**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------------------------------



**BÁO CÁO CHUYÊN ĐỀ AN TOÀN PHẦN MỀM**

**Đề tài:**

**“XÂY DỰNG HỆ THỐNG THANH TOÁN AN TOÀN THEO CHUẨN BẢO MẬT SET”**

**Giáo viên : TH.S HUỲNH TRỌNG THƯA**

**Sinh viên thực hiện : NGUYỄN QUỐC ĐẠT - N14DCAT124**

**NGUYỄN VŨ ĐỨC ANH – N14DCAT022**

**Lớp : D14CQAT01-N**

**Khóa : 2014-2019**

**Hệ : ĐẠI HỌC CHÍNH QUY**

**TP.HCM, THÁNG 11/2018**

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------------------------------



**BÁO CÁO CHUYÊN ĐỀ AN TOÀN PHẦN MỀM**

**Đề tài:**

**“XÂY DỰNG HỆ THỐNG THANH TOÁN AN TOÀN THEO CHUẨN BẢO MẬT SET”**

**Giáo viên : TH.S HUỲNH TRỌNG THƯA**

**Sinh viên thực hiện : NGUYỄN QUỐC ĐẠT - N14DCAT124**

**NGUYỄN VŨ ĐỨC ANH – N14DCAT022**

**Lớp : D14CQAT01-N**

**Khóa : 2014-2019**

**Hệ : ĐẠI HỌC CHÍNH QUY**

**TP.HCM, THÁNG 11/2018**

**MỤC LỤC**

[**CHƯƠNG 1: THỰC TRẠNG BẢO MẬT HỆ THỐNG THƯƠNG MẠI ĐIỆN TỬ** 1](#_Toc521347448)

[**1.1.** **Giới thiệu** 1](#_Toc521347449)

[**1.2.** **Những yêu cầu bảo mật trong thanh toán điện tử** 2](#_Toc521347450)

[**CHƯƠNG 2: TÌM HIỂU WEB SERVICE** 7](#_Toc521347451)

[**2.1.** **Web Service là gì?** 7](#_Toc521347452)

[**2.2.** **Các loại Web Service** 8](#_Toc521347453)

[**2.3.** **WSDL (Web services description language)** 9](#_Toc521347454)

[**2.4.** **Universal Description, Discovery, and Integration (UDDI)** 9](#_Toc521347455)

[**2.5.** **Lợi ích của Web Service** 9](#_Toc521347456)

[**2.6.** **Kiến trúc của Web Service** 10](#_Toc521347457)

[**2.7.** **Đặc điểm dịch vụ web** 10](#_Toc521347458)

[**CHƯƠNG 3: TÌM HIỂU CƠ CHẾ MÃ HÓA, CHỨNG THỰC VÀ XÁC THỰC TRONG GIAO THỨC SET** 18](#_Toc521347459)

[**3.1.** **Tổng quan về giao thức SET (Secure Electronic Transaction)** 18](#_Toc521347460)

[**3.2.** **Hạn chế của SSL trong thanh toán điện tử** 18](#_Toc521347461)

[**3.3.** **Các thành phần của SET:** 18](#_Toc521347462)

[**3.4.** **Quy ước ký tự viết tắt:** 20](#_Toc521347463)

[**3.5.** **Hoạt động của giao thức SET** 21](#_Toc521347464)

[**3.5.1.** **Registration Process (Quy trình đăng ký)** 21](#_Toc521347465)

[**3.5.2.** **Authorization Request (Yêu cầu xác thực)** 24](#_Toc521347466)

[**3.5.3.** **Authorization Response (Phản hồi xác thực)** 25](#_Toc521347467)

[**3.5.4.** **Cardholder Authentication Request** 29](#_Toc521347468)

[**3.5.5.** **Cardholder Authentication Response and final payment** 32](#_Toc521347469)

[**3.5.6.** **SET and Information Confidentiality** 33](#_Toc521347470)

[**3.5.7.** **SET and Authentication** 33](#_Toc521347471)

[**3.5.8.** **SET and Information Integrity** 34](#_Toc521347472)

[**3.5.9.** **SET and Non-Repudiation** 34](#_Toc521347473)

[**CHƯƠNG 4: XÂY DỰNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ CƠ BẢN** 22](#_Toc521347474)

[**4.1.** **Xây dựng website thương mại điện tử cơ bản gồm các chức năng chính:** 22](#_Toc521347475)

[**4.2.** **Xây dựng website ngân hàng đơn giản với chức năng:** 26](#_Toc521347476)

[**4.3.** **Xây dựng web service paymenet gateway với chức năng:** 27](#_Toc521347477)

**DANH MỤC HÌNH**

Hình 1: Web Service Architecture Diagram 7

Hình 2: Ví dụ truyền thông đơn giản thông qua SOAP 9

Hình 3: Tương tác Requestor, Provider và Registry 11

Hình 4: Sơ đồ tuần tự giao thức SET 16

*Hình 5 : Dual Signature* 18

Hình 6: Yêu cầu mua hàng từ cardholder đến merchant 19

Hình 7: Merchant giải mã OI đồng thời so sánh hash và gửi PI Encrypted cho Gateway 20

Hình 8: Authorization Request from payment gateway to issuer bank 21

Hình 9: Authorization response from issuer bank to payment gateway 23

Hình 10: Authorization response từ payment gateway to merchant 24

Hình 11: Authorization response từ merchant gửi cho cardholder 25

Hình 12: Yêu cầu xác thực từ Cardholder gửi cho Merchant 26

Hình 13: Yêu cầu xác thực của Cardholder được gửi từ merchant đến payment gateway 27

Hình 14: Yêu cầu xác thực của Cardholder từ payment gateway đến issuer 28

Hình 15: Payment response từ issuer đến payment gateway 29

Hình 16: Payment response từ payment gateway đến merchant 30

Hình 17: Giao diện trang chủ 36

Hình 18: Chi tiết sản phẩm 37

Hình 19: Login form 37

Hình 20: Register form 38

Hình 21: Check out 38

Hình 22: Update profile 39

Hình 23: Trang chủ ngân hàng 40

Hình 24: Trang đăng ký tài khoản 41

Hình 25: Mail cung cấp tài khoản 41

Hình 26: Nhập đúng CardID 42

Hình 27: Nhập đúng password 43

Hình 28: Thông báo xác thực thành công 43

Hình 29: Mua hàng thành công 44

Hình 30: Nhập sai ID 45

Hình 31: Nhập sai password 46

Hình 32: Xác thực thất bại 47

Hình 33: Mô hình CA 47

Hình 34: Yêu cầu khóa mới và lưu vào cơ sở dữ liệu 48

Hình 35: Sinh cặp khóa 48

**MỞ ĐẦU**

Ngày nay, với sự phát triển mạnh mẽ của công nghệ thông tin, việc phát triển vượt bậc của Internet cùng với các Website thông tin trực tuyến trong các lĩnh vực của cuộc sống đã làm cho nhu cầu triển khai các hệ thống ứng dụng trong lĩnh vực mạng máy và truyền thông tăng lên nhanh chóng. Đối với các doanh nghiệp, Internet đã trở thành một trong những nhân tố tăng sức mạnh, khả năng cạnh tranh trên thị trường.

Chính vì vậy bản chất cốt lõi để website và internet phát triển trong tương lai chính là thương mại. Các trung tâm thương mại trên mạng internet sẽ xuất hiện. Nó sẽ giúp các nhà cung cấp sản phẩm tiếp cận trực tiếp và nhanh nhất với người tiêu dùng. Hiện nay ngành Thương mại điện tử đang có tốc độ phát triển rất mạnh. Hầu hết các công ty bán hàng lập nên ngày nay đa số đều là các công ty thương mại điện tử và mua sắm qua mạng đã trở thành thói quen hàng ngày của nhiều người Việt Nam.

Tuy nhiên cùng với phát triển của mạng Internet, tình hình mất an ninh mạng đang diễn biến phức tạp và xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin phục vụ phát triển kinh tế xã hội và đảm bảo quốc phòng, an ninh. Do đó đối với các giao dịch mang tính nhạy cảm vì vậy vấn đề bảo mật và an toàn thông tin trong thương mại điện tử là một vấn đề hết sức quan trọng.

Vấn đề Bảo mật và an toàn thông tin trong TMĐT đã và đang được áp dụng phổ biến rộng rãi ở Việt Nam và trên phạm vi toàn cầu và đang được nhiều người tập trung nghiên cứu, tìm mọi giải pháp để đảm bảo Bảo mật và an toàn cho các hệ thống thông tin trên mạng.

Việc thiếu đầu tư và quan tâm đến hệ thống an ninh, bộ phận chuyên trách dẫn đến các vụ tấn công vào các Website rất dễ xảy ra. Điều này cũng đồng nghĩa với việc gây mất mát rất lớn đến cho các doanh nghiệp và lòng tin khách hàng

Nhận thấy việc cần đề cao cấu trúc bảo mật cho hệ thống thanh toán thương mại điện tử là một vấn đề thiết thực và cần phải thực hiện. Chính vì vậy: Đề tài ***“*Xây Dựng Hệ Thống Thanh Toán An Toàn Theo Chuẩn Bảo Mật Set*”*** trong bối cảnh có nhiều website thương mại điện tử xuất hiện ngày một nhiều như hiện này,nhằm đảm bảo 4 yếu tố bảo mật cần thiết cho các thanh toán điện tử an toàn bao gồm: tính tin cậy, tính toàn vẹn, tính xác thực, tính chống chối bỏ.

# **CHƯƠNG 1: ĐẶC TẢ HỆ THỐNG THƯƠNG MẠI ĐIỆN TỬ**

* 1. **Giới thiệu**

Ngày nay, thuật ngữ Thương mại điện tử (TMĐT) – Electronic Commerce (EC) không còn quá xa lạ đối với nhiều người. Cuộc cách mạng số từ những năm giữa của thế kỷ XX đã thúc đẩy nền kinh tế, văn hóa, xã hội triển lên một tầm cao mới – Xã hội thông tin. Trong đó, TMĐT là bộ phận thành của xã hội thông tin, sử dụng tất cả các phương pháp điện tử để hoạt thương mại, buôn bán góp phần thay đổi hình dáng của Xã hội với một nhanh chóng.

Ủy ban Châu Âu đưa ra định nghĩa về Thương mại điện tử như sau: Thương mại điện tử được hiểu là việc thực hiện hoạt động kinh doanh qua các phương tiện điện tử. Nó dựa trên việc xử lý và truyền dữ liệu điện tử dưới dạng text, âm thanh và hình ảnh. Thương mại điện tử gồm nhiều hành vi trong đó hoạt động mua bán hàng hóa và dịch vụ qua phương tiện điện tử, giao nhận các nội dung kỹ thuật số trên mạng, chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn điện tử, đấu giá thương mại, hợp tác thiết kế, tài nguyên mạng, mua sắm công cộng, tiếp thị trực tiếp tới người tiêu dùng và các dịch vụ sau bán hàng. Thương mại điện tử được thực hiện đối với cả thương mại hàng hóa (ví dụ như hàng tiêu dùng, các thiết bị y tế chuyên dụng) và thương mại dịch vụ (ví dụ như dịch vụ cung cấp thông tin, dịch vụ pháp lý, tài chính); các hoạt động truyền thống (như chăm sóc sức khỏe, giáo dục ) và các hoạt động mới (ví dụ như siêu thị ảo).

Tóm lại, theo nghĩa rộng thì thương mại điện tử có thể được hiểu là các dịch tài chính và thương mại bằng phương tiện điện tử như: trao đổi dữ liệu tử; chuyển tiền điện tử và các hoạt động gửi rút tiền bằng thẻ tín dụng.

Thương mại điện tử (E-Commerce) đã mang lại rất nhiều lợi ích và tiện lợi cho cả người tiêu dùng lẫn người bán hàng.

Trong các mô hình thương mại điện tử, mô hình Bussiness to Customer (B2C), thẻ tín dụng được sử dụng như là một phương thức thanh toán phổ biến trong các cuộc giao dịch trên mạng.

Tuy nhiên tình hình mất an ninh mạng đang diễn biến phức tạp và xuất hiện nhiều nguy cơ đe dọa nghiêm do đó đối với các giao dịch mang tính nhạy cảm vì vậy vấn đề bảo mật và an toàn thông tin trong thương mại điện tử là một vấn đề hết sức quan trọng.

* 1. **Những yêu cầu bảo mật trong thanh toán điện tử**

**Bảo mật thông tin (Information confidentiality)**

Những truy vấn trong suốt quá trình giao dịch phải được giữ được tính riêng tư như là số tài khoản, họ tên khách hàng. Do đó, thông tin giao dịch cần phải được mã hóa.

**Toàn vẹn dữ liệu (Data integrity)**

Dữ liệu Web cần phải được đảm bảo không bị thay đổi hay sửa chữa trong quá trình truyền tải.

**Xác thực các bên tham gia (Authentication of participants)**

Điều kiện tiên quyết trong giao dịch giữa các đối tượng tham gia vào quá trình thanh toán điện tử cần phải nhận diện được lẫn nhau.

**Không thể chối bỏ (Non-repudiation)**

Các bên tham gia không thể chối bỏ các hành động đã được thực hiện trong quá trình giao dịch.

Ví dụ: thông tin thanh toán và thông tin xác nhận thanh toán giữa khách hàng (customer) và merchant là không thể bị chối bỏ.

**End-user implementation Requirements**

Khả năng sử dụng - Hệ thống phải dễ thực hiện, bao gồm cả cài đặt. Người tiêu dùng yêu cầu thẻ tổ chức phát hành và người bán để cung cấp một hệ thống an toàn không phức tạp, trong khi người bán yêu cầu người thâu tóm và các nhà phát triển phần mềm bảo mật để cung cấp một đơn giản ứng dụng đáp ứng các yêu cầu bảo mật.

