A Model Certificate Authority for Sri Lanka

Thesis presented by
M. P. Dileepa Lathsara

Supervised by
Mr. Shantha Fernando

Co-Supervisors
Prof. Gihan Dias
Dr. Chandana Gamage

This research was carried out as a partial fulfillment of the requirement for the Degree of Master of Science

A report submitted to the
Department of Computer Science and Engineering
University of Moratuwa
Sri Lanka

December – 2008

Declaration

"*The work included in this report was done by me, and only me, and the work has not been submitted for any other academic qualification, at any institution*".

…….

Student

M. P. Dileepa Lathsara (078266U)

"*I certify that the declaration above by the candidate is true to the best of my knowledge and that this report is acceptable for evaluation for the MSc research project*".

……

Supervisor

Mr. Shantha Fernando

Abstract

Beginning with the widespread availability of Internet technologies, especially the World Wide Web, the trend has been for organizations to shift their operations online. There are many factors promoting this trend and the main ones among them are global reach, cost savings, and new business opportunities that organizations can achieve by operating in an online model. When moving from long established operating procedures and principles in the brick-and-mortar world, to the cyberspace, organizations are faced with a multitude of new requirements, which are taken for granted in the conventional business model. Some of the principle requirements are in the domain of identity and trust, two concepts that are closely related, as the notion of trust is reposed in an identified entity.

An entirely new layer of online support infrastructure has been developed to provide services in the area of identity and trust. This technical service layer is supported in the real world activities by legislative and judicial mechanisms. In Sri Lanka, the main legislative support structures for online activities have been the Electronics Transaction Act No 19, 2006 of Sri Lanka and the Computer Crimes Act No 24, 2007 of Sri Lanka. The first act provides for a legal framework in which transactions can be conducted on the cyberspace with methods and procedures for establishing validity and enforcing compliance with agreements. The second act provides for a protective barrier against online acts that are of criminal nature and is intended to enhance the prospects of adaptation, of online activities, in every sphere of activity in Sri Lanka.

The main set of technologies that are used in providing identity and trust services, in the online world is based on digital certificates and its management is done through a certification authority (CA). The focus of the research work presented in the dissertation is to analyze the use of digital certificates to provide identity authentication services and study models for implementing a secure and efficient CA for Sri Lanka that is scalable in its user base and extensible in service offerings. The dissertation presents the outcome of a case study in implementing a CA as a pilot project and evaluates different cryptographic technologies, security protocols, and policies that can be used for efficient operation of a CA.

Acknowledgement

I would like to express my gratitude to all, those who gave me the prospect of completing this dissertation. I am deeply grateful to my supervisor Mr. Shantha Fernando for supervising this project and using his valuable time to instruct and guide me, throughout my work. In addition, I would like to thank my co-supervisor Prof. Gihan Dias, for encouraging me to go ahead with my research and for his valuable insights and comments. My special thanks go to co-supervisor Dr. Chandana Gamage whose, stimulating suggestions and encouragement, helped me during the time of research and writing of this dissertation.

I want to thank the Department of Computer Science and Engineering of The University of Moratuwa, Head of the department, Ms Vishaka Nanayakkara, Dr. Sanath Jayasena and all the other lecturers in the department for their support and permission, to carry out the necessary research work. Thanks are also due to Dr. Shahani Weerawarna and Dr. Ajith Pasqual for offering imperative suggestions for improvement of this dissertation.

Furthermore, I have to thank the TechCERT and the LK Domain registry for providing the financial support and giving me permission to use the resources of the organization for my work. My colleagues from TechCERT, LK Domain Registry, and the Department supported me in my research work. I wish to thank them for all their help, support, interest, and valuable suggestions.

I would also wish to thank Information and Communication Agency (ICTA) of Sri Lanka and the Lanka Government Network (LGN) and its staff for the help and the support given to me in many ways.

Especially, I would like to give my special thanks to my parents and my loving wife Dulashinie whose patient temperament allows me to conclude this work.

Thank you

M. P. Dileepa Lathsara

Table of Contents

Table of Figures