
| **Đặc điểm** | **Marketing online** | **Marketing truyền thống** |
| **Phương thức** | Sử dụng internet,các thiết bị số hóa | Chủ yếu sử dụng các phương tiện truyền thông đại chúng |
| **Không gian** | Không bị giới hạn bởi biên giới quốc gia và vùng lãnh thổ | Bị giới hạn bởi biên giới quốc gia và vùng lãnh thổ |
| **Thời gian** | Mọi lúc mọi nơi,phản ứng nhanh, cập nhật thông tin sau vài phút | Chỉ vào một số giờ nhất định, mất nhiều thời gian và công sức để thay đổi mẫu quảng cáo hoặc clip |
| **Phản hồi** | Khách hàng tiếp nhận thông tin và phản hồi ngay lập tức | Mất một thời gian dài để khách hàng tiếp nhận thông tin và phản hồi |
| **Khách hàng** | Có thể chọn được đối tượng cụ thể,tiếp cận trực tiếp với khách hàng | Không chọn được nhóm đối tượng cụ thể |
| **Chi phí** | Thấp,với ngân sách nhỏ vẫn thực hiện được,có thể kiểm soát được chi phí quảng cáo | Cao, ngân sách quảng cáo lớn,được ấn định dùng 1 lần |
| **Lưu trữ thông tin** | Lưu trữ thông tin khách hàng dễ dàng, nhanh chóng | Rất khó lưu trữ thông tin của khách hàng |

# Câu 3: Hợp đồng điện tử: khái niệm, ký kết và quy trình B2B, B2C, C2C

*Khái niệm:*Theo điều 11, mục 1 của luật mẫu về TMĐT của UNCITRAL  
(1996) quy định: “*hợp đồng điện tử được hiểu là hợp đồng được hình  
thành thông qua việc sử dụng thông điệp dữ liệu*”, “Về mặt hình thức  
hợp đồng, trừ khi các bên có quy định khác, chào hàng và chấp nhận  
chào hàng có thể được thể hiện bằng thông điệp dữ liệu. Khi thông  
điệp dữ liệu được sử dụng để hình thành hợp đồng, thì hợp đồng đó  
không bị phủ nhận giá trị pháp lý chỉ vì nó được thể hiện bằng thông  
điệp dữ liệu”.  
Luật giao dịch điện tử VN cũng quy định: “*Hợp đồng điện tử là  
hợp đồng được thiết lập dưới dạng thông điệp dữ liệu theo quy định  
của luật này* ”. thông điệp dữ liệu cũng được quy định cụ thể là thông  
tin được tạo ra, được gửi đi và được lưu trữ bằng phương tiện điện  
tử, cũng theo đó phương tiện điện tử được quy định là phương tiện  
hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính,  
truyền dẫn không dây, quang học, điện tử hoặc công nghệ tương tự

*Ký kết và quy trình:  
B2B*Ký kết hợp đồng điện tử B2B:  
o Thường diễn ra tại các sàn giao dịch điện tử B2B (B2B  
emarketplace),  
o Trao đổi giao dịch qua thư điện tử hoặc mạng truyền tải dữ liệu  
điện tử (EDI)  
Quy trình thực hiện hợp đồng điện tử B2B  
o Cấp độ thứ nhất: các bên tiến hành thanh toán, giao hàng và  
cung cấp dịch vụ như giao dịch truyền thống với sự kết hợp của  
một số ứng dụng công nghệ thông tin.  
o Cấp độ thứ 2: các bên sử dụng những sàn giao dịch điện tử làm  
trung tâm để qua đó tiến hành các giao dịch, thanh toán, phân  
phối, đặc biệt là xử lý chứng từ điện tử  
*B2C*Quy trình thực hiện hợp đồng điện tử B2C  
o Bước 1: Kiểm tra thanh toán;  
o Bước 2: Kiểm tra tình trạng hàng trong kho;  
o Bước 3: Tổ chức vận tải;  
o Bước 4: Mua bảo hiểm;  
o Bước 5: Sản xuất hàng;  
o Bước 6: Dịch vụ;  
o Bước 7: Mua sắm và kho vận;  
o Bước 8: Liên hệ với khách hàng;  
o Bước 9: Xử lý hàng trả lại.

C2C:

Quy trình khách hàng giao dịch và ký kết hợp đồng điện tử trên website của Ebay.com gồm các bước cơ bản như sau:

Bước 1. Đăng ký thành viên

Bước 2. Tìm kiếm sản phẩm;

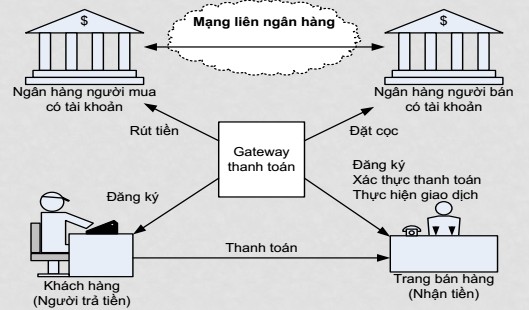
Bước 3. Lựa chọn cách thức mua hàng: Đấu giá, đặt hàng qua Ebay hoặc mua hàng trực tiếp từ Ebay;

Bước 4. Lựa chọn phương thức thanh toán;

Bước 5. Sử dụng My Ebay;

Bước 6. Liên hệ với các thành viên.

# Câu 4: Hệ thống thanh toán điện tử: mô hình B2B, B2C, các phương thức thanh toán, ứng dụng và các nguy cơ mất an toàn: thẻ tín dụng, thẻ ghi nợ, tiền điện tử, smart card, séc điện tử

**Mô hình**

***Các phương thức thanh toán***• Thẻ thanh toán: thẻ tín dụng (credit card), thẻ ghi nợ (debit  
card) và thẻ mua hàng (charge card)  
• Thẻ thông minh  
• Ví điện tử  
• Tiền điện tử  
• Thanh toán qua điện thoại di động  
• Thanh toán điện tử tại nơi bán hàng  
• Séc điện tử  
• Thẻ mua hàng  
• Thư tín dụng điện tử  
• Chuyển tiền điện tử  
***Các nguy cơ mất an toàn***Những rủi ro liên quan đến quá trình thanh toán

• Sao chép, làm giả thiết bị: Trong các hệ thống dựa trên thẻ, làm giả một thiết bị khác được chấp nhận như thiết bị thật, bao gồm cả chìa khóa giải mã, số dư và các dữ liệu khác trên thẻ.

• Sửa đổi, sao chép dữ liệu hoặc phần mềm: phương pháp này làm thay đổi trái phép dữ liệu lưu trữ trên thiết bị của phương tiện thanh toán điện tử.

