

LB/DON/13/02

①

# WEB BASED DOMAIN REGISTRATION AND PAYMENT SYSTEM FOR THE LK DOMAIN REGISTRY

This thesis was submitted to the  
**Department of Computer Science & Engineering**  
of the  
**University of Moratuwa**  
in partial fulfillment of the requirements of the  
**Degree of Master of Science**



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

ප්‍රධාන කාර්යාලය  
කොටුඹර විශ්ව විද්‍යාලය, ශ්‍රී ලංකාව  
කොටුඹර  
by

**Rasika Amarasiri**  
Department of Computer Science & Engineering,  
University of Moratuwa,  
Sri Lanka

074347



University of Moratuwa

681.3 "01"

681.324

TH

74347

74347

## DECLARATION

I, Rasika Amarasiri hereby certify that the work included in this thesis has not been submitted in part or whole for any other academic qualification at any institution.

*R. Amarasiri*  
.....

Rasika Amarasiri  
Research Student.



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

### ***UOM Verified Signature***

.....

Dr. P.G.V. Dias  
Supervisor

## ABSTRACT

This research developed and evaluated the different aspects such as security, feasibility, etc. of an online domain registration system and a payment gateway for the Sri Lanka Domain Registry as a pilot project in establishing a secure e-commerce infrastructure in Sri Lanka. In doing so, it was able to formalize and stream line the procedures and guidelines of registering domains and eliminate the delays that were earlier involved in registering domains at the registry.

The Internet today has become a place for people to do their day to day purchases as well as for the sale of products to a global market. The security of the information that is being exchanged in such transactions is vital. If the correct methodologies are not used, it could lead to losses to the consumers as well as heavy losses to vendors that could include damage to long built reputation.



University of Moratuwa, Sri Lanka  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

Although the Internet usage in Sri Lanka has risen dramatically since its introduction in 1995, local institutions have still not fully exploited its potential for reaching a global market, the main factor for this is the unavailability of a good secure online payment infrastructure in Sri Lanka. Currency regulations restrict people from using the facilities offered by such infrastructure in other countries. Many of the financial institutions in Sri Lanka are reluctant to offer such facilities because of the fear of fraudulent transactions raised by the myth that submitting sensitive information such as credit card numbers on the Internet is very insecure.

As a results of the research a web based registration system was developed and implemented to handle the domain registration process and a set of guidelines were also developed to assist in the acceptance of domain names. The security of the domain registry's servers was also scrutinized to enable smooth operations of the registry.

Recommendations on selecting a suitable online payment system were also made by evaluating the implementation of different mechanisms.



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)



## ACKNOWLEDGEMENTS

It is my pleasure to thank Dr. Gihan Dias for being my supervisor and committing his time to contribute, guide and instruct me in evaluating, revising and writing up this thesis. My thanks are due to Dr. N. K. Wickramarachchi, Head of the Department of Computer Science and Engineering for arranging the necessary formalities and Dr. Nalin Ranasinghe for serving as the External Examiner.

I should also be thankful to the former Chairman of CINTEC, Prof. V.K. Samaranyake and the CINTEC council for approving the necessary funding for the project. CINTEC also provided me with the opportunity of attending the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) in 1999 and 2000, which helped me in getting information as to how other NICs did their operations. I was also appointed as the Hostmaster for LKNIC which gave me an opportunity to understand the problems involved in managing an NIC and to cater to those problems in the development of the online registration system.

My sincere gratitude is also due to Hatton National Bank, which offered to accept the project as a pilot in introducing online transactions to Sri Lanka. The technical and operational information that was given to me by HNB during the course of the research helped me a lot in evaluating many options for the payment gateway system.

I also make this an opportunity to thank the fellow researchers at the CEEE research lab at University of Moratuwa for being great companions to do research with. Their support at times of difficulty and encouraging words were essential ingredients in accomplishing the tasks that were laid ahead.

# CONTENTS

<b>ABBREVIATIONS</b>	<b>x</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Objectives	1
1.2 The LK Domain Registry	2
1.3 Certification Authorities	3
1.3.1 The OpenCA Project	4
1.3.2 Verisign Registration Authority Service	5
1.3.3 Status of the CA	5
1.4 Payment Gateways	6
1.5 Summary of Work Done	6
1.5.1 Evaluating and Enhancing the Security of Overall System	7
1.5.2 Developing the Payment Gateway	7
1.5.3 Developing the Certification Authority	7
1.5.4 Developing the Web-Based Registration System	8
1.6 Organization of this Document	8
<b>2 THE DOMAIN REGISTRATION SYSTEM &amp; LKNIC</b>	<b>10</b>
2.1 History of The Domain Name System	10
2.2 Why DNS is Important	10
2.3 How DNS Works	11
2.3.1 The Internet Domain Name Space	11
2.3.2 Delegation	12
2.4 Role of a Domain Registry	12
2.4.1 Role of CINTEC	13
2.4.2 The Internet Committee	13

