ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
VÀ TRUYỀN THÔNG

ĐÀO QUANG HUYNH

HẠ TẦNG KHÓA CÔNG KHAI, XÂY DỰNG CỔNG TRUYỀN THÔNG THANH TOÁN SONG PHƯƠNG ỨNG DỤNG CHỮ KÝ SỐ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, 2012

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG

ĐÀO QUANG HUYNH

HẠ TẦNG KHÓA CÔNG KHAI, XÂY DỰNG CỔNG TRUYỀN THÔNG THANH TOÁN SONG PHƯƠNG ỨNG DỤNG CHỮ KÝ SỐ

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

TSKH. NGUYỄN MINH HẢI

Thái Nguyên, 2012

LỜI CAM ĐOAN

Tôi xin cam đoan Những nội dung trong luận văn "HẠ TẦNG KHÓA CÔNG KHAI, XÂY DỰNG CỔNG TRUYỀN THÔNG THANH TOÁN SONG PHƯƠNG ỨNG DỤNG CHỮ KÝ SỐ" là do tôi thực hiện dưới sự hướng dẫn trực tiếp của Thầy TSKH. Nguyễn Minh Hải.

Mọi tham khảo dùng trong luận văn đều được trích dẫn rõ ràng tên tác giả, tên công trình, thời gian, địa điểm công bố.

Mọi sao chép không hợp lệ, vi phạm quy chế đào tạo, hay gian trá, tôi xin chịu trách nhiệm hoàn toàn.

Thái Nguyên, tháng 10 năm 2012

Đào Quang Huynh

LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn chân thành nhất tới TSKH. Nguyễn Minh Hải, Thầy đã cho tôi những định hướng, tận tình chỉ bảo giúp đỡ tôi những ý kiến rất quý báu để tôi hoàn thành luận văn tốt nghiệp này.

Tôi xin cảm ơn Trường Đại Học Công Nghệ Thông tin và Truyền thông - Đại Học Thái Nguyên đã hết sức tạo điều kiện cho tôi trong quá trình học, làm và hoàn thành khóa luận này.

Xin chân thành cảm ơn quý Thầy Cô trong khoa Sau đại học Trường Đại học Công nghệ Thông tin và Truyền thông – ĐH Thái Nguyên đã nhiệt tình giảng dạy, trang bị cho tôi những kiến thức quý báu trong suốt thời gian học tập tại trường.

Tôi xin tỏ lòng biết ơn sâu sắc tới các thầy cô, bạn bè đã dìu dắt, giúp đỡ tôi tiến bộ trong suốt quá trình làm khóa luận tốt nghiệp.

Xin gửi lời cảm ơn tới gia đình, những người bạn của tôi đã động viên, giúp đỡ tôi trong suốt quá trình học tập và hoàn thành luận văn.

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

CA	**C**ertificate **A**uthority
COT	**C**ut **O**ff **T**ime
DSA	**D**igital **S**ignature **A**lgorithm
H	**H**ash function
HSM	**H**ardware **S**ecurity **M**odule
IBPS	**I**nter **B**ank **P**ayment **S**ystem
NH	**N**gân **H**àng
NHA	**N**gân **H**àng **A**
NHB	**N**gân **H**àng **B**
MD5	**M**essage **D**igest **5**
PKI	**P**ublic **K**ey **I**nfrastructure
PKCS	**P**ublic **K**ey **C**ryptography **S**tandards
RA	**R**egistration **A**uthority
RFC	**R**equest **F**or **C**omments
RSA	**R**ivest **S**hamir **A**dleman
SHA	**S**ecure Hash Algorithm
SHS	**S**ecure **H**ash **S**tandard
TTĐTSP	**T**hanh **T**oán **Đ**iện **T**ử **S**ong **P**hương
TTSP	**T**hanh **T**oán **S**ong **P**hương

LỜI NÓI ĐẦU

Trong xu hướng phát triển của thế giới và Việt Nam hiện nay, giao dịch qua mạng Internet đang đem đến sự bùng nổ thông tin một cách mạnh mẽ như việc ra đời Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005 và Nghị định Chính phủ số 26/2007/NĐ-CP quy định chi tiết thi hành luật giao dịch điện tử về chữ Ký số và dịch vụ chứng thực chữ Ký số. Để điều chỉnh, giải quyết các vấn đề phát sinh trong giao dịch điện tử và đảm bảo tính pháp lý của giao dịch điện tử.