• Lấy trộm thiết bị: lấy trộm thiết bị của người tiêu dùng hoặc người bán và sử dụng trái phép số dư trên đó

• Không ghi lại giao dịch: Một người sử dụng có thể cố tình không ghi lại giao dịch, không thực hiện nghĩa vụ trả tiền, dẫn tới thất thoát cho người bán cũng như nhà phát hành sản phẩm tiền điện tử

• 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

Rủi ro đối với Ngân hàng phát hành

• Khi chủ thẻ có ý định gian lận, họ sẽ sử dụng thẻ thanh toán ở những điểm tiếp nhận thẻ khác nhau để thực hiện giao dịch có mức thanh toán thấp hơn hạn mức thanh toán, nhưng tổng mức thanh toán lại cao hơn hạn mức thanh toán mà thẻ được phép.

• Lợi dụng tính chất của thẻ để lừa gạt Ngân hàng phát hành thẻ: chủ thẻ có thể thông đồng với người khác, giao thẻ cho người đó sử dụng ở các cơ sở bán hàng chấp nhận thẻ mà không phải là nơi chủ thẻ cư trú (ví dụ, ở nước ngoài). Khi ngân hàng phát hành gửi hóa đơn đến, chủ thẻ sẽ đưa ra những bằng chứng để chối bỏ trách nhiệm với đơn hàng này và từ chối thanh toán

• Chủ thẻ cũng có thể cố tình lấy tiền của ngân hàng bằng cách báo cho Ngân hàng phát hành là thẻ bị thất lạc, nhưng lại vẫn sử dụng thẻ đó để thanh toán trong thời gian thẻ chưa kịp đưa vào danh sách “đen”.

• Những nguyên nhân khách quan khác như:

o Việc sử dụng thẻ giả mạo trùng với thẻ đang lưu hành của Ngân hàng phát hành thẻ.

o Chủ thẻ mất khả năng thanh toán bởi lý do khách quan như tai nạn bất ngờ, không còn khả năng làm việc và mất thu nhập,…

o Rủi ro do các hoạt động gian lận và phi pháp: Lợi dụng sự chưa hoàn hảo trong các hệ thống bảo mật, các dữ liệu về thẻ thanh toán có thể bị đánh cắp và sử dụng bất hợp pháp.

o Thẻ mất cắp, thất lạc (Lost-Stolen Card): 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.

o Thẻ giả (Counterfeit Card): 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. Thẻ giả được sử dụng tạo ra các giao dịch giả mạo, gây tổn thất cho các Ngân hàng. 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.

o Đơn xin phát hành thẻ với thông tin giả mạo (Fraudulent Application): Do không thẩm định kỹ hồ sơ, Ngân hàng phát hành thẻ cho khách hàng mà không biết rằng thông tin trên đơn xin phát hành là giả mạo.

o Chủ thẻ không nhận được thẻ do ngân hàng phát hành gửi (Never received issue): Ngân hàng phát hành gửi thẻ cho chủ thẻ bằng đường bưu điện nhưng thẻ bị thất lạc hoặc bị đánh cắp trên đường gửi.

o Tài khoản của chủ thẻ bị lợi dụng (Account takeover): Đến kỳ phát hành lại thẻ, ngân hàng phát hành nhận được thông báo thay đổi địa chỉ của chủ thẻ.

o Thẻ bị giả mạo để thanh toán qua thư, điện thoại (Mail, telephone order). Nhân viên Cơ sở chấp nhận thẻ giả mạo hoá đơn thanh toán thẻ: (Multiple Imprints).

o Tạo băng từ giả (Skimming): Rủi ro xảy ra là do các tổ chức tội phạm dùng các thiết bị chuyên dụng thu thập thông tin thẻ trên băng từ của thẻ thật

Rủi ro tại ngân hàng thanh toán

• Sai sót trong việc cấp phép

• Không cung cấp kịp thời danh sách “đen” Rủi ro cho cơ sở chấp nhận thanh toán thẻ

Ngân hàng phát hành từ chối thanh toán toàn bộ hóa đơn hàng hóa và dịch vụ mà cơ sở chấp nhận thẻ đã cung ứng do:

• Thẻ hết thời hạn hiệu lực

• Thanh toán nhiều thương vụ vượt hạn mức

• Cố tình tách thương vụ thành nhiều thương vụ nhỏ để không cần phải xin phép.

• Sửa chữa số tiền trên hóa đơn do ghi nhầm hoặc cố ý mà quên rằng phía chủ thẻ cũng giữ một hóa đơn tương tự.

Rủi ro đối với chủ thẻ

• Bị lộ mã số định danh cá nhân – PIN

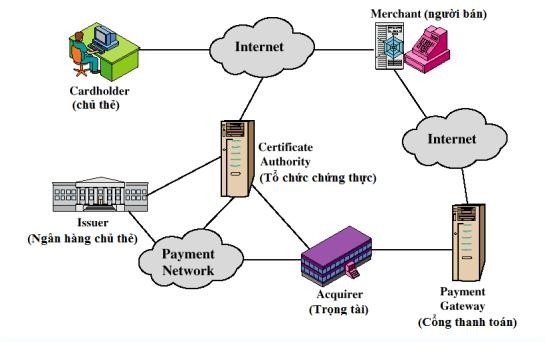
• Thẻ bị mất và bị sử dụng vào mục đích gian lậnCâu 5: Các kỹ thuật đảm bảo an toàn cho TMĐT

# Câu 6: Trình bày về giao thức SET

*Khái niệm:*

Là một chuẩn giao thức truyền thông đảm bảo an toàn cho các giao dịch thẻ tín dụng qua mạng không an toàn (Internet)

*Mô hình hoạt động*



*Quá trình tạo yêu cầu mua*

Yêu cầu mua hàng (Purchase Request) bao gồm 4 giao tác: Initiate Request, Initiate Response, Purchase Request, và Purchase Response. Initiate Request: người mua yêu cầu người bán cung cấp các chứng thực cần thiết (bản sao chứng thực của người bán và cổng thanh toán) cho người mua.

Initiate Response: chứa giá trị ngẫu nhiên (nonce) đã được tạo ra trước đó bởi người mua hàng, một giá trị ngẫu nhiên khác do người bán hàng tạo ra, nhận diện của giao tác hiện hành, cùng với các chứng thực của chính người bán hàng và cổng thanh toán. Tất cả các thông tin này được xác thực bởi

chữ ký của người bán hàng.

Purchase Request: người mua xác minh các chứng thực nhận được rồi gửi thông điệp này cho người bán. Thông điệp này chứa thông tin:

* Thông tin liên quan đến việc thanh toán bao gồm: PI, chữ ký song song, OIMD và một phong bì số (digital envelope). Các thông tin này được mã hoá bằng khoá đối xứng dùng một lần Ks do người mua tạo ra cho từng

phiên giao dịch.

* Thông tin liên quan đến đơn đặt hàng bao gồm: OI, chữ ký song song, PIMD. (OI được gởi đi trực tiếp mà không cần mã hoá).
* Chứng thực của người mua hàng.

Khi người bán nhận được Purchase Request, thực hiện:

* Xác minh chứng thực của người mua hàng.
* Kiểm chứng chữ ký song song của người mua hàng.
* Xử lý đơn đặt hàng và chuyển thông tin thanh toán cho Payment Gateway để kiểm tra.
* Gởi bản tin Purchase Response cho người mua hàng.