Tính linh hoạt - Hệ thống phải cho phép thương mại điện tử người tiêu dùng đặt mua sản phẩm hoặc dịch vụ từ bất kỳ vị trí, và không chỉ từ một máy tính. Ở đây, người tiêu dùng là thực thể yêu cầu dịch vụ linh hoạt trong khi người bán là tổ chức cung cấp dịch vụ.

Khả năng chi trả - Chi phí triển khai và sử dụng hệ thống phải phù hợp với người tiêu dùng và người bán, vì những người dùng cuối này khó có khả năng chuẩn bị trả thêm đáng kể để tham gia Giao dịch thương mại điện tử Internet. Ví dụ, người tiêu dùng không sẵn sàng trả tiền cho chứng chỉ số để thực hiện giao dịch thương mại điện tử mặc dù là bắt buộc trong một số chương trình thanh toán điện tử chẳng hạn như SET. Thương gia cũng sẽ không muốn đầu tư đáng kể vào cơ sở hạ tầng thanh toán điện tử.

Độ tin cậy - Hệ thống phải đáng tin cậy vì nó là được sử dụng để truyền và thao tác nhạy cảm thông tin.

Tính khả dụng - Hệ thống phải khả dụng khi cần thiết. Tốc độ giao dịch phải là chấp nhận được cho người dùng cuối thương mại điện tử.

Khả năng tương tác - Hệ thống phải tương thích giữa các nền tảng điện toán khác nhau, trình duyệt web và các gói phần mềm máy chủ để cho phép sử dụng nó bởi phổ rộng nhất có thể của thương mại điện tử người tiêu dùng và người bán

# **CHƯƠNG 2: TÌM HIỂU** **THIẾT KẾ THEO CƠ CHẾ MÃ HÓA, CHỨNG THỰC VÀ XÁC THỰC TRONG GIAO THỨC SET**

1. **Tổng quan về giao thức SET (Secure Electronic Transaction)**

SET (Secure Electronic Transaction) là một giao thức bảo mật khá toàn diện, 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. Để xác thực, những người mua hàng và người bán háng được yêu cầu cần phải có các chứng chỉ số được cấp bởi các tổ chức được đảm bảo.

Giao thức SET phức tạp và các chứng thực không được phân phối rộng rãi với một cách thức ổn định. Giao thức SET, giấu các thông tin về thẻ tín dụng của khách hàng đối với người kinh doanh và cũng giấu cả thông tin về đơn hàng đối với các ngân hàng bảo vệ sự riêng tư. Thiết kế này được gọi là chữ ký kép (Dual Signature).

SET đặt các mật mã riêng vào tay của cả người mua lẫn người bán trong một giao dịch. Điều này có ý nghĩa là một người dùng bình thường cần các mật mã riêng của riêng họ và cần phải đăng ký các mật mã này. Khi một giao dịch SET được xác nhận ủy quyền, mật mã riêng của người dung sẽ có chức năng như một chữ kí số.

1. **Hạn chế của SSL trong thanh toán điện tử**

Secure Sockets Layer (SSL) là giao thức được sử dụng phổ biến trong việc mã hóa thông điệp giữa web browsers và web servers. SSL được sử dụng để bảo vệ tính bảo mật và toàn vẹn của các dữ liệu nhạy cảm như mã số thẻ.   
Tuy nhiên, vấn đề lớn nhất của SSL là merchant có thể lưu trữ thông tin nhạy cảm của cardholder, và SSL cũng không ngăn được non-repudiation bởi vì việc xác thực khách hàng là không bắt buộc

SET (Secure Electronic Transaction) ra đời để khắc phục nhược điểm của SSL - xác thực và bảo vệt thông tin nhạy cảm - đảm bảo thông tin thanh toán được toàn vẹn, riêng tư và được xác thực bởi merchants và cardholders.

1. **Các thành phần của SET:**

**Người dùng thẻ (Cardholder)**: Người dùng thẻ tín dụng để thực hiện các giao dịch thanh tóan trên Internet (người mua hàng).

**Người bán hàng (Merchant)**: Một cá nhân hay tổ chức bán hàng hoặc dịch vụ trên mạng (thông qua web hoặc email). Người bán hàng phải có khả năng chấp nhận thanh tóan bằng thẻ, và phải có quan hệ với một tổ chức tài chính nào đó (Accquirer).

**Tổ chức phát hành thẻ (Issuer):** Đây là tổ chức tài chính (thường là ngân hàng) phát hành thẻ tín dụng. Tổ chức này có trách nhiệm thanh tóan theo yêu cầu của người sử dụng thẻ.

**Trọng tài (Acquirer):** Một tổ chức tài chính khác có quan hệ với người bán hàng, thực hiện việc xác thực tài khỏan của người mua hàng và thanh tóan. Trọng tài sẽ kiểm tra tài khỏan của người mua hàng để thông báo cho người bán hàng biết số dư trong tài khỏan của người mua có đủ để thực hiện giao dịch hay không. Sau khi giao dịch mua hàng được thực hiện, trọng tài thực hiện việc chuyển tiền từ tài khỏan của người mua hàng sang tài tòan khỏan của người bán hàng, đồng thời ra yêu cầu thanh tóan đối với ngân hàng phát hành thẻ (Issuer).

**Cửa thanh tóan (Payment gateway):** Đây là thành phần chịu trách nhiệm xử lý các bản tin thanh tóan (payment message) được điều hành bởi trọng tài hoặc một tổ chức thứ 3 được chỉ định. Payment gateway giao tiếp giữa SET và hệ thống thanh tóan của ngân hàng để thực hiện các thao tác xác thực và thanh tóan. Như vậy, người bán hàng thật ra trao đổi các thông báo với cửa ngõ thanh tóan thông qua mạng Internet, sau đó, Payment gateway mới liên kết đến hệ thống xử lý tài chính của Acquirer.

**Tổ chức chứng thực (Certification authority \_ CA):** Là thành phần có chức năng tạo ra các chứng thực (certificate) theo chuẩn X.509v3 và phân phối cho Cardholder, Merchant và Payment Gateway. Sự thành công của SET phụ thuộc vào sự tồn tại của CA. Thông thường, CA được tổ chức theo một mô hình phân cấp với nhiều CA liên hệ với nhau.

1. **Quy ước ký tự viết tắt:**

C : Cardholder

M : Merchant

PG : Payment Gateway

IB : Issuer Bank or Cardholder Bank

CA: Certificate authority

Vshop : Virtual Shopping Site

PAN: Card Number

CVV2: Card Verification Value or Crypto (three digits)

ExD: Expiry date of the card

OI: Order Information

PI: Payment Instructions

OIMD: OI Message Digest

PIMD: PI Message Digest

POMD: Payment Order Message Digest

K: Symmetric key generated randomly

Kum: Public key of merchant

Kupg: Public key of payment gateway

Kuis: Public key of issuer bank

Krm: Private key of merchant

Krpg: Private key of payment gateway

Kris: Private key of issuer bank

S: Sign

E: Encrypt

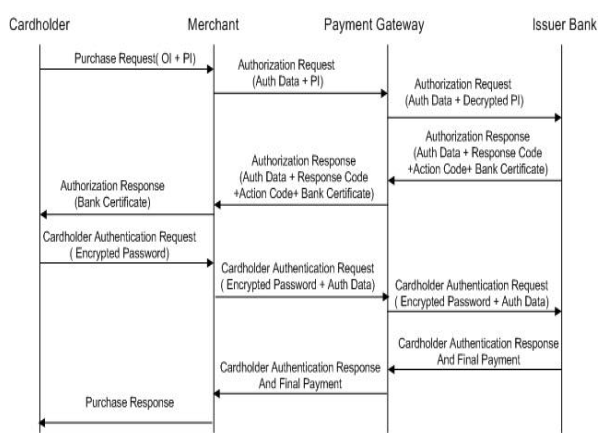
D: Decrypt

V: Verify signature

H: Hash

||: Concatenation

#: Disconnect CA: Certification Authority



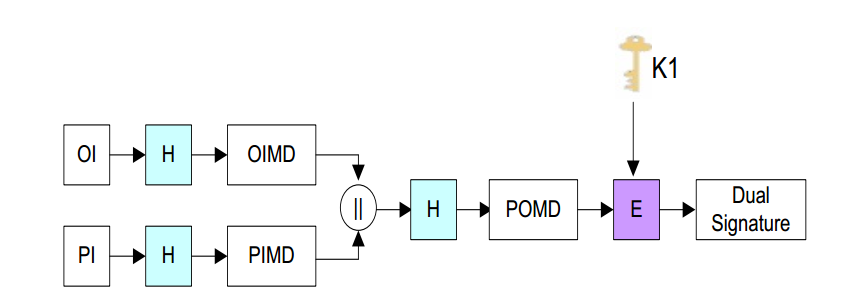
Hình 1: Sơ đồ tuần tự giao thức SET

1. **Hoạt động của giao thức SET**
2. **Registration Process (Quy trình đăng ký)**

Merchent, payment gateway và issuer bank phải đăng ký và có được chứng chỉ từ Certificate Authority (CA) để có thể sự dụng SEP

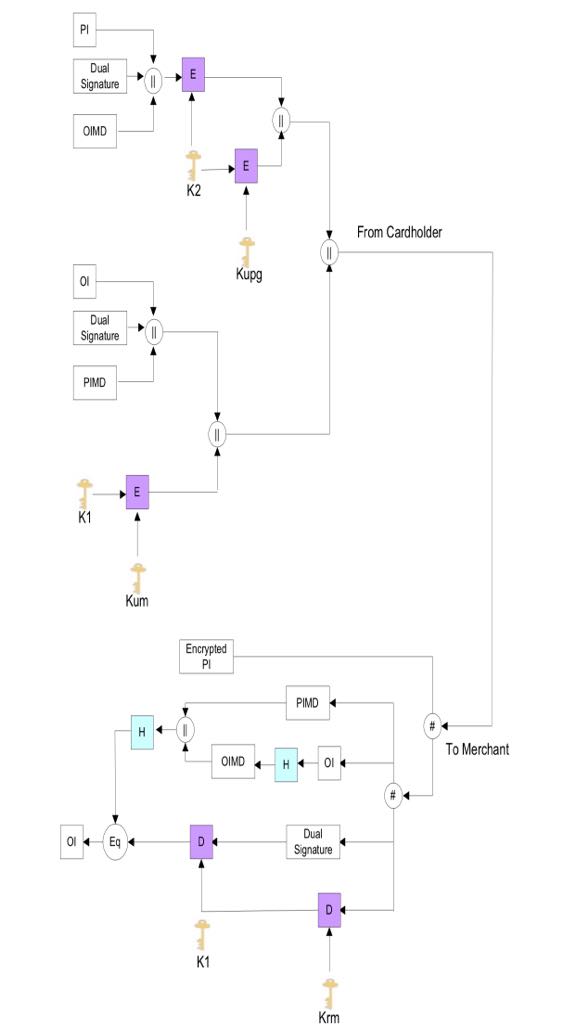
Cardholder phải đăng ký và có mật khẩu từ phía Issuer bank (IB) để có thể sử dụng SEP và mua hàng

Cardholder truy cập trang cửa hàng và lựa chọn sản phẩm mà mình muốn mua từ Vshop và đơn hàng. Trước khi bắt đầu mua hàng thì cả cardholder và merchant cần phải thống nhất về số lượng chi tiết trong đơn hàng. Cardholder gửi cho merchant local ID và fresh random challenge mục đích là tạo ra chữ ký số của merchant và chứng chỉ mã hóa thanh toán

Cardholder phát sinh OI, PI đã được mã hóa và chữ ký kép. Chữ ký kép được mã hóa dưới dạng mã đối xứng ngẫu nhiê

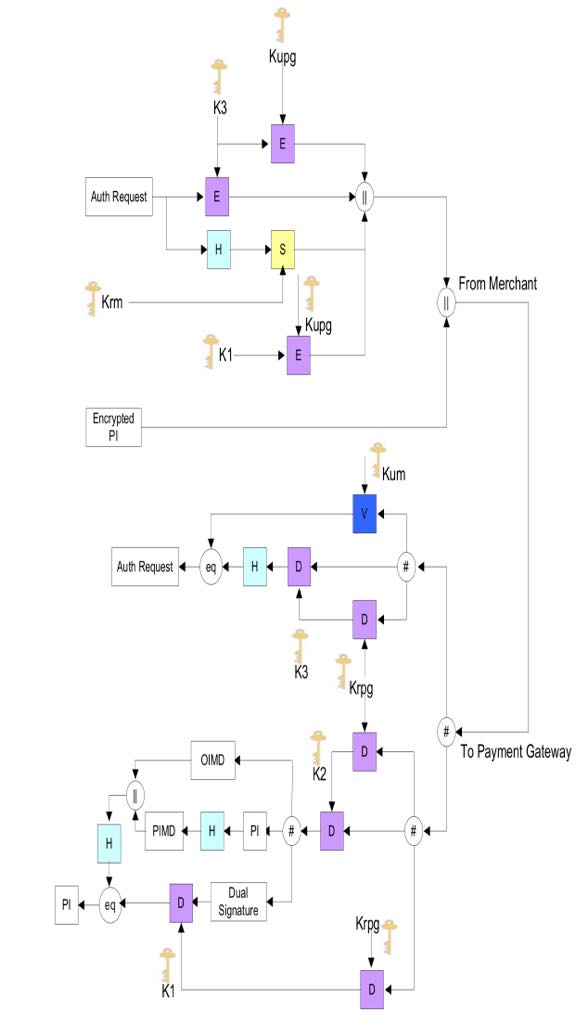
*Hình 2 : Dual Signature*

Cardholder xử lý yêu cầu thanh toán và gửi đến cho Merchant



Hình 3: Yêu cầu mua hàng từ cardholder đến merchant

Merchant giải mã được khóa K1, xử lý thông tin đơn hàng OI, đồng thời so sánh hash và gửi phần PI đã bị mã hóa cho Payment Gateway

