

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

**ĐÀO QUANG HUYNH**

**HẠ TÀNG KHÓA CÔNG KHAI,  
XÂY DỰNG CÔNG 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 CÔNG 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 CÔNG 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

LỜI NÓI ĐẦU .....	6
I. NỘI DUNG NGHIÊN CỨU CỦA ĐỀ TÀI .....	7
1. Đối tượng và phạm vi nghiên cứu.....	7
2. Hướng nghiên cứu của đề tài .....	7
3. Phương pháp nghiên cứu.....	7
4. Ý nghĩa khoa học của đề tài .....	7
II. BỐ CỤC CỦA LUẬN VĂN .....	8
CHƯƠNG 1 TỔNG QUAN VỀ KHÓA CÔNG KHAI VÀ CHỮ KÝ SỐ .....	9
1.1. Mật mã học khóa công khai .....	9
1.1.1. Mật mã học .....	9
1.1.1.1. Khóa đối xứng .....	10
1.1.1.2. Khóa công khai .....	11
1.1.1.3. Mục đích .....	11
1.1.2. Ứng dụng .....	13
1.2. Thuật toán và độ phức tạp thuật toán.....	14
1.2.1. Thuật toán .....	14
1.2.2. Độ phức tạp thuật toán.....	14
1.2.3. Phân tích thuật toán.....	15
1.2.3.1. Tính hiệu quả của thuật toán.....	15
1.2.3.2. Đánh giá thời gian thực hiện thuật toán.....	15
1.3. Hàm băm mật mã học .....	16
1.3.1. Hàm băm.....	16
1.3.2. Hàm băm mật mã học .....	16
1.3.3. Tính toàn vẹn dữ liệu .....	16
1.3.4. Một số hàm băm thông dụng .....	17
1.3.4.1. Thuật toán hàm băm MD5 .....	17
1.3.4.2. Chuẩn băm an toàn SHS .....	19
CHƯƠNG 2 HẠ TẦNG KHÓA CÔNG KHAI VÀ CÁC THÀNH PHẦN.....	20
2.1. Hạ tầng khóa công khai .....	20
2.1.1. Hạ tầng khóa công khai là gì và một số khái niệm.....	20
2.1.1.1. Cấu trúc phân tầng của hệ thống khóa công khai .....	21
2.1.1.2. Mô hình xác thực khóa công khai.....	22
2.1.1.3. Khái niệm X.509 và PKCS .....	23
2.1.2. Một vài kiến trúc và công nghệ PKI hiện hành .....	25
2.1.2.1. Một số ứng dụng .....	25
2.1.2.2. Một số hệ thống PKI.....	25
2.2. Chữ ký số, thuật toán tạo và kiểm tra chữ ký số.....	26
2.2.1. Thuật toán chữ ký số RSA .....	26
2.2.2. Thuật toán chữ ký số DSA.....	29
2.3. Cấp phát và xác thực chứng thực số .....	32
2.3.1. Chứng thực số .....	32
2.3.2. Cấp phát chứng thực số.....	33
2.3.3. Thu hồi và cấp phát lại chứng thực số .....	34
2.3.4. Xác thực chứng thực số .....	34

CHƯƠNG 3 XÂY DỰNG CÔNG TRUYỀN THÔNG THANH TOÁN SONG PHƯƠNG VÀ ỨNG DỤNG CHỮ KÝ SỐ .....	36
3.1. Tổng quan hệ thống .....	36
3.1.1. Quy định chung .....	36
3.1.1.1. Nội dung thanh toán .....	36
3.1.1.2. Phương thức thanh toán lãi, phí trong TTĐTSP .....	38
3.1.1.3. Thời gian làm việc của hệ thống TTĐTSP .....	38
3.1.2. Quy trình nghiệp vụ .....	40
3.1.2.1. Tài khoản hạch toán .....	40
3.1.2.2. Quy trình xử lý điện .....	40
3.1.2.3. Sai lầm, sự cố và xử lý .....	41
3.1.3. Quyết toán và đối chiếu .....	42
3.1.3.1. Quyết toán vốn .....	42
3.1.3.2. Đối chiếu .....	43
3.2. Đặc tả kỹ thuật kết nối .....	44
3.2.1. Mô hình kỹ thuật kết nối .....	45
3.2.1.1. Yêu cầu chung .....	45
3.2.1.2. Mô hình kỹ thuật kết nối sử dụng IBM Message Queue .....	46
3.2.1.3. Mô hình kỹ thuật kết nối sử dụng Webservice .....	47
3.2.2. Đặc tả message .....	48
3.2.3. Cấu trúc message .....	49
3.2.3.1. Cấu trúc message Header .....	50
3.2.3.2. Yêu cầu đối với Header .....	51
3.2.3.3. Cấu trúc của message body .....	53
3.3. Một số lệnh thanh toán .....	53
3.3.1. Lệnh thanh toán MT103 .....	53
3.3.1.1. Quy trình xử lý .....	53
3.3.1.2. Luồng message .....	54
3.3.1.3. Mô tả chi tiết .....	54
3.3.2. Điện tra soát MT195 .....	62
3.3.2.1. Quy trình xử lý .....	62
3.3.2.2. Luồng message .....	62
3.3.2.3. Mô tả chi tiết .....	63
3.3.3. Điện tra soát MT196 .....	65
3.3.3.1. Quy trình xử lý .....	65
3.3.3.2. Luồng message .....	66
3.3.3.3. Mô tả chi tiết .....	66
3.4. Cài đặt chữ ký số và xác thực chữ ký số .....	68
3.4.1. Cài đặt hàm ký số .....	68
3.4.2. Cài đặt hàm xác thực chữ ký số .....	70
3.4.3. Một số giao diện chương trình .....	72
3.4.3.1. Kiểm tra Queue .....	72
3.4.3.2. Ký và Put điện thanh toán lên Queue .....	73
3.4.3.3. Get điện thanh toán trên Queue về và xác thực chữ ký .....	74
KẾT LUẬN .....	75
TÀI LIỆU THAM KHẢO .....	76

## DANH MỤC TỪ VIẾT TẮT

CA	<b>Certificate Authority</b>
COT	<b>Cut Off Time</b>
DSA	<b>Digital Signature Algorithm</b>
H	<b>Hash function</b>
HSM	<b>Hardware Security Module</b>
IBPS	<b>Inter Bank Payment System</b>
NH	<b>Ngân Hàng</b>
NHA	<b>Ngân Hàng A</b>
NHB	<b>Ngân Hàng B</b>
MD5	<b>Message Digest 5</b>
PKI	<b>Public Key Infrastructure</b>
PKCS	<b>Public Key Cryptography Standards</b>
RA	<b>Registration Authority</b>
RFC	<b>Request For Comments</b>
RSA	<b>Rivest Shamir Adleman</b>
SHA	<b>Secure Hash Algorithm</b>
SHS	<b>Secure Hash Standard</b>
TTĐTSP	<b>Thanh Toán Điện Tử Song Phương</b>
TTSP	<b>Thanh Toán Song Phương</b>

## 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 khóa, dịch vụ chứng thực khóa công khai.

Xây dựng công 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 công 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 bày tổng quát và một số 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 công truyền thông trong Thanh toán song phương và ứng dụng chữ ký số.

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

Xây dựng công 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.