UNIVERSITI TEKNOLOGI MARA

SECURE FILE SHARING WITH PUBLIC KEY INFRASTRUCTURE (PKI) ENABLEMENT

NOOR AZLINA BINTI ISMAIL @ HASSAN

BACHELOR OF COMPUTER SCIENCE (Hons.)
FACULTY OF COMPUTER AND MATHEMATICAL SCIENCES

JULY 2015

UNIVERSITI TEKNOLOGI MARA

Secure File Sharing with Public Key Infrastructure (PKI) Enablement

Noor Azlina Binti Ismail @ Hassan

Thesis submitted in fulfillment of the requirements
for Bachelor of Computer Science (Hons)
Faculty of Computer and Mathematical Sciences

July 2015

SUPERVISOR'S APPROVAL

SECURE FILE SHARING WITH PUBLIC KEY INFRASTRUCTURE (PKI) ENABLEMENT

By

NOOR AZLINA BINTI ISMAIL @ HASSAN
2012240752

This report was prepared under the supervision of the project supervisor, Miss Hajar Izzati Binti Mohd Ghazalli It was submitted to the Faculty of Computer and Mathematical Sciences and was accepted in partial fulfillment of the requirements for the degree of Bachelor of Computer Science (Hons).

Approved by

……..……..
Miss Hajar Izzati Binti Mohd Ghazalli
Project Supervisor

JULY 30, 2015

STUDENT'S DECLARATION

I certify that this report and the project to which it refers is the product of my own work and that any idea or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

……
NOOR AZLINA BINTI ISMAIL @ HASSAN
2012240752

JULY 30, 2015

ABSTRACT

Nowadays, security and privacy is needed in during transferring a file through network especially when transferring an important and confidential document. By using digital certificate that issuance by Certificate Authority with Public Key Infrastructure (PKI) approach for this sytem, people can ensure the security and privacy of exchange file with digital signature through insecure network. The public key and private key cryptographic key pair that is obtained and shared through trusted authority will used to sign and verify the document file. The PKI is used to secure the exam question file during the preparation of exam question at Universiti Teknologi MARA, Jasin, Melaka. This system will used RSA and SHA-256 to produce digital signature because both of the algorithm consist more advantages than other algorithm which is suitable to used to protect document in current insecure network. The result of digital signature that has been produce by the system can be seen in the sign file module. As for digital storage, USB token with authentication mechanism can be used to protect the digital certificate from being stolen by other people as future recommendation.

Keywords: public key cryptography, encryption, asymmetric cryptography