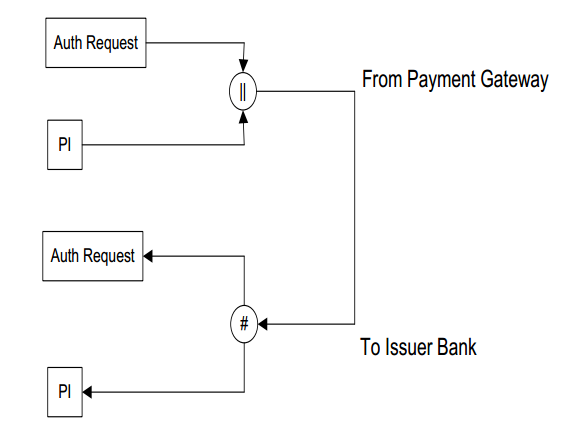


Hình 4: Merchant giải mã OI đồng thời so sánh hash và gửi PI Encrypted cho Gateway

1. **Authorization Request (Yêu cầu xác thực)**

Merchant ký và gửi Auth Request tới gateway, khóa đối xứng K1 mã hóa vởi Kupg. Auth Request được mã hóa theo một khóa đối xứng được tạo ngẫu nhiên. Gateway xác minh dual signature và nhận PI

The payment gateway chuyển thông tin xác thực và PI đến the issuer bank thông qua một hệ thống mạng tài chính liên ngân hàng an toàn



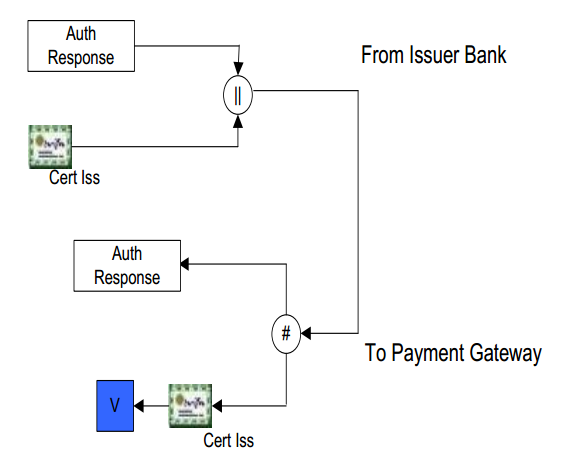
Hình 5: Authorization Request from payment gateway to issuer bank

1. **Authorization Response (Phản hồi xác thực)**

issuer bank xác thực PI, và xác thực authorization request và thực hiện một vài công việc ngân hàng để kiểm tra xem cardholder này có được phép thực hiện giao dịch hay không

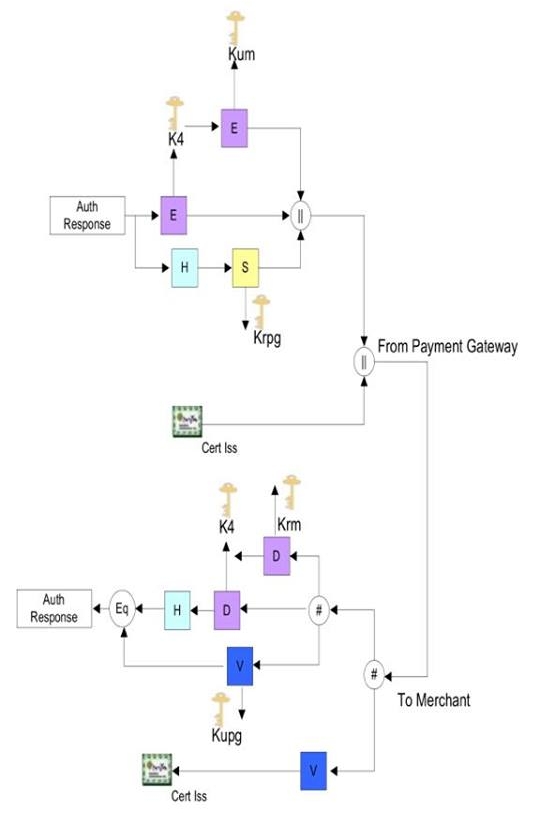
Issuer gửi một authorization response và bank certificate về cho payment gateway thông qua mang liên ngân hàng

authorization response chứa response code và action code. The response code chỉ ra liệu authorization request có được chấp thuận hay không, the action code chỉ ra liệu cardholder có bị yêu cầu cung cấp password hay không. Mục đích của bước này là để gửi the cardholder issuer bank encryption certificate.



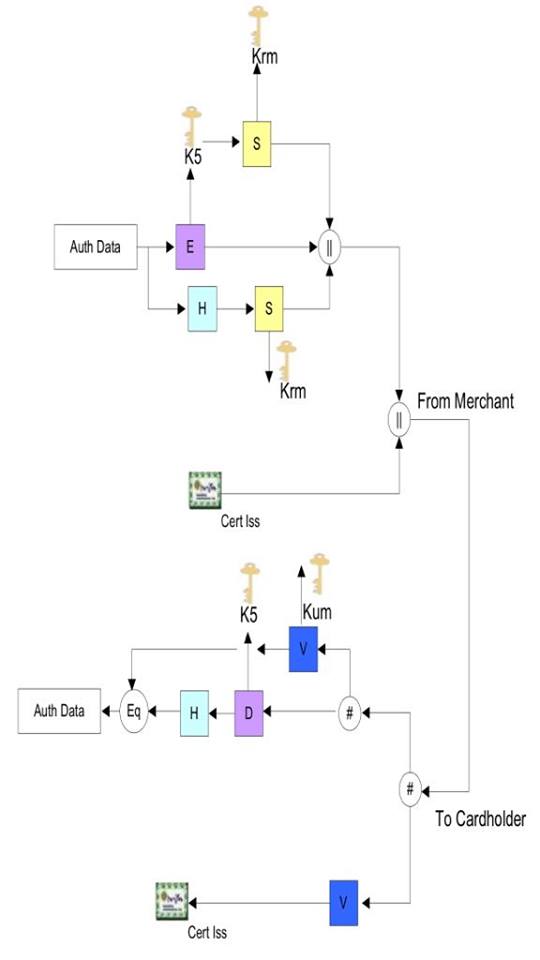
Hình 6: Authorization response from issuer bank to payment gateway

The payment gateway ký và gửi the authorization response và issuer certificate cho merchant.



Hình 7: Authorization response từ payment gateway to merchant

The merchant kiểm tra action code, nếu như chấp thuận thì điều đó có nghĩa là cardholder đã được xác thực, merchant gửi một authentication request đến cardholder bao gồm kèm theo issuer certificate và authorization data

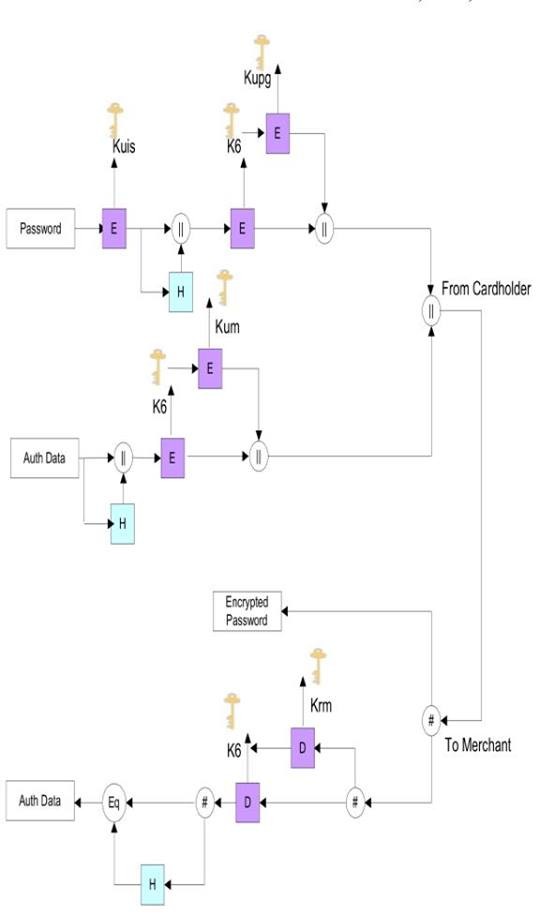


Hình 8: Authorization response từ merchant gửi cho cardholder

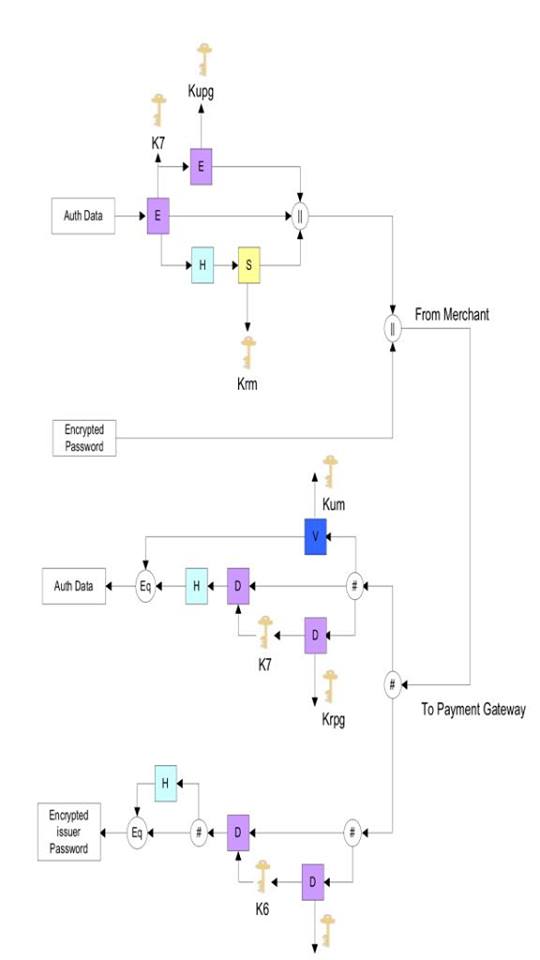
1. **Cardholder Authentication Request**

Cardholder xác thực issuer certificates và gửi mật khẩu ngân hàng được mã hóa bằng khóa đối xứng

Hình 9: Yêu cầu xác thực từ Cardholder gửi cho Merchant

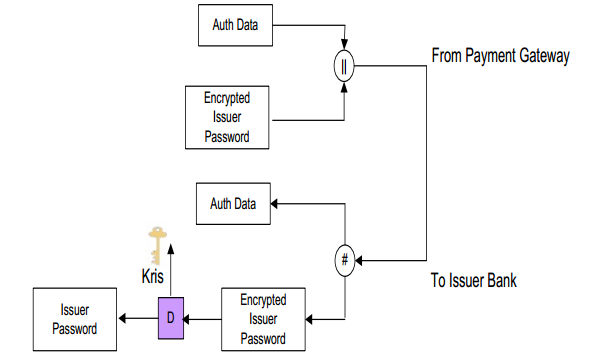


The merchant xác thực authorization data và password đã bị mã hóa gửi cho payment gateway.



Hình 10: Yêu cầu xác thực của Cardholder được gửi từ merchant đến payment gateway

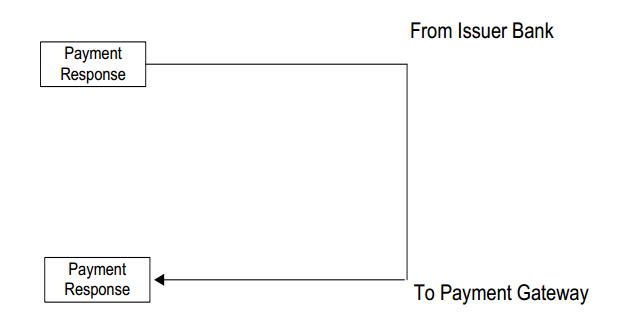
Payment gateway xác thực authorization data, encrypted password và chuyển encrypted password cho the issuer để chứng thực. The issuer giải mã encrypted password và kiểm tra xem có đúng không



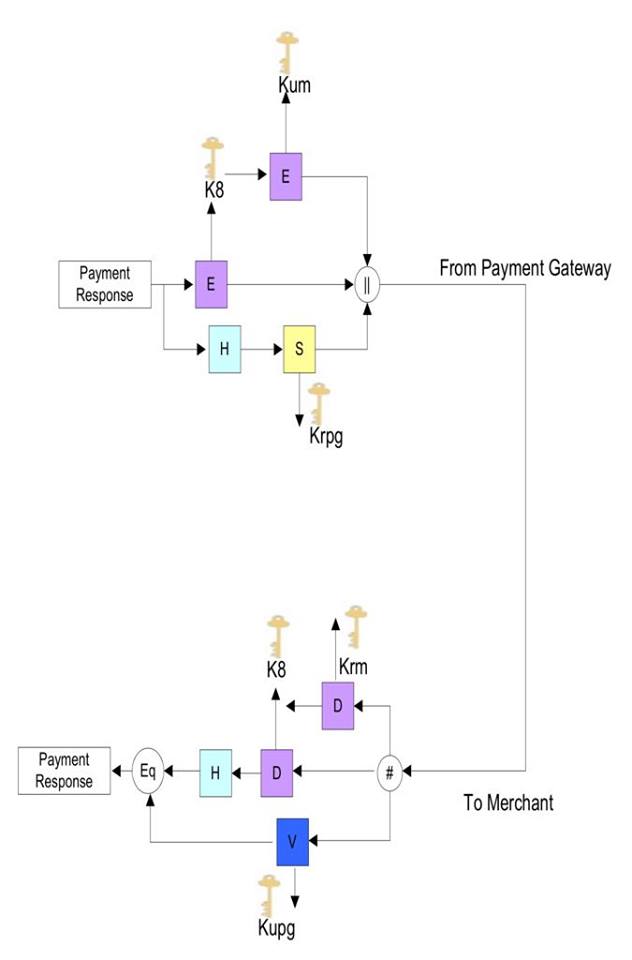
Hình 11: Yêu cầu xác thực của Cardholder từ payment gateway đến issuer

1. **Cardholder Authentication Response and final payment**Issuer bank giải mã và xác thực password, đảm bảo tính thống nhất giữa authorization request và cardholder authentication request, và gửi về payment response cho the payment gateway.