Purchase Response: chứa thông tin để chấp nhận đơn đặt hàng. Thông tin này được ký bởi người bán và gởi cho người mua cùng với chứng thực của người bán

Người mua khi nhận được bản tin Purchase Response sẽ tiến hành kiểm tra chữ ký và chứng thực của người bán.

*Xác minh của công ty thương mại đối với yêu cầu mua*

Đây là thủ tục mà người bán hàng xác thực tính hợp lệ của người mua hàng thông qua Payment Gateway. Quá trình xác thực nhằm bảo đảm rằng giao dịch này được chấp thuận bởi ngân hàng phát hành thẻ (Issuer), nghĩa là người bán hàng sẽ được đảm bảo thanh toán. Quá trình này được thực hiện thông qua hai thông điệp: Authorization Request và Authorization response.

Authorization Request: được người bán hàng gởi đến Payment Gateway bao gồm các thông tin sau:

* Thông tin liên quan đến việc mua hàng, bao gồm: PI, chữ ký song song, OIMD và phong bì số (digital envelope).
* Thông tin liên quan đến xác thực bao gồm: nhận diện giao tác, được mã hoá bằng khoá bí mật dùng một lần do người bán hàng tạo ra và phong bì số được mã hoá bằng khoá công khai của Payment gateway.

` • Các chứng thực của người mua hàng và người bán hàng

Khi nhận được Authorization Request, Payment Gateway thực hiện các thao tác sau:

* + - Xác minh tất cả các chứng thực.
    - Giải mã phong bì số của khối thông tin mua hàng.
    - Xác minh chữ ký song song.
    - Giải mã phong bì số của khối thông tin xác thực.
    - Xác minh chữ ký của người bán hàng.
    - Xác minh nhận diện giao tác (transaction ID).
    - Yêu cầu xác thực từ ngân hàng phát hành thẻ.

Nếu nhận được thông tin xác thực thành công từ ngân hàng phát hành thẻ, Payment Gateway sẽ hồi đáp bằng thông điệp Authorization Response tới người bán chứa các thông tin sau:

* + - Thông tin liên quan đến xác thực bao gồm: thông tin xác thực được ký bởi Payment Gateway và mã hoá bằng khoá bí mật do Payment Gateway tạo ra, ngoài ra còn có phong bì số.
    - Thông tin liên quan đến thực hiện thanh toán.
    - Chứng thực của Payment gateway.

Với thông tin xác thực này, người bán đã có thể bắt đầu giao hàng hoặc cung cấp dịch vụ cho người mua.

# Câu 7: Trình bày ưu nhược điểm của tiền điện tử và phương thức lưu trữ, các thuộc tính mong muốn và vấn đề gặp phải.

**Ưu điểm:**

* Chi phí giao dịch thấp ( có những đồng hoàn toàn miễn phí giao dịch)
* Thuận tiện trong giao dịch: Bạn có thể chuyển hoặc nhận tiền điện tử ngay lập tức mà không cần thông qua bên trung gian như ngân hàng, chính phủ,…
* Độ bảo mật an toàn cao, không bị lộ danh tính khi giao dịch ẩn danh.
* Tạo tiềm năng phát triển cho ngành thương mại điện tử
* An toàn và bảo vệ môi trường
* Tiền điện tử không thể làm giả: Vì không tồn tại dưới dạng vật chất và mỗi đồng tiền điện tử tồn tại dưới 1 dãy bit mã hóa duy nhất trên Internet.
* Khả năng sinh lời rất cao, đặc biệt đối với những đồng có giá trị nhỏ
* Có tiềm năng phát triển thương mại điện tử.

**Nhược điểm:**

* Sử dụng không quá dễ dàng: Với những người đã quen sử dụng công nghệ thì vấn đề này không quá khó khăn. Nhưng đối với ai ít có cơ hội tiếp xúc công nghệ thì việc tạo ví và quản lý lại khá khó khăn.
* Giá tiền điện tử thường biến động lên xuống mà chúng ta rất khó để đoán trước được. Điều này gần giống với sự lên xuống của thị trường chứng khoán. Nhà đầu tư giao dịch có nguy cơ bị thua lỗ, mất vốn nếu không thường xuyên theo dõi biến động.
* Là nơi cho tội phạm hoạt động rửa tiền: Có lẽ đây là nhược điểm lớn nhất. Cũng vì lý do này mà có những quốc gia chưa chấp nhận đồng coin là một loại tiền tệ hợp pháp.
* Là mục tiêu hàng đầu của các hacker hiện nay cũng như gắn liền với các hoạt động bất hợp pháp khác
* Đầu tư dễ dẫn đến tình trạng bong bóng tài chính trên Internet

**Phương thức lưu trữ:**

Hiện nay có đa dạng chủng loại ví tiền điện tử phục vụ cho nhiều mục đích sử dụng khác nhau. Nếu ưu tiên hàng đầu của bạn là tính riêng tư, bạn đơn giản có thể sử dụng một tờ giấy hoặc một ví phần cứng. Đây là cách an toàn nhất để lưu trữ quỹ crypto. Ngoài ra, trên thị trường cũng cung cấp những ví “lạnh” (offline) được lưu trữ trên đĩa cứng hoặc ví trực tuyến, liên kết với sàn giao dịch hoặc các nền tảng độc lập.

**Phần này mình bịa ra thôi chưa chắc đúng bạn nào biết có thể trả lời:**

**Các thuộc tính muốn có ở tiền điện tử:** Tiền điện tử có tất cả các thuộc tính nội tại như tiền vật lý (tiền giấy, tiền xu) và chúng cho phép các giao dịch tức thời có thể được thực hiện liền mạch để thực hiện thanh toán qua biên giới khi được kết nối với các thiết bị và mạng được hỗ trợ.

**Các vấn đề của tiền điện tử:**

Rủi ro khi sử dụng tiền điện tử

Biến động của thị trường điện tử

Quan điểm về tiền điện tử thay đổi theo thời gian

# Câu 8: Trình bày smart card và ứng dụng của nó

Thẻ thông minh (Smart Card) đang được ứng dụng rộng rãi tại Việt Nam trong nhiều lĩnh vực như viễn thông, ngân hàng, thương mại điện tử, điều khiển tự động, kiểm soát người và phương tiện… Các ứng dụng của thẻ thông minh rất thiết thực, dễ triển khai và tích hợp phần mềm điều khiển bởi ưu điểm vượt trội về khả năng lưu trữ, xử lý thông tin và bảo mật dữ liệu. Để có cái nhìn tổng quan về thẻ thông minh, cần tìm hiểu về cấu tạo, nguyên lý hoạt động, các loại thẻ thông minh trên thị trường, cách thức phát triển phần mềm quản lý thẻ thông minh, từ đó đề xuất ý tưởng sử dụng thẻ thông minh trong hoạt động kiểm tra, kiểm soát của Bộ đội Biên phòng.

