

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

---

HOÀNG VĨNH HÀ

**NGHIÊN CỨU GIẢI PHÁP XÁC THỰC WEB  
ỨNG DỤNG TRONG GIAO DỊCH ĐIỆN TỬ**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**Chuyên ngành: KHOA HỌC MÁY TÍNH**

**Mã số: 60.48.01**

**Người hướng dẫn khoa học: TS. HỒ VĂN HƯƠNG**

**Thái Nguyên, 2014**

## LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của bản thân. Các số liệu kết quả trình bày trong Luận văn này là trung thực. Những tư liệu được sử dụng trong Luận văn có nguồn gốc rõ ràng, đầy đủ.

*Thái nguyên, tháng 9 năm 2014*

## LỜI CẢM ƠN

Lời đầu tiên, tôi xin gửi lời cảm ơn chân thành nhất tới thầy giáo, TS. Hồ Văn Hương, Ban Cơ yếu Chính phủ, người đã hướng dẫn và chỉ bảo tận tình cho tôi trong suốt quá trình thực hiện Luận văn.

Tôi cũng xin gửi lời cảm ơn tới các thầy, cô giáo đã dìu dắt tôi trưởng thành trong suốt quá trình học tập tại trường Đại học CNTT-TT Thái Nguyên.

Cảm ơn các anh, chị, em trong Công ty EcoIT đã chỉ bảo tận tình trong thời gian tôi học tập thực tế tại Công ty. Đồng thời, cảm ơn anh Hoàng Chiến Thắng, Ban Cơ yếu Chính phủ đã giúp tôi hiểu rõ hơn về hệ thống đăng nhập duy nhất SSO, CAS, SSL, Chữ ký số và ứng dụng trong thực tế.

Cuối cùng tôi muốn gửi lời cảm ơn sâu sắc nhất tới gia đình và bạn bè – nguồn động viên lớn lao mỗi khi tôi gặp khó khăn.

Cảm ơn tất cả mọi người đã luôn bên cạnh giúp đỡ tôi!

*Thái Nguyên, ngày 29 tháng 09 năm 2014*

**Học viên thực hiện**

*(ký và ghi họ tên)*

**Hoàng Vĩnh Hà**

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	iii
DANH MỤC CÁC CHỮ VIẾT TẮT .....	vi
DANH MỤC CÁC HÌNH.....	vii
LỜI MỞ ĐẦU .....	1
CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ .....	3
1.1 Tổng quan về giao dịch điện tử .....	3
1.1.1 Giới thiệu về giao dịch điện tử .....	3
1.1.2 Những hạn chế trong giao dịch điện tử .....	4
1.2 An toàn thông tin trong giao dịch điện tử.....	5
1.3 Tổng quan về Web và ứng dụng WEB .....	8
1.3.1 Kiến trúc một ứng dụng WEB.....	10
1.3.2 Nguy cơ mất an toàn dịch vụ WEB.....	11
1.4 Một số kỹ thuật mật mã ứng dụng trong bảo mật và xác thực web.....	14
1.4.1 Mật mã khoá đối xứng.....	14
1.4.2 Mật mã khoá công khai .....	15
1.4.3 Hàm băm .....	17
1.4.4 Chữ ký số.....	17
1.4.5 Hoạt động gửi và nhận văn bản trong thực tế .....	19
CHƯƠNG 2: MỘT SỐ GIẢI PHÁP XÁC THỰC WEB .....	21
2.1. Một số giải pháp xác thực người dùng của website .....	21
2.1.1. Các yếu tố xác thực .....	21
2.1.2 Một số phương pháp xác thực .....	21
2.2 Hệ thống đăng nhập duy nhất [3] .....	24
2.2.1 Khái niệm .....	24
2.2.2 Đặc điểm.....	24
2.2.3 Mô tả hoạt động.....	25