Hình 12: Payment response từ issuer đến payment gateway



Cuối cùng payment gateway chuyển payment response đến merchant. Merchant xác thực response và hoàn tất giao dịch với cardholder



Hình 13: Payment response từ payment gateway đến merchant

1. **SET and Information Confidentiality**

Với mỗi bước chuyển tiếp, một khóa đồng bộ được sinh ra ngẫu nhiên để mã hóa thông tin thanh toán. Việc mã hóa ngăn chặn việc truy cập trái phép hoặc đánh cắp thông tin trong quá trình chuyển tiếp thông tin

1. **SET and Authentication**

Cardholder xác thực Merchant và Issuer bank

Merchant xác thực payment gateway và issuer bank

Payment gateway xác thực merchant và issuer bank

Issuer bank xác thực cardholder bằng password

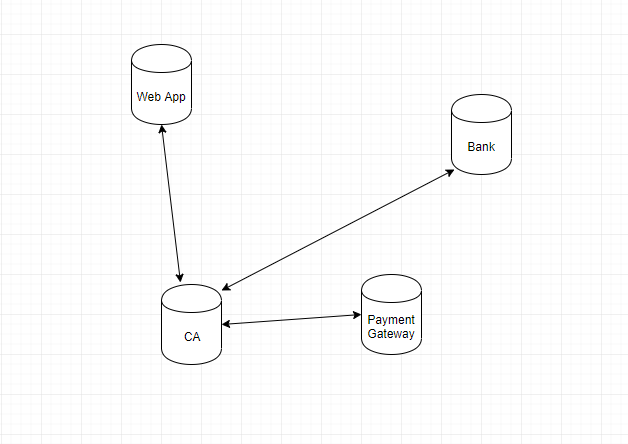
1. **SET and Information Integrity**

Dữ liệu được đảm bảo toàn vẹn nhờ vào sử dụng các giải thuật HASH SHA-256, SHA-1.

1. **SET and Non-Repudiation**

Yếu tố không thể chối bỏ được đảm bảo thông qua việc sử dụng mật khấu trong suốt quá trình yêu cầu xác thực. Issuer bank xác thực card và cardholder, vì vậy cardholder không thể phủ nhận việc đã gửi thông tin.

1. **Mô hình CA sinh khóa cho hệ thống giao dịch**

Hình 14: Mô hình CA

Các thành phần của hệ thống thanh toán sẽ tương tác với CA và xin cặp khóa chung và riêng dùng để mã hóa các giao dịch thực hiện trong mô hình SET. Cặp khóa sẽ được

lưu trữ và chia sẻ giữa các thành phần và lưu trữ trong cơ sở dữ liệu trong thời gian còn hiệu lực trước khi yêu cầu được cấp khóa mới từ CA.

**CHƯƠNG 3 : XÂY DỰNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ TRÊN WEB APPLICATION**

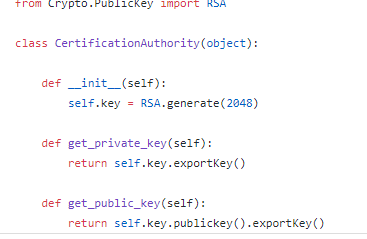
1. **Công nghệ và ngôn ngữ.**

Hệ thống được xây dựng bằng framework flask cho web dựa trên ngôn ngữ python và cơ sở dữ liệu Mongodb được triển khai và lưu trong container Docker.

* **Flask** là một web frameworks, nó thuộc loại micro-framework được xây dựng bằng ngôn ngữ lập trình Python. Flask cho phép bạn xây dựng các ứng dụng web từ đơn giản tới phức tạp. Nó có thể xây dựng các api nhỏ, ứng dụng web chẳng hạn như các trang web, blog, trang wiki hoặc một website dựa theo thời gian hay thậm chí là một trang web thương mại. Flask cung cấp cho bạn công cụ, các thư viện và các công nghệ hỗ trợ bạn làm những công việc trên.
* **Flask** là một micro-framework. Điều này có nghĩa Flask là một môi trường độc lập, ít sử dụng các thư viện khác bên ngoài. Do vậy, Flask có ưu điểm là nhẹ, có rất ít lỗi do ít bị phụ thuộc cũng như dễ dàng phát hiện và xử lý các lỗi bảo mật.
* **Docker** là một nền tảng để cung cấp cách để building, deploying và running ứng dụng một cách dễ dàng trên nền tảng ảo hóa.

1. **Thực hiện.**
2. **CA tạo khóa cung cấp cho hệ thống**

Hình 15: Yêu cầu khóa mới và lưu vào cơ sở dữ liệu



Hình 16: Sinh cặp khóa

Khóa sẽ được lưu và truy xuất khi cần thiết từ chủ sở hữu (các thành phần của hệ thống giao dịch) và CA sẽ không can thiệp vào các giao thức giao dịch của hệ thống mà chỉ là trung gian xác nhận chứng thực các thành phần trong hệ thống để đảm bảo tính đúng đắn và tin cậy cho giao dịch được an toàn.

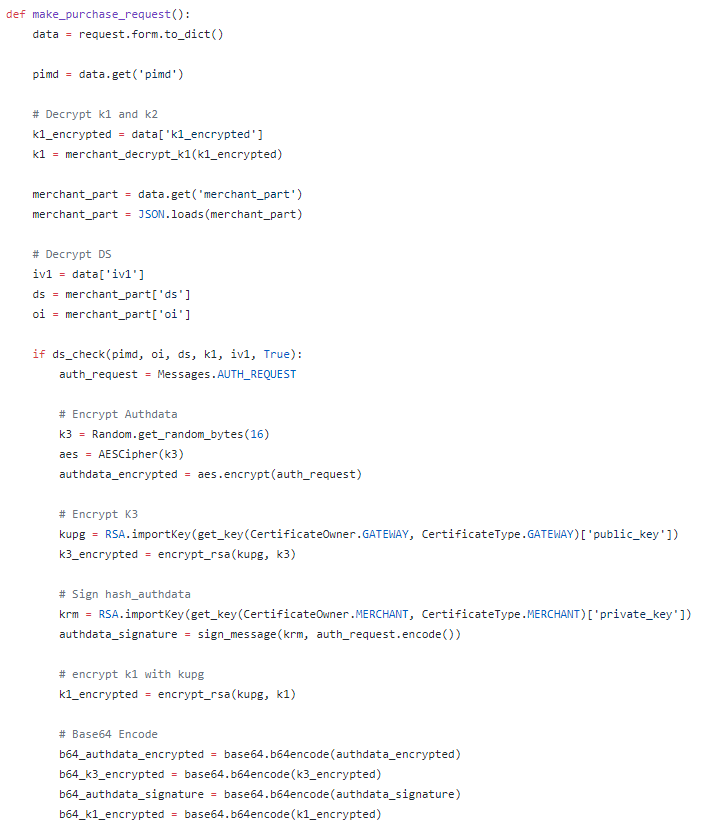
1. **Xây dựng Web app**

Web app được xây dựng gồm các view của các trang mua hàng thanh toán và qunả lý người dùng được đăng kí và thực hiện khởi chạy trong file app.py:



Hình 17: Cấu hình ứng dụng web

Web app được khởi tạo với đường dẫn các trang thuộc app nằm trong folder webapp/templates và các file tĩnh trong đường dẫn /webapp/static, đồng thời kết nối với mongodb cùng với những cài đặt mặc định trong file settings.py cùng cấp. Đăng kí và xử lý session kèm theo (tạo hoặc update session có sẵn trước khi thực hiện các request với hàm before\_request và tự set cookie sau khi request với hàm after\_request của flask).



Hình 18: Nhận thông tin từ người dùng để xử lý qua các loại mã hóa



Hình 19: Gửi thông tin thanh toán và xử lý xác nhận từ gateway



Hình 20: Gửi mật khẩu người dùng đã mã hóa và nhận xác nhận giao dịch cho thanh toán

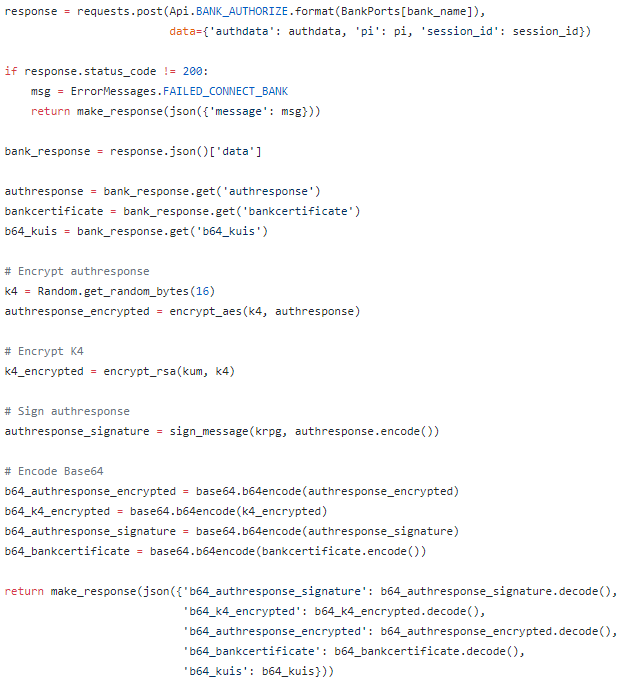
1. **Xây dựng cổng thanh toán**

Cổng thanh toán có những chức năng như:

* Nhận thông tin thanh toán đã mã hóa để giải mã và chuyển tiếp đến đúng ngân hàng để xác nhận thanh toán và trả về xác nhận xét duyệt cho web app.

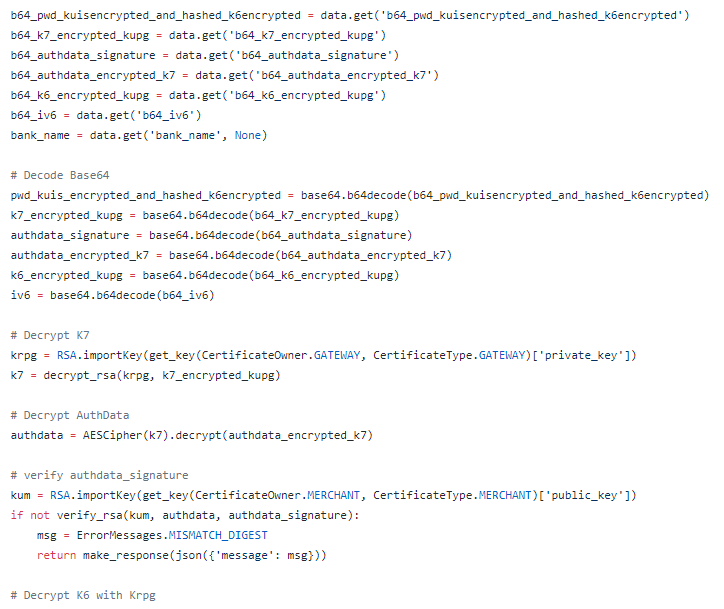


Hình 19: Nhận, giải mã và xác nhận thông tin từ ứng dụng



Hình 20: Chuyển tiếp thông tin thanh toán và trả xác nhận cho ứng dụng web

* Nhận thông tin mật khẩu đã mã hóa từ người dùng được chuyển tiếp từ web app và chuyển tiếp cho ngân hàng đó để giải mã và xác nhận thanh toán bằng mật khẩu tài khoản và trả về chi tiết thanh toán.



Hình 20: Nhận, giải mã và xác nhận mật khẩu đã mã hóa và thông tin ủy quyền



Hình 21: Gửi dữ liệu mật khẩu cho ngân hàng và trả về xác nhận

* Sau khi đã giải mã theo sơ đồ của SET sẽ có được các thông tin cần thiết (mật khẩu đã mã hóa và thông tin ủy quyền) gateway sẽ tiến hành gửi những thông tin đó tới ngân hàng tương ứng trước đó (**BankPorts[bank\_name]**) và chờ thông tin xác nhận việc thanh toán về cho ứng dụng web.

1. **Xây dựng ngân hàng**

* Xây dựng ngân hàng gồm có 2 phần: xử lí request và giao diện xử lý thông tin tài khoản người dùng cho ngân hàng.
  + Phần xử lý thông tin tài khoản được xây dựng thông qua file home.py xử lý đăng nhập, đăng ký và tra cứu/gửi tiền của ngân hàng.



Hình 22: Xử lý thông tin tài khoản

* + Phần xử lí request gồm có xử lí xác thực thẻ hợp lệ và xác thực mật khẩu thẻ để xác nhận thanh toán thành công hay thất bại.