Nhà nước khuyến khích việc sử dụng chữ ký số và dịch vụ chứng thực chữ ký số trong các lĩnh vực kinh tế, chính trị, xã hội để thúc đẩy việc trao đổi thông tin và các giao dịch qua mạng nhằm nâng cao năng suất lao động; mở rộng các hoạt động thương mại; hỗ trợ cải cách hành chính, tăng tiện ích xã hội, nâng cao chất lượng cuộc sống của nhân dân và bảo đảm an ninh, quốc phòng

Không nằm ngoài xu hướng đó các đơn vị Thanh toán và đặc biệt là trong lĩnh vực Tài chính Ngân hàng các dạng chứng thực và mã hóa thông tin sẽ được chuyển sang nền tảng mã hóa công khai và sử dụng chữ ký số định danh.

Nắm bắt tình hình, xu hướng kết hợp với với được sự định hướng tận tình của TSKH. Nguyễn Minh Hải tôi đã chọn đề tài này có cơ hội tìm hiểu sâu rộng hơn trong Hạ tầng khóa công khai và xây dựng cổng truyền thông ứng dụng chữ ký số cho hệ thống Thanh toán song phương. Trong ngân hàng hiện nay thay thế các phương pháp mã hóa cổ điển, giải thuật không công khai.

I. NỘI DUNG NGHIÊN CỨU CỦA ĐỀ TÀI

1. Đối tượng và phạm vi nghiên cứu

Tìm hiểu quy trình nghiệp vụ chuyển tiền điện tử và cấu trúc điện thanh toán theo chuẩn SWIFT.

Nghiên cứu hạ tầng khóa công khai, chính sách cấp phát, chứng thực, thu hồi kóa, dịch vụ chứng thực khóa công khai.

Xây dựng cổng truyền thông nhận điện thanh toán đến, kiểm tra chữ ký và đi ký trên điện thanh toán đi và gửi điện thanh toán đi.

2. Hướng nghiên cứu của đề tài

Một số điện thanh toán, yêu cầu nghiệp vụ thanh toán, điện phản hồi theo chuẩn quốc tế - SWIFT.

Mô hình truyền nhận dữ liệu hướng dịch vụ SOA, message queue, chứng thực khóa công khai.

Xây dựng cổng thanh toán song phương trong Ngân hàng cho các điện đi và kiểm tra chữ ký số cho điện đến ứng dụng chữ ký số.

3. Phương pháp nghiên cứu

Thu thập, tìm hiểu và phân tích yêu cầu trong thanh toán, mô hình thanh toán điện tử liên Ngân hàng, quy định giá trị pháp lý của chữ ký số trong giao dịch điện tử.

Tìm hiểu yêu cầu đảm bảo tính bảo mật trong thanh toán, đảm bảo tính tin cậy trong truyền thông.

Kết hợp với các nghiên cứu ứng dụng trước đây trong quá trình chuẩn hóa dữ liệu thanh toán đồng bộ theo chuẩn SWIFT.

4. Ý nghĩa khoa học của đề tài

Ứng dụng các tiêu chuẩn trong Thanh toán điện tử trong Ngân hàng.

An toàn, bảo mật và tính nhất quán trong thanh toán điện tử của Ngân hàng là một trong những vấn đề cấp thiết giúp cho các thanh toán viên và giao dịch viên vận hành hệ thống thanh toán theo một quy trình thống nhất.

Đảm bảo tính ổn định nhất quán trong truyền nhận điện đi và đến trong thanh toán được liên tục, an toàn, đồng bộ và tin cậy.

Định danh nhất quán trong điện thanh toán đi với khóa bí mật định danh cho Ngân hàng gửi điện đi là duy nhất.

II. BỐ CỤC CỦA LUẬN VĂN

Luận văn được chia thành 3 chương chính với nội dung như sau:

Chương 1: Tổng quan về Khóa công khai và chữ ký số

Trình bầy tổng quát và một sô khái niệm cơ bản về mật mã và hạ tầng khóa công khai.

Chương 2: Hạ tầng khóa công khai và các thành phần của hạ tầng khóa công khai

Giới thiệu về Hạ tầng khóa công khai, các thành phần của hạ tầng khóa công khai, chính sách cấp phát, chứng thực và thu hồi khóa, quy trình mã hóa và xác thực chữ ký số.

Chương 3: Xây dựng cổng truyền thông trong Thanh toán song phương và ứng dụng chữ ký số.

Giới thiệu về quy trình nghiệp vụ thanh toanh toán viên với hệ thống Thanh toán song phương và quy trình tác nghiệp trên hệ thống.

Xây dựng cổng truyền thông cho Hệ thống Thanh toán song phương ứng dụng chữ ký số cho các điện thanh toán với một số điện thanh toán MT103, MT195, MT196.