1. Cấu tạo và nguyên lý hoạt động

Thẻ thông minh là một loại thẻ nhựa, kích thước theo chuẩn ID-1 (ISO/IEC 7810) là 85,60 × 53,98mm hoặc chuẩn ID-000 kích thước 25 x 15mm, bề dày mặt thẻ là 0,76mm. Thẻ được gắn một bộ mạch tích hợp (Integrated Card) cho phép giao tiếp với hệ thống, tính toán, mã hóa đảm bảo tính toàn vẹn của dữ liệu. Dung lượng bộ nhớ trên thẻ thông minh khá lớn, từ 64KB - 128KB (tương đương 65.536 đến 131.072 ký tự).

Thẻ thông minh có thể là thẻ nhớ (Read Only Memory) chỉ lập trình, xóa được bằng tín hiệu điện hoặc là thẻ có gắn một bộ vi xử lý kích thước rất nhỏ kết hợp với bộ nhớ truy cập ngẫu nhiên (Random Access Memory), các bộ phận này có vai trò tương tự như một máy tính. Tài nguyên trên thẻ được quản lý bởi hệ thống quản trị trung tâm cho phép trao đổi thông tin, cấu hình và cài đặt dữ liệu thẻ.

Phân loại thẻ thông minh:

Thẻ tiếp xúc (contact card): Là loại thẻ có tiếp điểm mạ vàng diện tích khoảng 1cm2, được chia thành các phần riêng biệt gồm đầu vào, ra dữ liệu, tín hiệu reset (phục hồi trạng thái ban đầu của thẻ), tín hiệu xung đồng hồ, chân điện áp.

Để đọc, ghi thông tin, bề mặt chip phải tiếp xúc trực tiếp với đầu đọc thẻ. Loại thẻ này được sử dụng nhiều trong tài chính và truyền thông (sim điện thoại) vì ưu điểm giá cả rẻ, 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 không tiếp xúc (contactless card): Là loại thẻ mà chip trên nó liên lạc với máy đọc thẻ thông qua công nghệ sóng vô tuyến RFID (Radio Frequency Identification) với tốc độ trao đổi dữ liệu từ 106 đến 848kbit/s, thân thẻ chứa chip và đường dây ăngten được dấu ngầm. Ăngten đi vòng quanh thẻ, nó có nhiệm vụ làm trung gian nhận/phát sóng radio giữa đầu đọc thẻ và chip trên thẻ. Trong thẻ có một cuộn cảm có khả năng dò tín hiệu vô tuyến trong một dài tần nhất định, chỉnh lưu tín hiệu và dùng nó để cung cấp năng lượng hoạt động cho chip trên thẻ, khoảng cách giao tiếp giữa đầu đọc thẻ và máy khoảng 10cm. Tốc độ xử lý của thẻ không tiếp xúc nhanh hơn so với thẻ tiếp xúc, vì vậy thẻ không tiếp xúc thường được ứng dụng tại những nơi cần phải xử lý nhanh như kiểm soát phương tiện công cộng, xe bus, thẻ ra vào…thẻ không tiếp xúc đắt hơn thẻ tiếp xúc, tuy nhiên độ bảo mật thông tin không an toàn bằng thẻ tiếp xúc.

Thẻ lưỡng tính: 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 2 loại thẻ trên.

Đầu đọc thẻ thông minh: Là đầu đọc dùng cho việc giao tiếp với thẻ, dữ liệu và điện năng được truyền trực tiếp hoặc gián tiếp qua công nghệ RFID từ thẻ vào máy đọc. Đầu đọc thẻ dễ dàng tích hợp vào các hệ thống khác nhau thông qua thiết bị đầu cuối. Tùy vào công nghệ sử dụng, có 2 dạng cổng kết nối là USB và COM. Nếu sử dụng kết nối USB tốc độ truyền tín hiệu đạt 12 Mbps (High speed), điện áp cung cấp thông thường 5V (DC), 200mA.

2. Một số loại thẻ thông minh

Hiện tại, trên thị trường có rất nhiều loại thẻ thông minh, tuy nhiên chỉ một số loại sau đây được sử dụng nhiều nhất:

Thẻ Combi (combi card): Là thẻ thông minh lưỡng tính, có cách thức giao tiếp kép, thẻ chỉ bao gồm một chíp thông minh có bản mặt tiếp xúc và có hệ thống ăngten truyền phát tín hiệu RFID.

Thẻ chíp hoặc IC: Gồm một tổ hợp mạch nhúng có bộ nhớ và khả năng xử lý vi mô được sử dụng để lưu giữ thông tin những giao dịch của người sử dụng thẻ. Thẻ có thể được gắn 1 hoặc 2 chip bán dẫn như các loại thẻ nhớ để bảo vệ thông tin hay xử lý các quy trình tự động.

Thẻ thông minh đa ứng dụng (multi-applications smart card): Là thẻ thông minh vi mạch được dùng trong nhiều ứng dụng với dung lượng bộ nhớ lớn và khả năng xử lý nhanh như một máy vi tính, đáp ứng các yêu cầu khác nhau của từng ứng dụng. Thẻ này có độ bảo mật dữ liệu rất cao.

Thẻ từ (magnetic stripe card): Là loại thẻ có dải từ kim loại trên bề mặt, thẻ có thể ghi, xóa thông tin trực tiếp bằng máy in thẻ từ. Đây là công nghệ chuẩn cho các thẻ dùng trong ngân hàng như thẻ tín dụng, thẻ ghi nợ…

Thẻ quang Hologram (hologram card): Là thẻ nhận dạng có phủ lớp tạo ánh sáng 3 chiều, các thông tin trên thẻ quang được bảo mật rất tốt, thẻ quang thường được sử dụng như một biện pháp an ninh hữu hiệu để chống lại sự giả mạo, đảm bảo tích xác thực của chủ thẻ.

3. Các ứng dụng của thẻ thông minh

Ứng dụng cơ bản và thông dụng của thẻ thông minh bao gồm thẻ tín dụng (thẻ ATM), thẻ đổ xăng, SIM cho điện thoại di động, thẻ truyền hình cho các kênh phải trả tiền, các thẻ dùng cho thu phí giao thông tự động. 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 an ninh cho máy tính, hệ thống mã hóa dữ liệu trên đĩa cứng (phần mềm FreeOTFE) có thể dùng thẻ thông minh để giữ các khóa mã bảo mật, tạo thêm một lớp cho việc mã hóa các dữ liệu quan trọng trên đĩa. Trình duyệt web Mozilla Firefox cũng dùng thẻ thông minh để lưu trữ chứng nhận thông tin người dùng giúp cho việc duyệt web an toàn nhất. Thẻ thông minh còn được dùng cho việc xác nhận và cho phép truy cập đến các máy tính mà không phải sử dụng thêm một phương tiện nào khác như mật khẩu.

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) 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.

Hệ thống giấy phép lái xe dùng thẻ thông minh sẽ lưu trữ và cập nhật thông tin vi phạm và số tiền phạt của tài xế. Thẻ cũng lưu thông tin cá nhân, loại và số giấy phép cũng như ảnh của chủ thẻ. Ngoài ra, các thông tin cần thiết cho cấp cứu như nhóm máu, sinh trắc học cũng được lưu vào trong chip nếu người chủ thẻ yêu cầu.