Hình 23: Xác thực thẻ hợp lệ



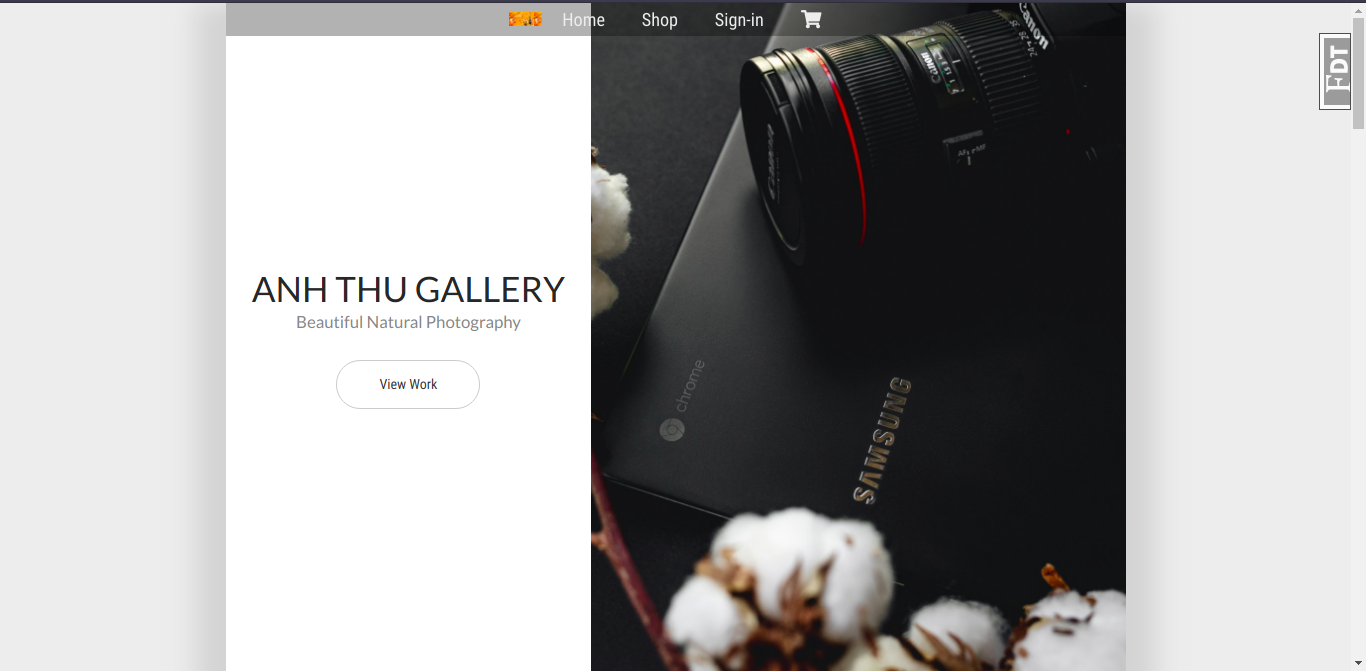
Hình 24: xác thực mật khẩu thẻ và trả về thông tin thanh toán

# **CHƯƠNG 4: XÂY DỰNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ CƠ BẢN**

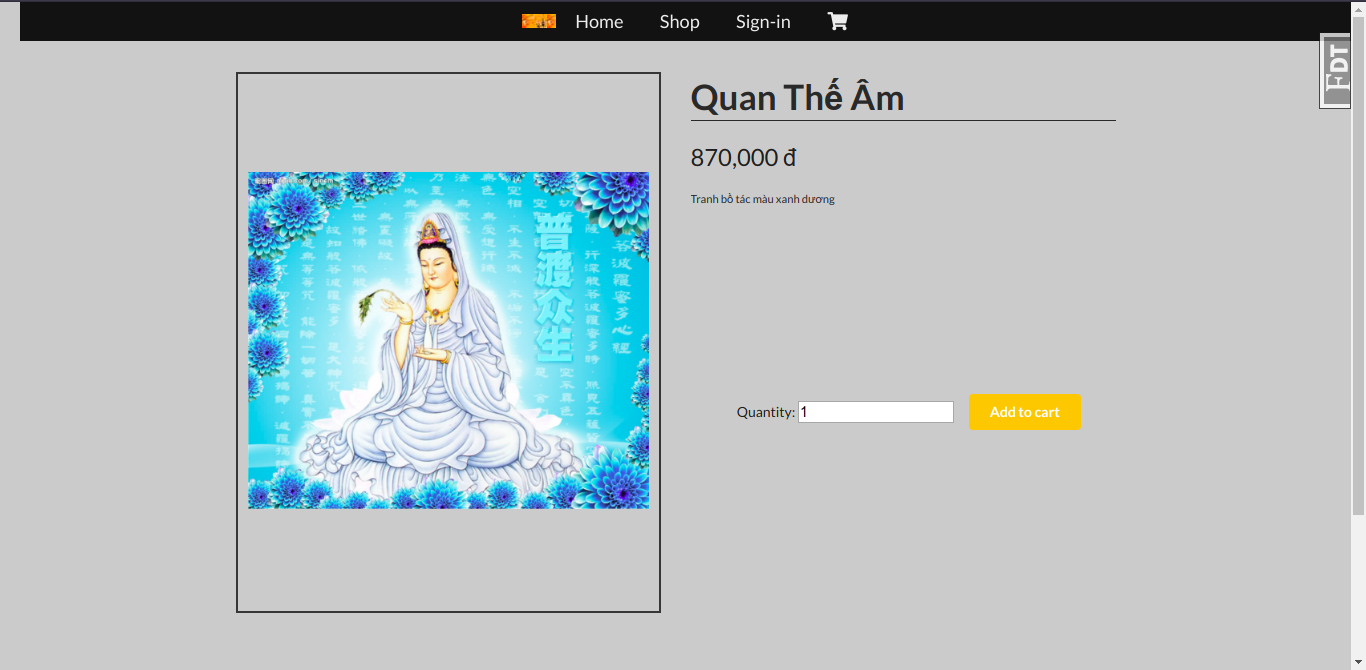
1. **Xây dựng website thương mại điện tử cơ bản gồm các chức năng chính:**

Đăng kí tài khoản, sửa thông tin tài khoản.

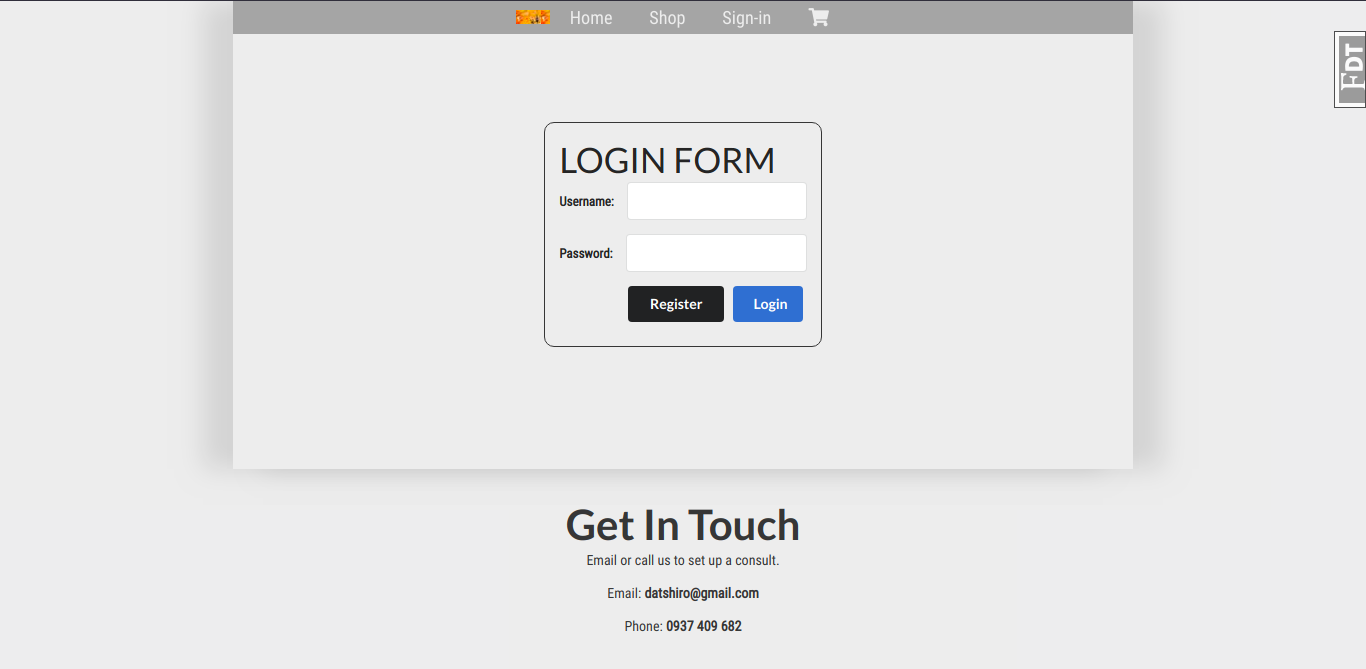
Xem hàng, mua hàng thanh toán trực tuyến.



