DESIGN AND IMPLEMENTATION OF SECURE SOLUTION FOR M-GOVERNMENT ON MOBILE PLATFORMS USING HYBRID OF NTRU-PKI AND AES-RIJNDAEL

By

MALIK ANAS TAWFEEQ

A Dissertation Submitted in Fulfillment of

the Requirement for the Degree of Master of Information Technology

College of Graduate Studies

Universiti Tenaga Nasional

December 2013

ABSTRACT

In recent years and specifically in the era of rapid technology development, many changes have taken place in the field of communication technologies (ICT), where mobile devices have replaced computers in multiple significant tasks. This has influenced the interactions between citizens and government agencies in what is called the m-Government, which is an extension of the e-Government that provides services to citizens in general or subscribers in particular. As these services range from public to private bodies and data transmitted sometimes require authentication and confidentiality, the need to secure them has been found to be inevitable. In this dissertation, the author proposes a technique to secure the transmission of the Electronic Medical Records using hybrid security algorithms of AES-Rijndael and NTRU, since with concentration on confidentiality and authentication as core services in m-Government current transactions, in order to enhance the security of transmission medium and achieve better security of m-Government services. The findings of this dissertation have shown proof of the powerful presence of security factors concerning confidentiality and authentication in the field of m-Government, and test performance approves that the proposed technique is applicable on smartphone devices.

DECLARATION

I hereby declare that this thesis, submitted to Universiti Tenaga Nasional as fulfillment of requirements for the degree of Master of Information Technology has not been submitted as an exercise for a similar degree at any other university. I also certify that the work described here is entirely my own except for excerpts and summaries whose sources are appropriately cited in the references.

This thesis may be made available within the university library and may be photocopied or loaned to other libraries for the purposes of consultation.

December 2013 MALIK ANAS TAWFEEQ

TABLE OF CONTENTS