2.2.4	Một số yếu tố quyết định đến hệ thống SSO .....	27
2.2.5	Một số giải pháp đăng nhập duy nhất .....	28
2.3	Giải pháp ký số, xác thực nội dung Web [4] .....	36
2.3.1	Một số giải pháp ký số đã triển khai trên nền tảng Web .....	36
2.3.2	Phương pháp tiếp cận ký số trên nền tảng Web .....	37
2.4	Sử dụng giao thức SSL/TLS trong quá trình trao đổi giữa Web client và WebServer .....	39
<b>CHƯƠNG 3: XÂY DỰNG VÀ TÍCH HỢP GIẢI PHÁP XÁC THỰC WEB TRÊN CÔNG THÔNG TIN NGUỒN MỞ LIFERAY .....</b>		<b>43</b>
3.1	Xây dựng, tích hợp CAS với cổng thông tin nguồn mở Liferay .....	43
3.1.1	Mô hình xác thực người dùng .....	44
3.1.2	Mô tả quy trình xác thực .....	45
3.1.3	Thiết kế và xây dựng tiện ích quản lý định danh xác thực người dùng ..	45
3.1.4	Xây dựng dịch vụ đăng nhập cho người dùng .....	46
3.2	Xây dựng ứng dụng ký số, xác thực trên nền tảng Web .....	51
3.2.1	Mô hình tổng quan giải pháp ký số, xác thực trên nền tảng Web .....	51
3.2.2	Phân tích thiết kế quy trình ký số, xác thực .....	52
3.2.3	Thiết kế và xây dựng ứng dụng ký số, xác thực trên nền tảng Web .....	58
3.3	Cấu hình, tích hợp giao thức SSL/TLS trong quá trình trao đổi giữa Web Client và Web Server .....	60
3.3.1	Mô tả giải pháp .....	60
3.3.2	Sử dụng giao thức SSL/TLS 2 chiều trong quá trình xác thực người dùng của các website có sử dụng chứng thư số .....	61
<b>KẾT LUẬN .....</b>		<b>66</b>
<b>DANH MỤC CÁC CÔNG TRÌNH LIÊN QUAN ĐẾN LUẬN VĂN .....</b>		<b>67</b>
<b>TÀI LIỆU THAM KHẢO .....</b>		<b>68</b>

## DANH MỤC CÁC CHỮ VIẾT TẮT

TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	DỊCH RA TIẾNG VIỆT
ATTT		An Toàn Thông Tin
CNTT		Công Nghệ Thông Tin
CA	Certificate Authority	Thẩm quyền chứng thực
DES	Data Encrytion Standard	Chuẩn mã hóa dữ liệu
DNS	Domain Name System	Hệ thống tên miền
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Secure Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản an toàn
LDAP	Lightweight Directory Access Protocol	Lightweight Directory Access Protocol
PKCS	Public Key Cryptography Standards	Chuẩn mật mã khóa công khai
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
RA	Registration Authority	Thẩm quyền đăng ký
RSA	Rivest Shamir Adleman	Thuật toán mã hóa RSA
SHA	Secure Hash Algorithm	Thuật toán băm
SPKC	Simple Public Key Certificate	Chứng thư khoá công khai đơn giản
SSL	Secure Socket Layer	Giao thức bảo mật web
TLS	Transport Layer Security	Giao thức bảo mật tầng truyền thông

## DANH MỤC CÁC HÌNH

Hình 1.1 Thống kê bảo mật ứng dụng WEB.....	10
Hình 1.2 Kiến trúc một ứng dụng WEB. ....	10
Hình 1.3 Mã hóa khóa bí mật.....	14
Hình 1.4 Mã hóa khóa công khai .....	15
Hình 1.5 Xác thực thông tin.....	16
Hình 1.6 Ký và mã hoá với khóa công khai.....	17
Hình 1.7 Sơ đồ tạo và ký số văn bản.....	18
Hình 1.8 Sơ đồ kiểm tra chữ ký .....	19
Hình 1.9 Ký và gửi tệp văn bản .....	20
Hình 1.10 Nhận và kiểm tra chữ ký .....	21
Hình 2.1 Mô hình Single Domain SSO.....	26
Hình 2.2 Mô hình Multi Domain SSO .....	27
Hình 2.3 Mô hình CAS .....	31
Hình 2.4 Mô hình OpenSSO .....	32
Hình 2.5 Mô hình OpenID .....	35
Hình 2.6 Mô hình ký số dữ liệu trên Server.....	39
Hình 3.1 Kiến trúc Liferay portal.....	43
Hình 3.2 Mô hình xác thực người dùng .....	44
Hình 3.3 Mô hình tiện ích quản lý định danh chuẩn.....	46
Hình 3.4 Cài đặt tệp tin server.xml .....	46
Hình 3.5 Giao diện tích hợp CAS .....	47
Hình 3.6 Cài đặt giao diện tích hợp với CAS .....	47
Hình 3.7 Tạo khóa riêng bằng câu lệnh .....	48
Hình 3.8 Tạo chứng nhận từ khóa riêng .....	48
Hình 3.9 Đăng ký xác thực vào keystore của java.....	49
Hình 3.10 Cài đặt CAS trên Liferay Portal .....	49
Hình 3.11 Kiểm tra kết nối tới CAS và thành công.....	49
Hình 3.12 Hoàn thành tích hợp CAS .....	50