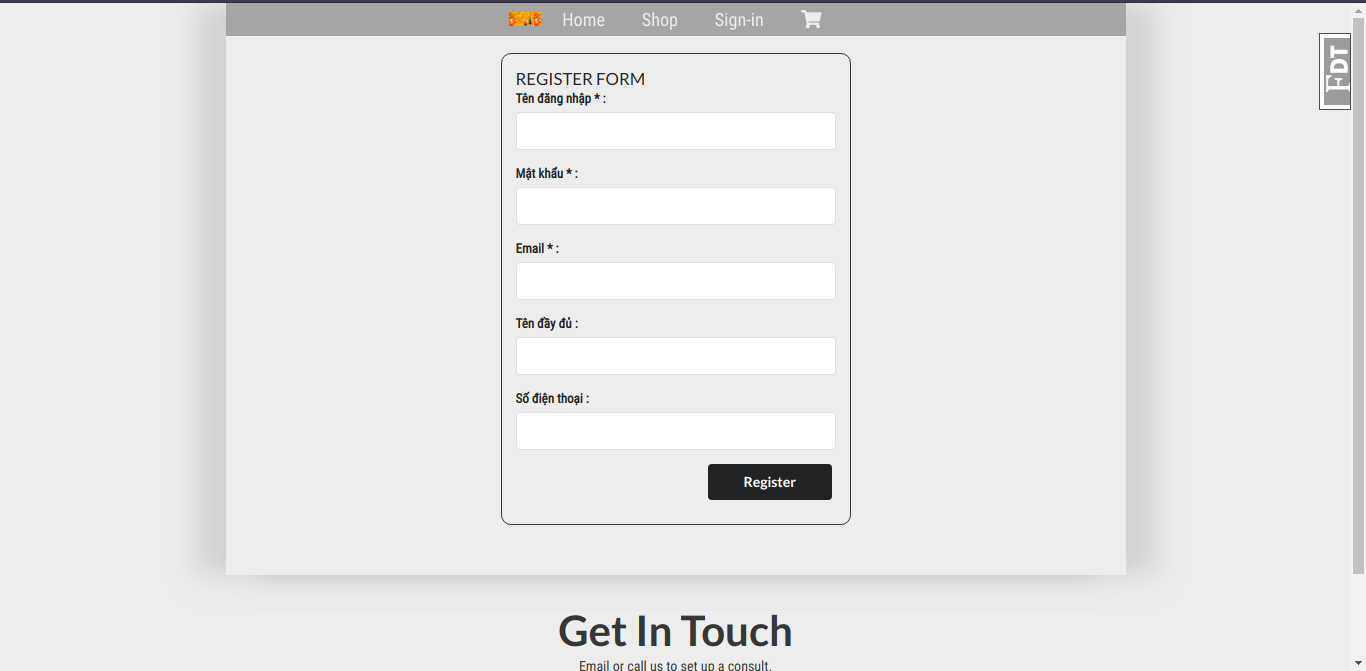
Hình 17: Giao diện trang chủ

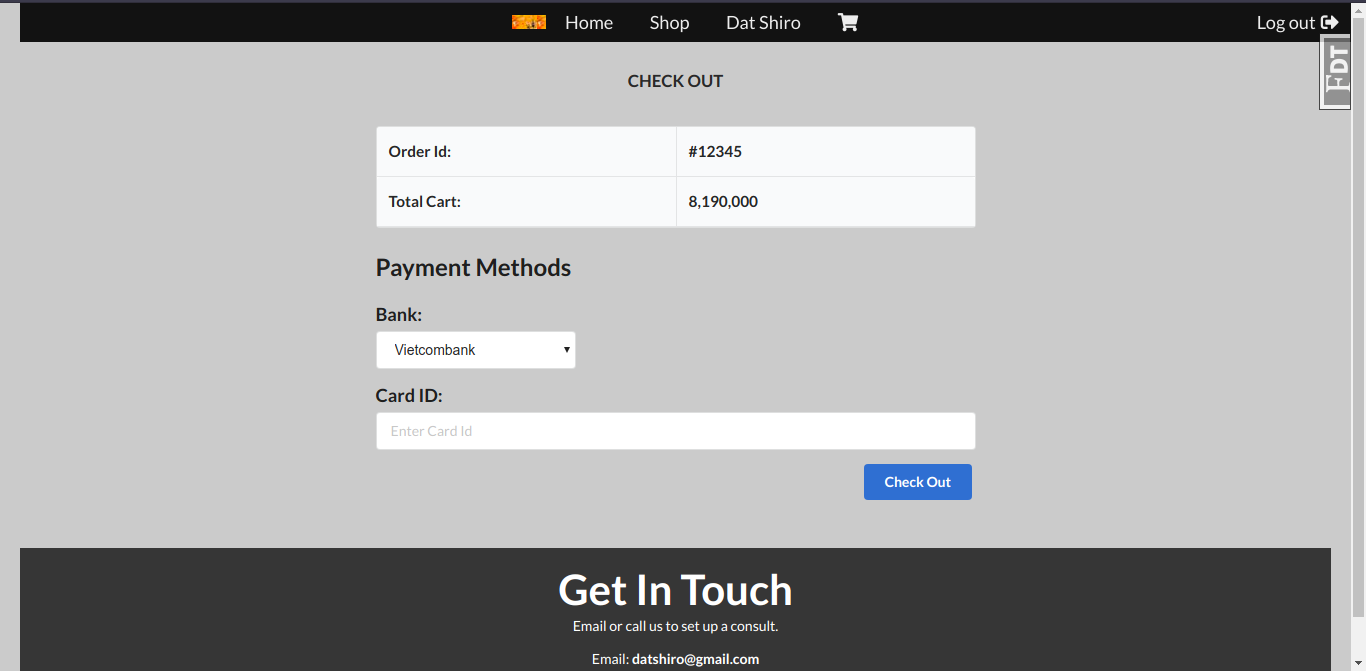


Hình 18: Chi tiết sản phẩm

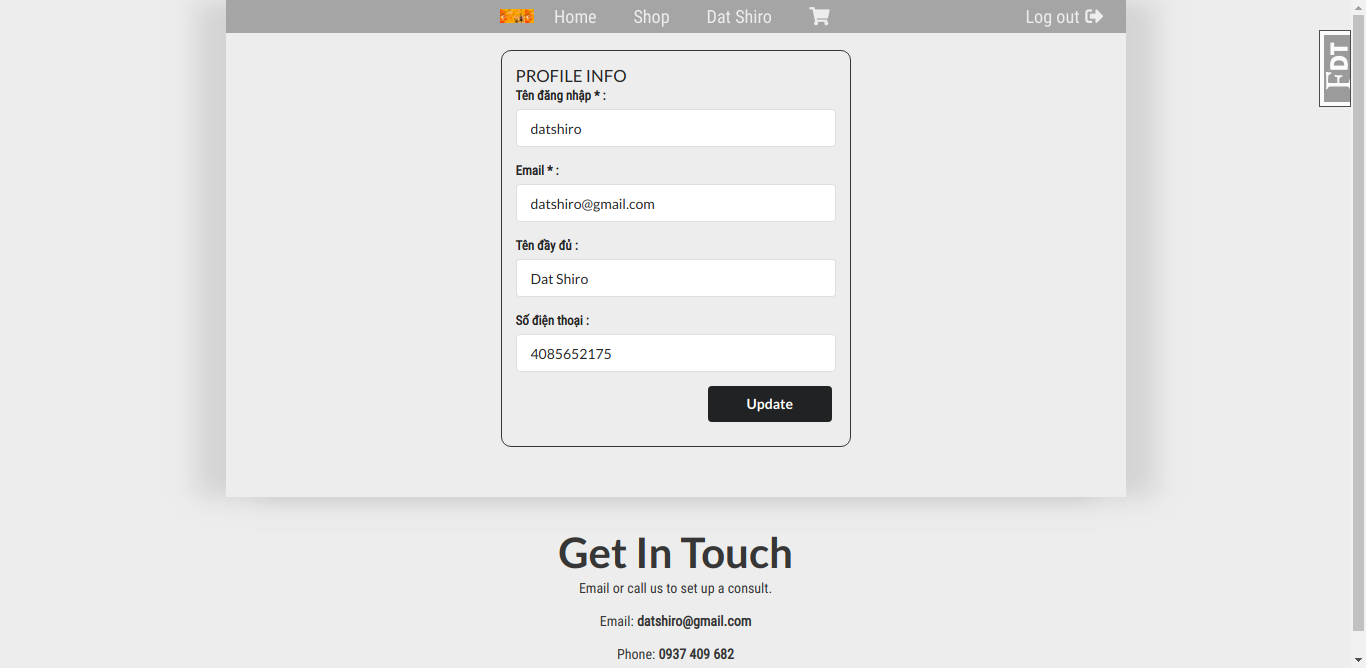
****

Hình 19: Login form



Hình 20: Register form****

Hình 21: Check out

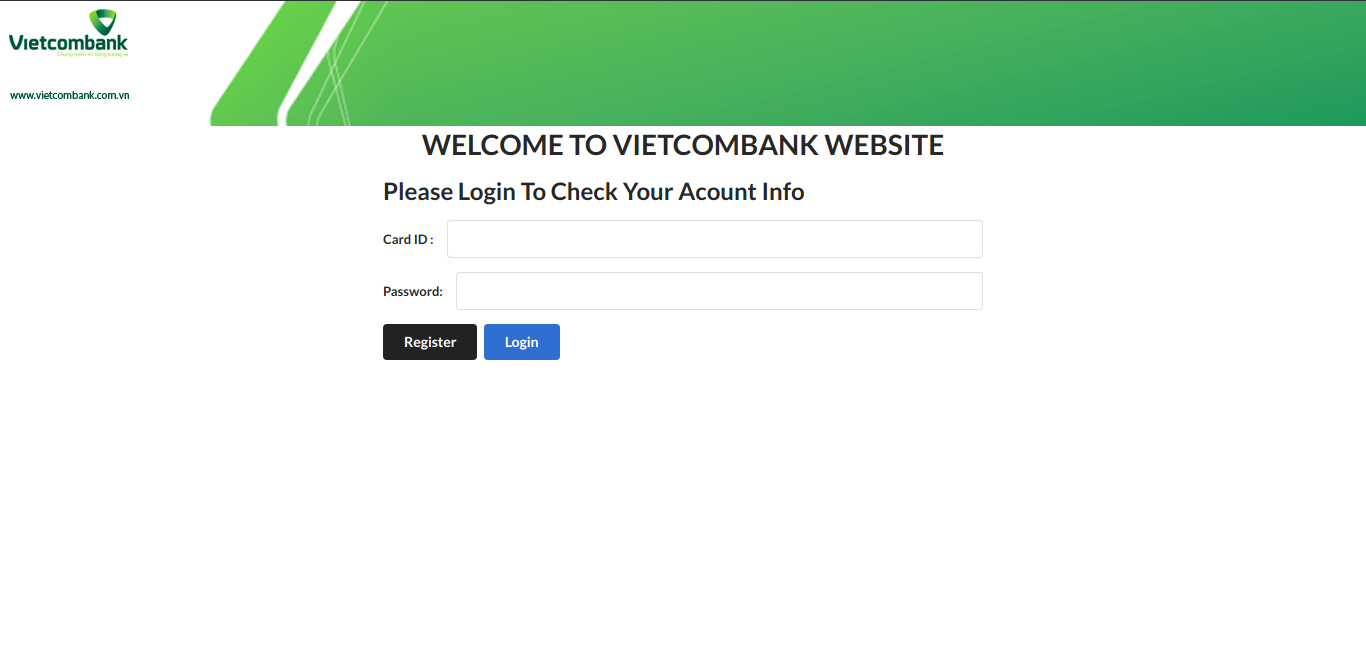


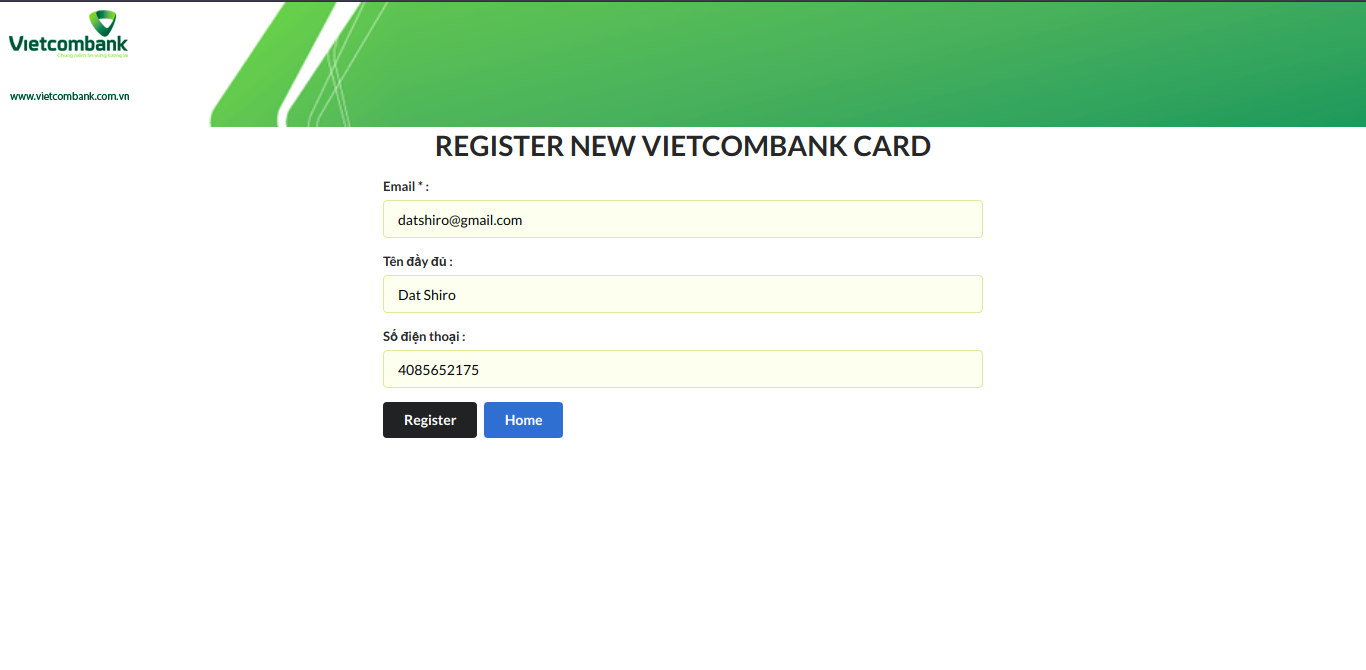
Hình 22: Update profile

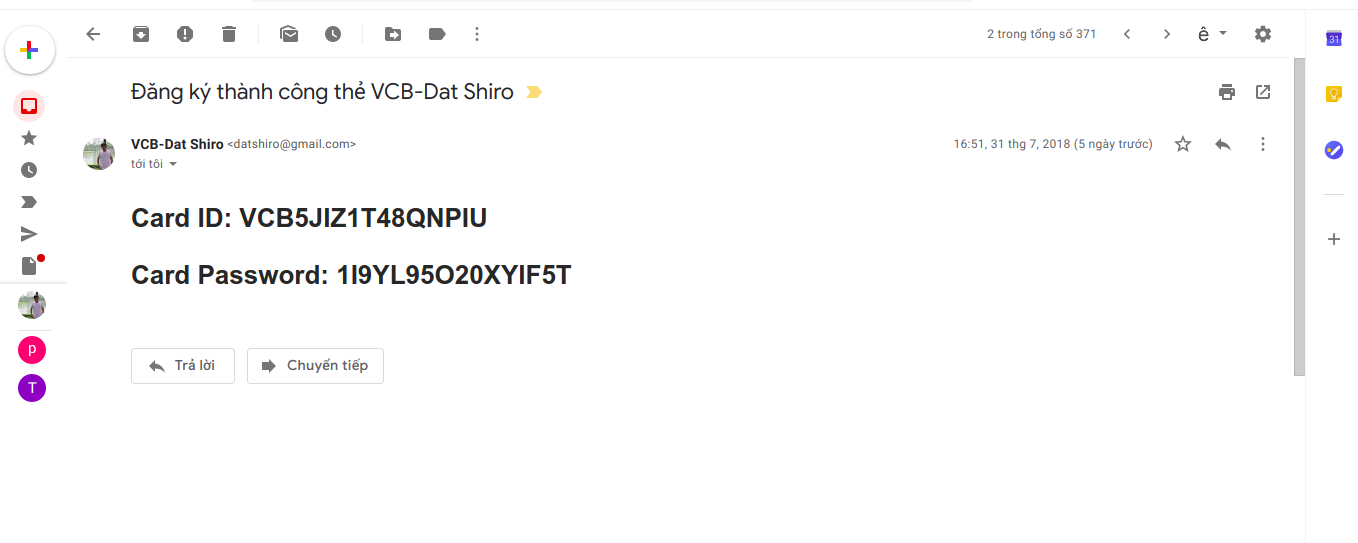
1. **Xây dựng website ngân hàng đơn giản với chức năng:**

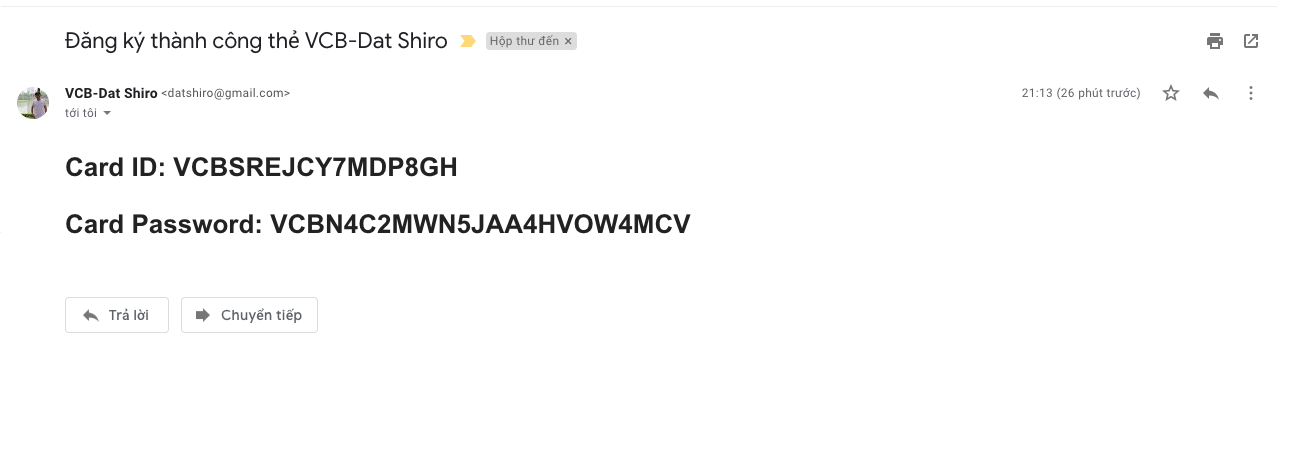
Đăng ký tài khoản ngân hàng

Gửi Email thông tin tài khoản

Hình 23: Trang chủ ngân hàng

****

Hình 24: Trang đăng ký tài khoản

****

Hình 25: Mail cung cấp tài khoản

1. **Xây dựng web service paymenet gateway với chức năng:**

Thực hiện các nhiệm vụ trung gian giữa merchant và issuer bank trong giao thức SET