2.5	<i>Domain Registration at LKNIC</i>	13
2.6	<i>Registration Process in Other Countries</i>	14
<b>3</b>	<b>DEVELOPING THE REGISTRATION PROCESS, GUIDELINES AND REQUIREMENTS</b>	<b>16</b>
3.1	<i>The Process</i>	16
3.1.1	Initiation	16
3.1.2	Evaluation	18
3.1.3	Registration	18
3.1.4	Modifications	19
3.2	<i>The Guidelines</i>	19
3.3	<i>The Role of the Panel</i>	20
<b>4</b>	<b>DEVELOPING THE WEB BASED REGISTRATION SYSTEM</b>	<b>22</b>
4.1	<i>The Main Components</i>	22
4.2	<i>Secure Server</i>	23
4.3	<i>Database Back End</i>	23
4.4	<i>Database Design</i>	25
4.5	<i>The Tables</i>	25
4.5.1	The Requests Table (requests)	25
4.5.2	The Domains Table (domains)	26
4.5.3	The Request Revision Table (dreq_rev)	26
4.5.4	The Panel Table (panel)	26
4.5.5	The Rejects Table (rejects)	26
4.5.6	The Users Table (users)	27
4.5.7	The Online Requests Table (onlreq)	27
4.6	<i>The Front End</i>	27
4.7	<i>CGI Interface</i>	28
4.7.1	Perl	28
4.8	<i>The Modules</i>	29
4.8.1	Requests Module	29
4.8.2	Administration Module	31
4.8.3	Information Search Module	33
4.8.4	Modification Module	34



<b>5</b>	<b>EVALUATING THE SECURITY OF THE DOMAIN REGISTRATION SYSTEM</b>	<b>36</b>
5.1	<i>Implemented Security Features</i>	37
5.2	<i>Recommendations for Further Security</i>	39
<b>6</b>	<b>DEVELOPING THE PAYMENT GATEWAY</b>	<b>41</b>
6.1	<i>Merchant Account</i>	41
6.2	<i>The Hatton National Bank</i>	42
6.3	<i>Credit Card Verification System (CCVS)</i>	43
6.4	<i>Internet Payment Gateway System (IPGS)</i>	45
6.5	<i>MasterCard Payment Gateway System</i>	46
6.6	<i>International Payment Gateway Systems</i>	46
6.6.1	OneWorldCardServices.com	47
6.6.2	Planet Payment	48
6.7	<i>HSBC Payment Gateway System</i>	48
6.8	<i>Summary of Features and Recommendations</i>	49
6.8.1	CCVS	49
6.8.2	IPGS	50
6.8.3	MasterCard Payment Gateway	50
6.8.4	Planet Payment	51
6.8.5	HSBC Payment Gateway System	51
6.9	<i>Overall Recommendation</i>	52
<b>7</b>	<b>CONCLUSIONS AND RECOMMENDATIONS</b>	<b>53</b>
7.1	<i>Summary of Work Done</i>	53
7.1.1	Evaluating and Enhancing the Security of the Overall System	53
7.1.2	Developing the Payment Gateway	53
7.1.3	Developing the Certification Authority	54
7.1.4	Developing the Web-Based Registration System	54
7.2	<i>Experiences</i>	55
7.3	<i>Common Problems Encountered</i>	56
7.4	<i>Future Enhancements</i>	57





<b>APPENDIX A - PUBLIC KEY INFRASTRUCTURE</b>	<b>60</b>
<i>Introduction to Cryptography</i>	60
Symmetric Cryptography	60
Asymmetric Cryptography	61
<i>Public Key Infrastructure</i>	62
<i>Digital Certificates</i>	62
<i>Certification Authority</i>	62
<i>X.509</i>	63
<i>Certificate Hierarchy</i>	65
<i>Certificate Issuing</i>	66
<i>Certificate Distribution</i>	66
<i>Certificate Revocation</i>	66
<b>APPENDIX B - ELECTRONIC PAYMENTS FOR E-COMMERCE</b>	<b>68</b>
<i>History of Electronic Payments</i>	68
<i>Current Methods</i>	69
<i>Stored Account Payment Schemes</i>	69
Secure Electronic Transaction (SET)	70
<i>Stored Value Payment Schemes</i>	72
<b>APPENDIX C - WEB BASED INTERFACES</b>	<b>73</b>
<i>Common Gateway Interface</i>	73
<i>Web Based Database Applications</i>	73
<i>Secure Servers</i>	74
<i>Secure Sockets Layer (SSL)</i>	74
The SSL Handshake	75
<b>APPENDIX C - STRUCTURE OF THE TABLES</b>	<b>78</b>
<b>APPENDIX D - SCREEN SHOTS</b>	<b>83</b>


 University of Moratuwa, Sri Lanka.  
 Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)





University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

## ABBREVIATIONS

TLD	- Top Level Domain
ccTLD	- Country Code Top Level Domain
gTLD	- Global Top Level Domain
LKNIC	- Sri Lanka (LK) Network Information Center
DNS	- Domain Name System
CINTEC	- Council for INFORMATION TECHNOLOGY in Sri Lanka
CA	- Certification Authority
RA	- Registration Authority
PKI	- Public Key Infrastructure
SSL	- Secure Sockets Layer



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)