4. Thực trạng sử dụng thẻ thông minh ở Việt Nam

Trong lĩnh vực tài chính, ngân hàng, bảo hiểm: Đây là lĩnh vực có nhu cầu sử dụng thẻ lớn nhất tại Việt Nam để giao dịch, thanh toán, quản lý tài khoản,… Bên cạnh nhu cầu lớn thì yêu cầu về bảo mật, mã hóa thông tin của thẻ ở lĩnh vực này cũng đòi hỏi rất cao. Một trong những công ty cung cấp thẻ thông minh cho ngành tài chính, ngân hàng là MK Smart. MK Smart là công ty duy nhất ở Việt Nam đã đạt 3 chứng chỉ quốc tế về an ninh sản xuất thẻ bảo mật bao gồm S.A.S, VISA và MASTER CARD.

Việc sử dụng thẻ thông minh trong lĩnh vực này đang làm thay đổi phương thức thanh toán. Các nhà cung cấp và triển khai giải pháp thẻ thông minh tại các ngân hàng đã đầu tư, mở rộng mạng lưới các thiết bị sử dụng thẻ góp phần tăng số lượng các giao dịch thanh toán không sử dụng tiền mặt.

Dự án chứng minh thư điện tử của Bộ Công an: Đây là dự án sử dụng thẻ thông minh lớn nhất tại Việt Nam. Mỗi công dân sẽ được cấp 1 thẻ, để xây dựng cơ sở dữ liệu chứng minh điện tử, cần tiến hành thu thập các thông tin sinh trắc học như ảnh số, các đặc điểm nhận dạng, dấu vân tay, họ tên, địa chỉ, giới tính và ngày sinh của chủ thẻ,… sau khi hoàn tất quá trình xử lý, thông tin sẽ được lưu trữ trên hệ thống máy chủ và trên vi mạch nhớ của thẻ. Mỗi người dân sẽ được cấp cho một mã ngẫu nhiên 12 chữ số. Các thông tin khác như hộ chiếu, bằng lái xe hay thẻ y tế đều dùng chung mã số của chứng minh thư điện tử.

Trong lĩnh vực giao thông: hệ thống thu phí tự động sử dụng thẻ kiểm soát RFID đã được triển khai ở các đường cao tốc mới của Việt Nam. Tất cả các phương tiện khi vào đường cao tốc đều được nhận dạng, mã hóa các dữ liệu liên quan như thời gian vào, tên trạm vào, biển kiểm soát, loại xe… lưu trên thẻ kiểm soát RFID và phát cho chủ phương tiện. Trước khi phương tiện đi ra đường cao tốc lái xe sẽ trả thẻ kiểm soát cho nhân viên thu phí, đồng thời các thiết bị đọc sẽ đọc các dữ liệu trên thẻ và máy tính sẽ tự động tính toán đưa ra mức phí phải trả dựa trên loại xe, số ki lô mét đường cao tốc phương tiện đã sử dụng. Sau khi nhận tiền, máy tính sẽ tự động in hóa đơn (vé cước phí) và mở barie cho phương tiện đi qua.

Với việc triển khai hình thức thu phí kín sử dụng thẻ RFID phương tiện qua trạm sẽ bỏ qua được giai đoạn kiểm tra và soát vé đồng thời thời gian trao đổi dữ liệu giữa chip nhớ và máy tính được diễn ra trong thời gian rất ngắn do đó sẽ giảm thời gian lưu thông của xe qua trạm. Hơn nữa, hệ thống thu phí kín dùng máy tính tự động tính toán mức phí trên cơ sở số ki lô mét đường cao tốc phương tiện sử dụng nên bảo đảm tính minh bạch và công bằng cho người sử dụng đường cao tốc, thuận lợi trong quá trình giám sát, hậu kiểm, hạn chế tối đa các tiêu cực trong công tác thu phí.

Trong viễn thông: tất cả các sim điện thoại ở Việt Nam đều là các thẻ thông minh tiếp xúc. Chức năng chính của sim là thẻ nhận dạng thuê bao di động (đặc trưng bởi số IMSI - International Mobile Subscriber Identity - mỗi sim có 1 số duy nhất trên thế giới), sim còn chứa các dữ liệu khác như các mã số PIN, PIN2, PUK, PUK2, số của trung tâm dịch vụ nhắn tin SMS, danh bạ điện thoại…, đây là một ứng dụng phổ biết nhất ở Việt Nam.

5. Sử dụng thẻ thông minh vào hoạt động kiểm tra, kiểm soát của Bộ đội Biên phòng

Với đặc thù của lực lượng Bộ đội Biên phòng (BĐBP) kiểm soát số lượng lớn cửa khẩu, lối mở dọc biên giới đất liền và các cửa khẩu cảng biển, lượng hành khác, phương tiện xuất nhập cảnh qua các cửa khẩu luôn tăng theo từng năm. Việc ứng dụng công nghệ thẻ thông minh vào hoạt động kiểm tra, kiểm soát cần tập trung phát triển trên một số loại thẻ:

1. Thẻ thông minh chứa chíp: Hiện tại trên thị trường loại thẻ này khá phổ biến, giá thành rẻ. Ứng dụng thẻ thông minh chứa chíp để kiểm soát vào ra của BĐBP phải xây dựng thêm hệ thống phần mềm tích hợp dựa trên bộ công cụ phát triển phần mềm SDK (Software Developement Kit) được phân phối bởi nhà cung cấp thẻ và thiết bị. Các module phần mềm phải phát triển bao gồm phần ghi thông tin hành khách vào thẻ, mã hóa thông tin trên thẻ, đọc thẻ và giải mã thông tin để cập nhật vào hệ thống cơ sở dữ liệu kiểm tra, giám sát của BĐBP.

2. Hộ chiếu điện tử mới: Hộ chiếu điện tử có hình dạng giống như các loại hộ chiếu hiện hành nhưng được gắn thêm một con chip điện tử mỏng ở bìa sau (thực chất là 1 thẻ thông minh không tiếp xúc). Khi sản xuất hộ chiếu, các thông tin về thân nhân theo chuẩn ICAO của tổ chức hàng không dân dụng thế giới được lưu trữ vào chíp này. Chip trong hộ chiếu là chip nhận dạng tần số radio (RFID), thông tin trên chíp còn có thể chứa thêm dấu vân tay và đặc điểm sinh trắc học của của người mang hộ chiếu. Chíp trên hộ chiếu được cấu tạo bằng vật liệu đặc biệt để ít bị ảnh hưởng bởi các lực tác động, chống hấp thụ nhiệt để bảo vệ các linh kiện điện tử hoạt động ổn định.