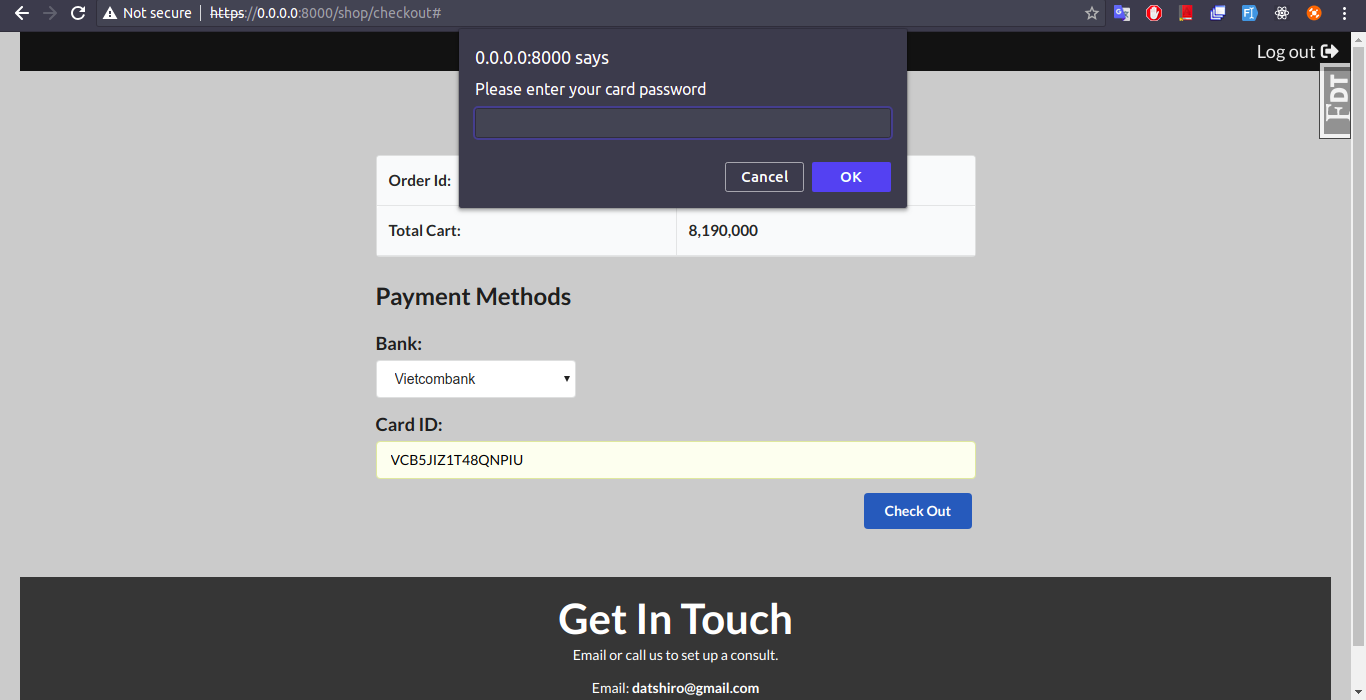
**Ứng dụng giao thức SET vào website thương mại điện tử:**

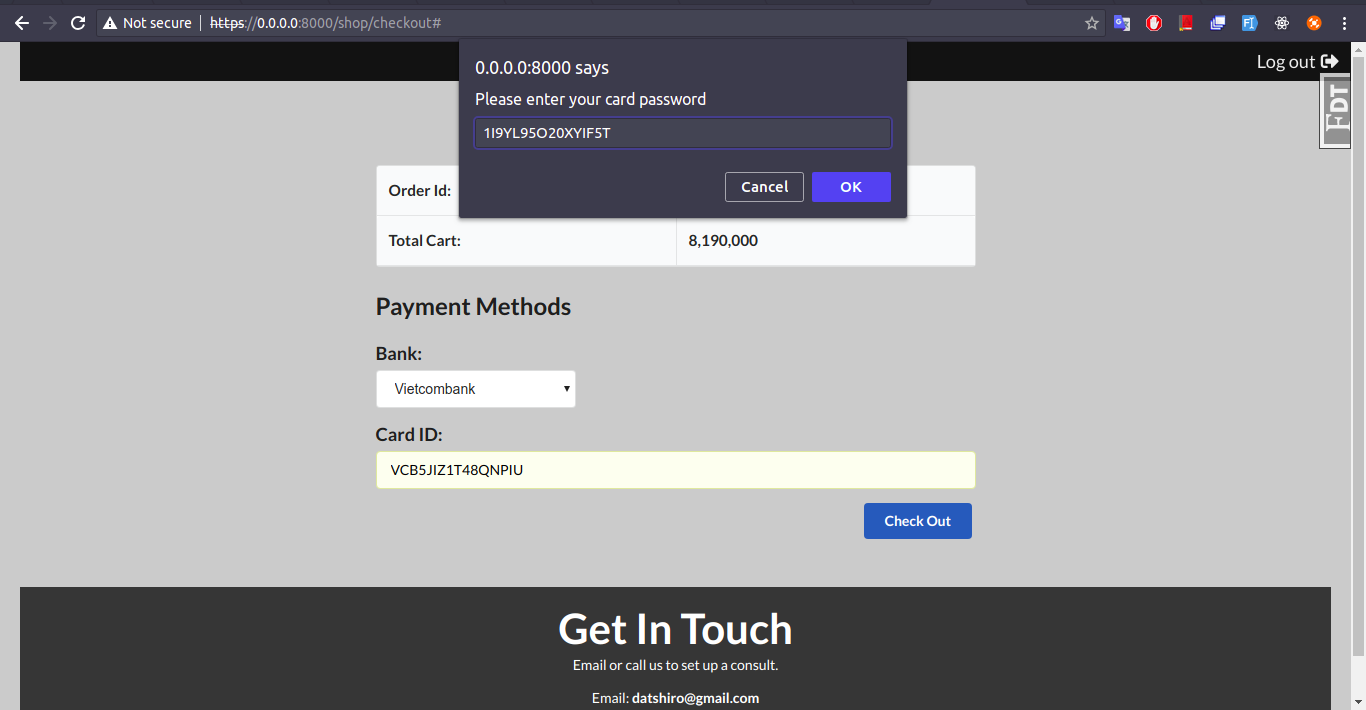
Bảo mật các giao dịch mua bán và thanh toán trực tuyến.

Request từ client với OI và PI được mã hóa bằng Javascript ở phía client trước khi được gửi đến cho Merchant (Website)

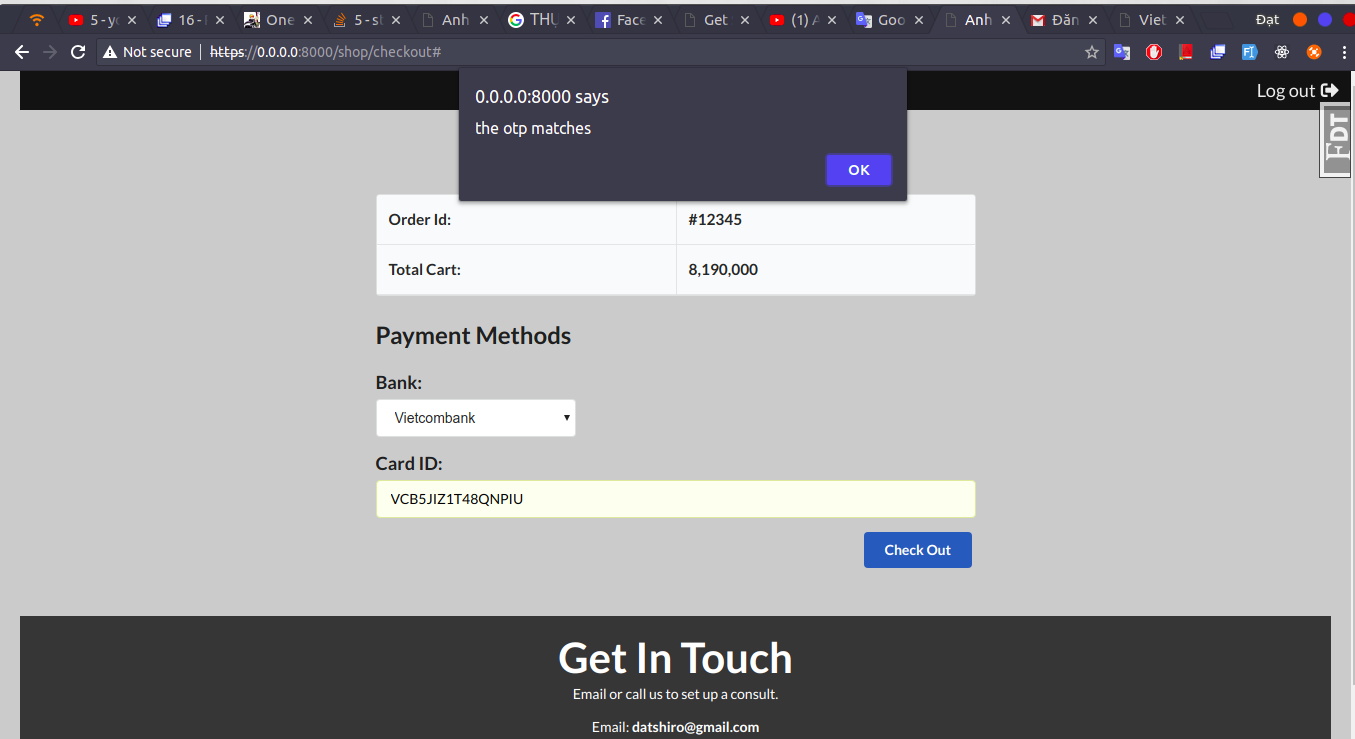
Các thông tin giao dịch, thông tin giỏ hàng, tài khoản và mật khẩu ngân hàng đều được mã hóa trước khi gửi đến Merchant - Gateway - Issuer bank

Chứng thực, xác thực với ngân hàng.