Hình 3.13 Đăng nhập xác thực CAS .....	50
Hình 3.14 Thông báo thành công đăng nhập xác thực CAS.....	51
Hình 3.15 Trạng thái thoát khỏi xác thực CAS.....	51
Hình 3.16 Mô hình tổng quan .....	52
Hình 3.17 Các kiểu cơ bản của CMS .....	54
Hình 3.18 Lược đồ ký số dữ liệu .....	56
Hình 3.19 Lược đồ xác thực dữ liệu tổng quan .....	57
Hình 3.20 Giao diện chính .....	58
Hình 3.21 Giao diện chính – Mở rộng .....	59
Hình 3.22 Chọn đường dẫn thư viện PKCS#11 .....	60
Hình 3.23 Xây dựng giải pháp sử dụng giao thức SSL/TLS trong quá trình trao đổi giữa Web Client và Web Server.....	61
Hình 3.24 Mô hình sử dụng giải pháp xác thực 2 chiều SSL/TLS .....	62
Hình 3.25 Lựa chọn chứng thư số xác thực vào website .....	64
Hình 3.26 Nhập mật khẩu thiết bị lưu khóa .....	65



## LỜI MỞ ĐẦU

Ngày nay, công nghệ thông tin phát triển rất nhanh và được ứng dụng vào hầu hết những lĩnh vực trong cuộc sống. Vai trò của công nghệ thông tin ngày càng được nâng cao, không chỉ dừng lại ở những ứng dụng văn phòng, công nghệ thông tin còn được triển khai ở nhiều lĩnh vực khác trong đời sống, kinh tế xã hội và an ninh quốc phòng. Bên cạnh những lợi thế trong việc áp dụng công nghệ thông tin, việc sử dụng CNTT còn tiềm ẩn nhiều vấn đề còn tồn tại, trong đó có việc đảm bảo an toàn thông tin ví dụ như bị đánh cắp dữ liệu, được phép đọc các tài liệu mà không đủ thẩm quyền, dữ liệu bị phá hủy ... Do đó, bên cạnh việc triển khai và sử dụng CNTT, chúng ta cũng phải đảm bảo ATTT. Đảm bảo ATTT chính là đảm bảo hệ thống có được ba yếu tố:

- Tính toàn vẹn
- Tính bí mật
- Tính sẵn sàng

Trong lĩnh vực ATTT, sử dụng chứng thư số đã trở thành một trong các phương pháp giúp chúng ta có thể bảo mật thông tin. Với chứng thư số, người sử dụng có thể mã hóa thông tin một cách hiệu quả, chống giả mạo thông tin, xác thực người gửi. Ngoài ra, chứng thư số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

Bố cục đề tài Luận văn gồm có 3 phần, với nội dung từng phần cụ thể như sau:

### **Chương 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ BẢO MẬT THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ**

Chương này chúng tôi sẽ tìm hiểu về giao dịch điện tử, phân loại giao dịch điện tử, an toàn thông tin trong giao dịch điện tử, một số giải pháp bảo mật giao dịch điện tử, tổng quan về web và ứng dụng web, an toàn dịch vụ web, mật mã khóa đối xứng, mật mã khóa công khai, hàm băm, chữ ký số.

## **Chương 2. MỘT SỐ GIẢI PHÁP XÁC THỰC WEB**

Chương này trình bày về một số giải pháp xác thực web bao gồm: Giải pháp xác thực người dùng Web, hệ thống đăng nhập duy nhất, giải pháp ký số, xác thực nội dung Web và giải pháp sử dụng giao thức SSL/TLS trong quá trình trao đổi giữa Web client và WebServer để xây dựng ứng dụng cho chương tiếp theo.

## **Chương 3. XÂY DỰNG VÀ TÍCH HỢP GIẢI PHÁP XÁC THỰC WEB TRÊN CÔNG THÔNG TIN NGUỒN MỞ LIFERAY**

Chương này xây dựng ứng dụng cụ thể: Xây dựng, tích hợp hệ thống đăng nhập duy nhất CAS với công thông tin nguồn mở Liferay, xây dựng ứng dụng ký số, xác thực trên nền tảng Web, cấu hình, tích hợp giao thức SSL/TLS cũng như tích hợp với thiết bị Etoken.

Do thời gian hoàn thành đề tài có hạn cũng như khả năng nghiên cứu còn hạn chế cho nên em không tránh khỏi những khiếm khuyết, em rất mong có được những góp ý và giúp đỡ của các thầy cô giáo để em có thể tiếp tục đề tài này ở mức ứng dụng cao hơn trong tương lai.

Em xin chân thành cảm ơn.

**Học viên**

**Hoàng Vĩnh Hà**