Để kiểm soát việc vào ra bằng hộ chiếu điện tử chỉ cần phát thêm module phần mềm đọc thông tin trên hộ chiếu, trang bị thêm máy đọc hộ chiếu điện tử. Máy đọc hộ chiếu sẽ kiểm tra sự tồn tại của chip RFID, nếu không có, hộ chiếu này sẽ được coi như hộ chiếu thông thường và quy trình kiểm tra của kiểm soát viên BĐBP sẽ tuân thủ đúng quy trình truyền thống. Nếu có chíp RFID, hệ thống sẽ tiến hành đọc dữ liệu trong thẻ nhớ và kiểm tra tính hợp lệ của những dữ liệu qua hệ thống chữ ký số Signing Certification Authority (SCA), song song với bước này, kiểm soát viên kết hợp tiến hành kiểm tra an ninh của hộ chiếu điện tử về mặt trực quan, khi hợp lệ các thông tin trên hộ chiếu sẽ được đọc vào máy tính và tiến hành làm thủ tục cho hành khách.

3. Hệ thống thẻ từ: Thẻ từ cũng là một loại thẻ thông minh, một hệ thống ứng dụng thẻ từ kiểm soát vào ra gồm bốn thành phần chính là thẻ gốc, các đầu đọc (Reader) hoặc sensor (cái cảm biến) để truy cập các thẻ, máy chủ chứa hệ thống phần mềm giao diện (host computer - server and sortware) và cơ sở hạ tầng truyền thông gồm hệ thống mạng có dây, không dây. Các bộ phận này kết nối với nhau để hệ thống kiểm tra, kiểm soát vào ra hoạt động có hiệu quả.

Dữ liệu của khách được lưu trữ trên bề mặt từ tính phía sau của thẻ. Khi đọc thẻ thông tin sẽ được truyển trực tiếp tới máy tính kết nối với đầu đọc, phần mềm quản lý tiến hành kiểm tra các thông tin trên thẻ, nếu hợp lệ thông tin xuất nhập cảnh sẽ được lưu trữ vào hệ thống máy tính.

4. Hệ thống thẻ mã vạch: Thẻ chứa mã vạch là thẻ nhựa, không chứa chíp nhưng quy trình quản lý, hoạt động tương tự hệ thống thẻ thông minh. Thông tin về hành khách được mã hóa theo chuẩn mã vạch (thường dùng code 39 hoặc 128) và được in trên thẻ, để đọc thông tin thẻ, sử dụng đầu đọc mã vạch. Đây là giải pháp hợp lý, kinh tế nhất để kiểm soát hành khách xuất nhập cảnh của BĐBP. Đầu đọc mã vạch có tốc độ đọc nhanh, đáng tin cậy, được thiết kế kiểu dáng gọn tạo cảm giác thoải mái khi sử dụng, lắp đặt đơn giản, không mất thời gian đào tạo người dùng.

# Câu 9: Các kỹ thuật bảo mật giao dịch thanh toán

*Nhóm 1: bảo mật giao dịch thanh toán:*

* + - Người dùng nặc danh: bảo vệ không tiết lộ danh tính người dùng trong mạng giao dịch;
    - Không theo dấu được địa điểm: bảo vệ chống tiết lộ địa điểm phát lệnh giao dịch;
    - Người trả tiền nặc danh: bảo vệ không tiết lộ danh tính người trả tiền;
    - Không theo dấu được giao dịch thanh toán: bảo vệ không liên hệ hai giao dịch thanh toán khác nhau của cùng một khách hàng không liên kết với nhau;
    - Bảo mật dữ liệu giao dịch bảo vệ chống tiết lộ các dữ liệu cụ thể trong giao dịch;
    - Chống từ chối thông điệp giao dịch thanh toán: không cho phép từ chối nguồn xuất phát thông điệp giao thức xuất phát giao dịch thanh toán;
    - Không lặp thông điệp giao dịch

*Nhóm 2: Bảo mật tiền điện tử*

* + - Bảo vệ chống tiêu tiền nhiều lần: trên cùng một khối lượng tiền;
    - Chống giả mạo tiền: chống bên không phép tạo ra tiền điện tử giả;
    - Bảo vệ tiền không bị ăn trộm, sao chép.

*Nhóm 3: Bảo mật Séc điện tử*

* + - Dựa trên công nghệ đặc thù của hệ thống thanh toán này.
    - Có dịch vụ Trung gian chuyển & chứng nhận thanh toán: B1: bên xác thực hợp pháp đứng ra chứng nhận,

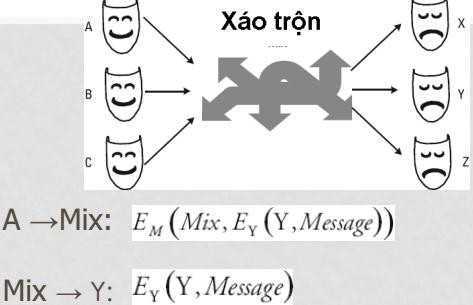
B2: chuyển tiếp tới bên xác thực trung gian tiếp theo được lựa chọn theo nguyên tắc xác thực có giới hạn

# Câu 10: Các kỹ thuật nặc danh người dùng không theo dấu địa điểm. Bài toán áp dụng: mã hóa dữ liệu và hàm trộn Mix

*Nặc danh người dùng:*

Phương pháp: sử dụng chuỗi xáo trộn

* + - Thông tin được gửi từ Khách hàng A -> mix,
    - Từ mix -> X (người bán, hoặc ngân hàng muốn biết thông tin khách hàng)
    - Thông tin được mã hóa bằng khóa công khai của Mix: EM



Hạn chế: Mix phải hoàn toàn tin cậy

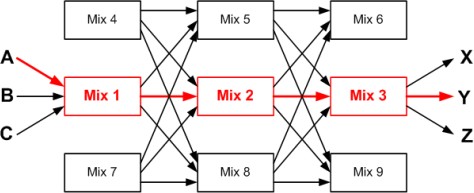
* + - Nhiều mix: bảo vệ chống lại trước tấn công

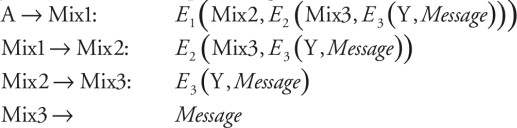
Gửi thông tin giả từ A,B,C -> Mix và từ Mix->X,Y,Z

Các thông tin (giả + nguyên bản) chia thành các khối, cố định, mã hóa => gửi đi =>không thể đọc được

* + - Lựa chọn 1 mix ngẫu nhiên là chuỗi xáo trộn thật
    - Ei là khóa công khai của Mix (i=1,2,3…)







Nhận xét:

* + - * Cần phải có mix tin cậy
      * Giá thành cao,
      * Công nghệ và điểm thực hiện phức tạp

# Câu 11: Các kỹ thuật giúp không theo dấu thanh toán

Hàm băm ngẫu nhiên iKP

• là 1 phần của cơ chế bảo mật tiền điện tử

• Khách hàng tạo 1 tên giả theo công thức:

IDC = hK (RC , BAN)

• RC : số ngẫu nhiên do khách hàng lựa chọn khi bắt đầu giao dịch

• BAN: số tài khoản ngân hàng của Khách hàng

• hK : Hàm hash 1 chiều

• IDC : tên giả, tên ảo của khách hàng

Người bán

Chỉ nhận được IDC, không thể tính được BAN, do không biết RC Mỗi giao dịch, người mua lựa chọn RC khác nhau