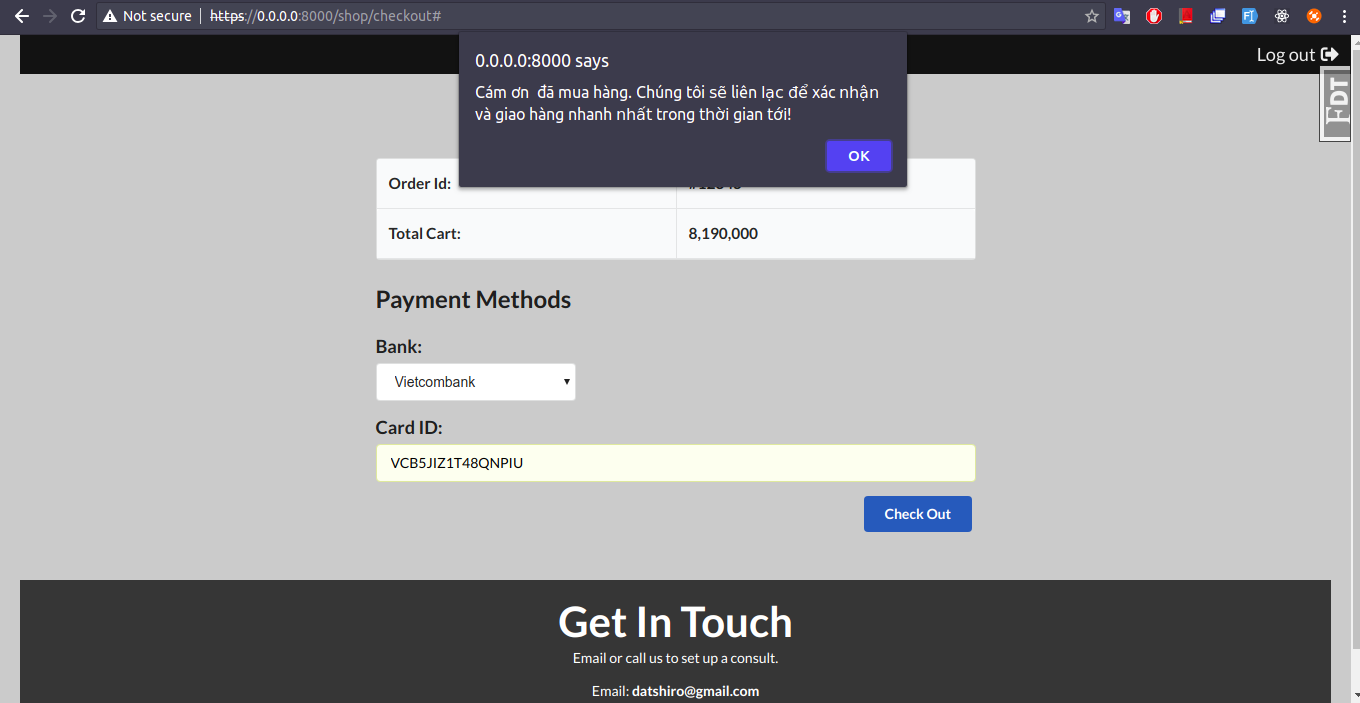
Hình 26: Nhập đúng CardID



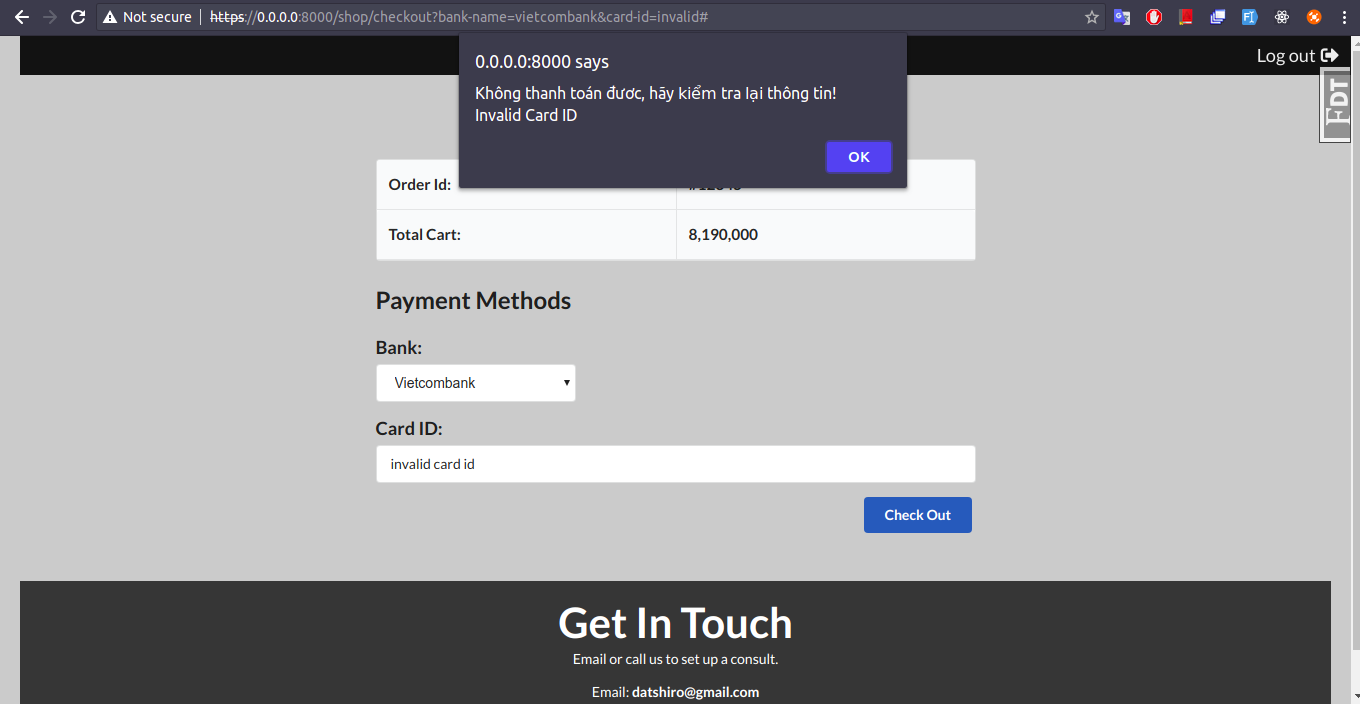
Hình 27: Nhập đúng password



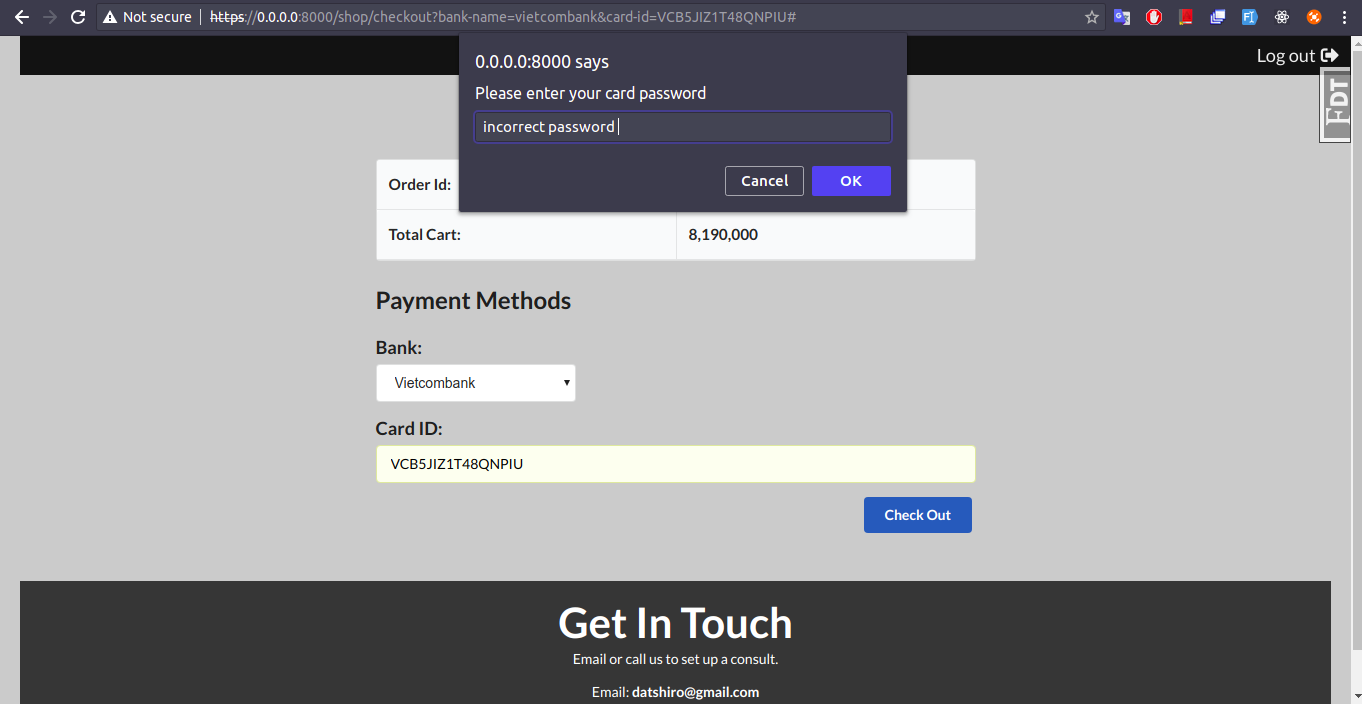
Hình 28: Thông báo xác thực thành công

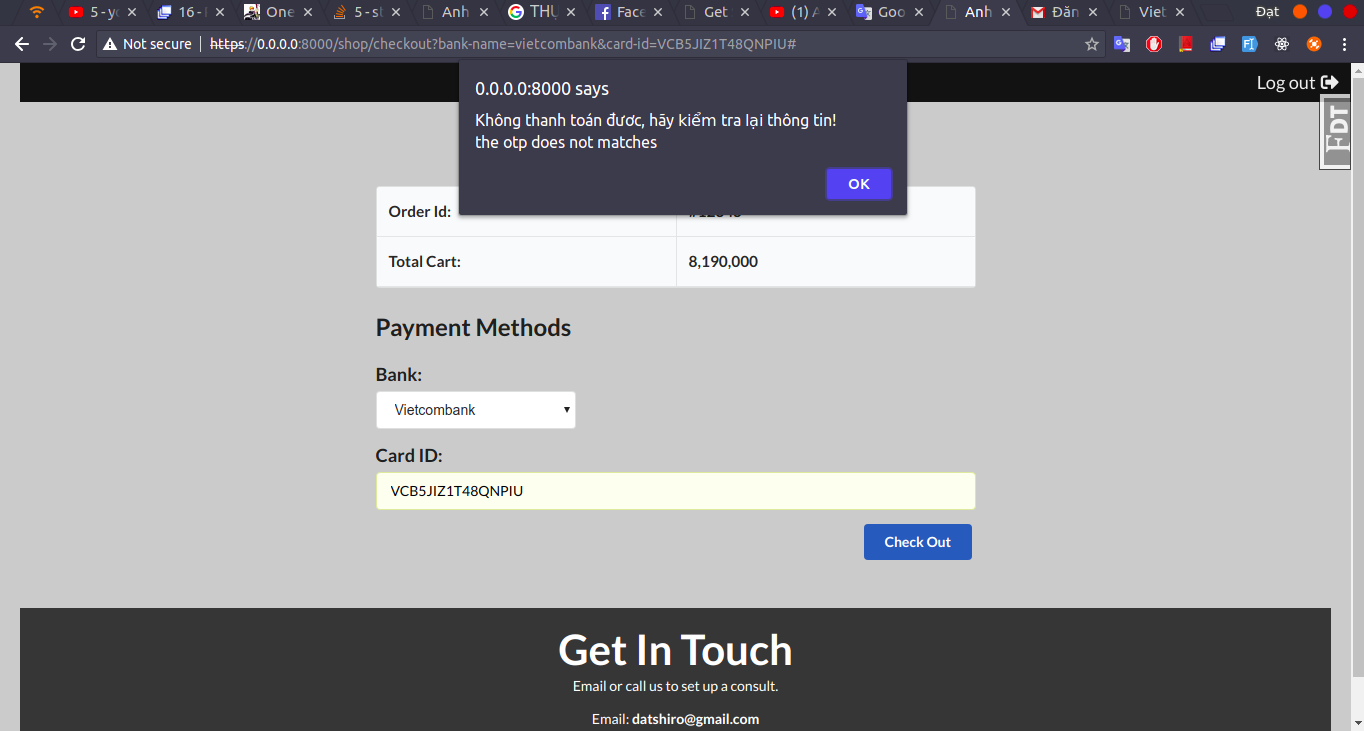


Hình 29: Mua hàng thành công



Hình 30: Nhập sai ID



Hình 31: Nhập sai password

Hình 32: Xác thực thất bại

**KẾT LUẬN**

Giao thức SET là một giao thức an toàn cho thanh toán điện tử, đáp ứng các yêu cầu bảo mật trong thương mại điện tử và xác định danh tính người dùng cuối.

• Usability: cardholder, merchant cần được cài đặt đặc biệt. Quá trình khởi tạo thì đơn giản vì cardholder không cần phải có certificate.

• Flexibility: Giao thức SET có thể sử dụng trên bất cứ máy tính nào vì ở thời điểm hiện tại giao dịch thương mại điện tử chỉ đơn giản dựa trên SSL/TLS cho giao tiếp giữa Cardholder và Merchant.

• Affordability: SET chỉ cần có security certificates merchant, payment gateway và issuer bank, là có thể cấu hình.

• Reliability: Các yếu tố quan trọng bảo mật của giao thức SET là không chắc chắn, vẫn còn một khả năng đáng kể là các lỗ hổng tình cờ sẽ xuất hiện trong quá trình thực hiện. Kinh nghiệm quá khứ cho thấy rất khó để sản xuất phần mềm không có lỗ hổng có thể khai thác bởi phần mềm độc

• Availability: Giao thức SET, card issuers và acquirers không cần thiết phải lệ thuộc vào một hệ thống nào với VISA. Vì issuer có phần mềm và có thể hỗ trợ giao dịch SET. Công bằng mà nói, người dùng sẽ thoải mái thực hiện một bước đăng ký đơn giản để có mật khẩu và cài đặt mà không cần có chứng chỉ bảo mật

• Speed of transaction: Giao thức SET sử dụng AES cho mã hóa đối xứng và RSA để xác minh chứng chỉ. Việc xác minh issuer của chủ thẻ là một yếu tố quan trọng đối với hiệu suất giao dịch. Giao thức SET tránh sự phức tạp liên quan đến Visa. Rất khó để xác định tốc độ giao dịch vì nó liên quan đến tốc độ mạng và hiệu suất của máy chủ

• Interoperability: SET có thể được cài đặt trên máy tính dễ dàng, vì vậy khả năng tương thích rất cao

**TÀI LIỆU THAM KHẢO**

**Tiếng Anh:**

1. Miguel Grinberg, Flask Web Development, O’Reilly Media Inc, USA,1st Edition, 2014

2. A Secure Electronic Transaction Payment Protocol Design and Implementation - (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 5, 2014

**Tiếng Việt**

3. Bảo Mật Hệ Thống Thông Tin - Lê Phúc

**Danh mục Website tham khảo:**

1. https://semantic-ui.com/

2. https://docs.mongodb.org/manual/

3. http://flask.pocoo.org/docs/1.0/

4. <https://vi.wikipedia.org/wiki/>

5. https://pycryptodome.readthedocs.io/en/latest/src/public\_key/rsa.html

**BẢNG PHÂN CHIA CÔNG VIỆC**

* **Nguyễn Vũ Đức Anh:**
  + Xây dựng hệ thống CA cung cấp khóa và ứng dụng trong các thành phần trong hệ thống.
  + Viết các công cụ chuyển đổi sử dụng các thư viện có sẵn.
  + Xử lý các hàm viết không đúng quy tắc và viết lại theo cấu trúc mới, gạt bỏ code thừa.
  + Viết hoạt động xử lý thanh toán của ứng dụng web và gateway.
  + Viết các thành phần module liên quan tới phần xử lý được giao