Người bán nhận được IDC khác nhau

Không thể liên kết 2 giao dịch có cùng số BAN

Hàm băm ngẫu nhiên theo SET

• Người bán chỉ nhận được duy nhất hashsum của hướng dẫn thanh toán

o Số tài khoản chính, PAN (vd: số thẻ tín dụng)

o Ngày hết hạn lưu hành thẻ

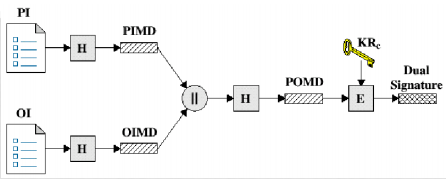
o Giá trị bí mật của chủ thẻ, cổng thanh toán, và dịch vụ xác thực cùng chia sẻ (CVV)

o Exnonce

• Số nonce khác nhau => người bán cũng không thể liên kết được 2 giao dịch có cùng số PAN

# Câu 12: Chữ ký kép, khái niệm, mục đích

*Khái niệm:*Gắn hai thông điệp cho hai người nhận khác nhau thành một thông  
điệp gồm có:  
• Thông tin đặt hàng  
• Thông tin thanh toán  
*Mục đích:*Hạn chế thông tin nhạy cảm đến những thành phần không cần biết  
• Công ty thương mại không cần phải biết đến số của thẻ tín dụng  
• Ngân hàng không cần biết đến thông tin chi tiết của đơn đặt  
hàng của khách hàng  
• Tạo ra khả năng bảo vệ bằng cách giữ thông tin các đối tượng  
này một cách riêng rẽ  
*Các bước tạo và xác minh chữ ký kép:*Ký hiệu:  
• P là cổng thanh toán  
• OI là thông tin đặt hàng (Order Information)  
• PI là hướng dẫn thanh toán (Payment Information)  
• M là người bán

  
Các bước thực hiện hai chữ ký như sau  
• Lấy giá trị hàm băm của đơn đặt hàng và thông tin thanh toán  
• Hai giá trị băm này được gắn kết với nhau *[H(PI) áá H(OI)]* và được băm tiếp  
• Khách hàng mã hóa giá trị băm cuối cùng với khóa bí mật

*DS = Eprivate key C [ H(H(PI) áá H(OI)) ]*Chữ ký được xác minh bởi công ty thương mại  
Công ty thương mại có  
• Giá trị DS  
• khóa công khai của khách hàng nhận được từ chứng chỉ của khách  
hàng,  
• Giá trị băm của thông tin thanh toán (PIMD)  
• Thông tin về đơn hàng OI  
• Công ty thương mại có thể tính hai giá trị này, và hai giá trị này phải  
bằng nhau:  
*H(PIMD áá H(OI))  
Dpublic key C[DS]*Chữ ký được xác minh bởi ngân hàng  
Ngân hàng được có các thông tin gồm:  
• giá trị DS,  
• Thông tin thanh toán PI,  
• giá trị băm OI (OIMD)  
• khóa công khai của khách hàng  
Ngân hàng dựa trên đó có thể tính được các giá trị sau:  
*H(H(PI) || OIMD)  
Dpublic key C [ DS ]*

# Câu 13: Trình bày Họ giao thức IKP, so sánh họ giao thức IKP

Khái niệm: iKP là họ các giao thức thanh toán do trung tâm nghiên cứu của IBM phát triển.

Họ giao thức con

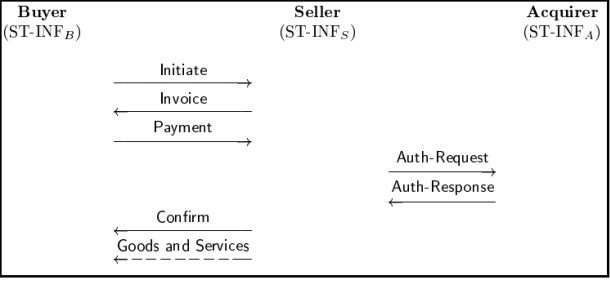
- iKP (i = 1,2,3; KP = key protocol)

- sự khác nhau về số lượng căp khóa công khai của mỗi bên tạo ra các giao thức con (bên mua (B), bên bán(S), cổng thanh toán(A))

+ 1KP: chỉ A có cặp khóa công khai

+ 2KP: A và S có cặp khóa công khai

+ 3KP: A, S, B có cặp khóa công khai

*Các bước thực hiện giao dịch trong các giao thức con*

1KP:

Trước khi giao thức bắt đầu, mỗi bên X ∈ àA; B; Sâ có một số thông tin bắt đầu được đại diện bởi ST-INFX.

1. Initiate:
   * Người mua tạo ra một tên giả dùng một lần bằng cách tạo một số ngẫu nhiên *RB* và tính *IDB = Hk(RB, BAN).*
   * Người mua tạo ra một số ngẫu nhiên khác là SALT B dùng để “salting” bảng băm của mô tả đơn hàng (DESC) trong các luồng tiếp theo.
   * Người mua gửi luồng Initiate.



1. Invoice:
   * Người bán lấy ra SALTB và IDB từ Initiate. Có được DATE. Tạo đại lượng ngẫu nhiên (nonce) NONCES (Sự kết hợp của

DATE và NONCES được dùng bởi A để nhận dạng thanh toán này).

* + Người bán lựa chọn id giao dịch TIDS để xác định ngữ cảnh và tính Hk(SALTB, DESC).
  + Người bán tạo Common: AUTHPRICE, IDS , TIDS , DATE, NONCES, IDB, Hk(SALTB, DESC) và tính H(Common).
  + Người bán gửi luồng Invoice. (CERTA có thể được gắn thẻ vào thông điệp này hoặc gửi cho B sau, ví dụ, cùng với thông điệp Confirm.)



Clear: IDS , TIDS , DATE, NONCES, H(Common)

IDS : Id người bán.

1. Payment:
   * Người mua lấy Clear: IDS , TIDS , DATE, NONCES, H(Common)) từ Invoice.
   * Người mua xác nhận DATE trong khoảng thời gian đã xác định trước.
   * Người mua đã có AUTHPRICE và IDB.
   * Người mua tính Hk(SALTB, DESC).
   * Người mua tạo Common: AUTHPRICE, IDS , TIDS, DATE, NONCES, IDB, Hk(SALTB, DESC) và tính H(Common).
   * Kiểm tra giá trị H(Common) vừa tính với giá trị H(Common) nhận được trong Clear xem nó có phù hợp hay không.
   * (Phù hợp) Người mua tạo SLIP: AUTHPRICE, H(Common), BAN, RB, [PIN[SALTC]], EXPIRATION (với mã PIN là tùy chọn).
   * Người mua mã hóa SLIP bằng khóa công khai của cổng thanh toán: EncSlip = EA(SLIP)
   * Người mua gửi luồng Payment.
2. Auth-Request:

Người bán chuyển tiếp EncSlip cùng với Clear và Hk(SALTB, DESC) tới cổng thanh toán, yêu cầu cổng thanh toán ủy quyền thanh toán.



1. Auth-Response:

Cổng thanh toán lấy: Clear, EncSlip và Hk(SALTB, DESC) từ Auth- Request, sau đó thực hiện như sau:

1. Lấy từ Clear: IDS , TIDS , DATE, NONCES, H(Common)). Đặt giá trị h1 = H(Common). Giờ đây A kiểm tra các lần phát lại, tức là đảm bảo rằng không có yêu cầu xử lý trước đó với cùng một bộ bốn: IDS

, TIDS , DATE và NONCES.

1. Giải mã EncSlip.

* Nếu giải mã không thành công -> EncSlip đã bị thay đổi (bởi attacker hoặc bởi S) -> giao dịch không hợp lệ.
* Ngược lại, nhận được SLIP : AUTHPRICE, H(Common), BAN, EXPIRATION, RB và PIN (tùy chọn). Đặt giá trị h2 = H(Common). (3)Cổng thanh toán kiểm tra giá trị h1 với h2. (phù hợp) đảm bảo rằng người mua và người bán đã thỏa thuận về thông tin đặt hàng (giá, danh

tính của người bán,…)

1. Cổng thanh toán xây dựng lại Common:

* SLIP: AUTHPRICE, H(Common), BAN, RB, [PIN[SALTC]], EXPIRATION
* Clear: IDS, TIDS, DATE, NONCES, H(Common))
* Tính IDB = Hk(RB, BAN) (vì có RB và BAN từ SLIP).
* Auth-Request: Hk(SALTB, DESC).

=> Common: AUTHPRICE, IDS, TIDS, DATE, NONCES, IDB, Hk(SALTB, DESC)

* Tính H(Common) và kiểm tra xem có khớp với h1 ở trên.

1. A chuyển tiếp: BAN, EXPIRATION, PIN (nếu có), giá cả,… (như được quy định bởi hệ thống ủy quyền) tới hệ thống thanh toán bù trừ và ủy quyền hiện có của tổ chức thẻ tín dụng để có được sự cho phép trực tuyến về khoản thanh toán này.

* Khi nhận được phản hồi RESPCODE từ hệ thống ủy quyền, cổng thanh toán tạo chữ ký:

SigA = SA(RESPCODE, H(Common))

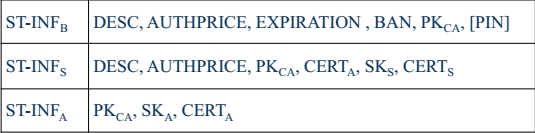
* Cổng thanh toán gửi luồng Auth-Response

1. Confirm:
   * Người bán lấy RESPCODE và SigA từ AuthResponse.
   * Xác minh SigA
   * Người bán chuyển RESPCODE và SigA cho người mua.

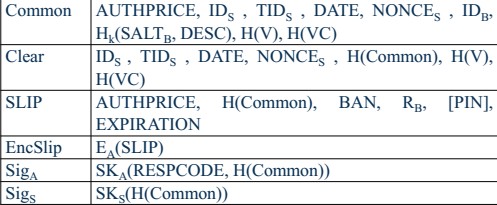
Nhận xét 1KP:

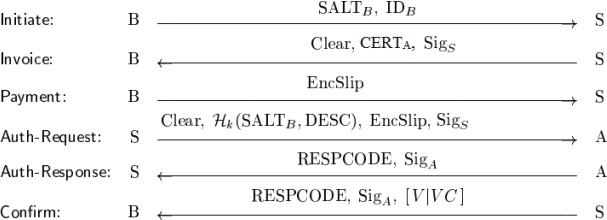
* Chỉ yêu cầu cổng thanh toán sở hữu cặp khóa công khai – bí mật;
* Người mua được xác thực qua cổng thanh toán dựa trên số tài khoản và mã PIN tùy chọn;
* Thông tin thanh toán được mã hóa bằng khóa công khai của cổng thanh toán;
* Không cung cấp việc chống chối bỏ đối với các thông điệp được gửi bởi người mua và người bán

2KP:

Trước khi giao thức bắt đầu, mỗi bên X ∈ àA; B; Sâ có một số thông tin bắt đầu được đại diện bởi ST-INFX.

Các trường kết hợp

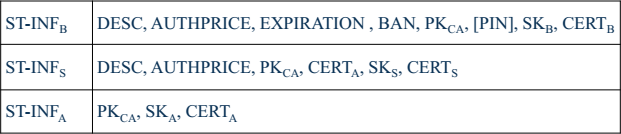


Luồng giao thức

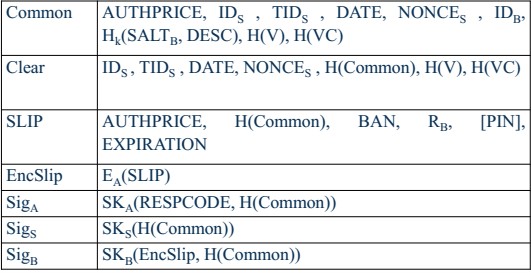
Nhận xét 2KP:

* Cổng thanh toán và người bán sở hữu cặp khóa công khai – bí mật cho mỗi bên;
* Người mua được xác thực qua cổng thanh toán dựa trên số tài khoản và mã PIN tùy chọn;
* Thông tin thanh toán được mã hóa bằng khóa công khai của cổng thanh toán;
* Cung cấp tính chống chối bỏ với các thông điệp được gửi bởi người bán;
* Không cung cấp việc chống chối bỏ đối với các thông điệp được gửi bởi người mua.

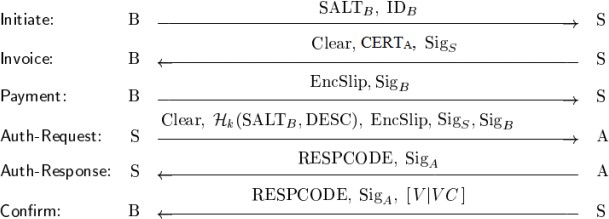
3KP:

Trước khi giao thức bắt đầu, mỗi bên X ∈ àA; B; Sâ có một số thông tin bắt đầu được đại diện bởi ST-INFX.

Các trường kết hợp



Luồng giao thức



Nhận xét 3KP:

* Cổng thanh toán, người bán và người mua sở hữu cặp khóa công khai – bí mật cho mỗi bên;
* Người mua được xác thực qua cổng thanh toán dựa trên số tài khoản và mã PIN tùy chọn và chữ ký số của người mua;
* Thông tin thanh toán được mã hóa bằng khóa công khai của cổng thanh toán;
* Cung cấp tính chống chối bỏ với các thông điệp được gửi bởi tất cả các bên tham gia.

# Bài tập

Chữa 1 bài đơn giản đủ 3 bước cho anh em. Lưu ý học thuộc Base64 nhé cứ nhờ theo thứ tự bảng chữ cái trong tiếng anh 0-25⬄A-Z, 26-51⬄a-z, 52-61⬄ 0-9, 62⬄+, 63⬄/

