THE USABILITY AND SECURITY OF ENCRYPTION APPLICATIONS USING TOKEN-BASED AUTHENTICATION

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Information Security

By:

Riham AlMahawes

Under Supervision of:

Dr. Fahad Al- Harby

Submitted to:

Department of Information Security, Computer and Information Security College

Naïf Arab University for Security Sciences

April 2019

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviations	Explanations
3DES	Triple DES
AES	Advanced Encryption Standard
API	Application programming interface
ASQ	Ages and Stages Questionnaires
ASVS	The OWASP Application Security Verification Standard
CA	Certificate Authority
CBS	Crypto-Biometric System
CC	Common Criteria
CERT	A Computer Emergency Response Team
CIF	Common Industry Format Standards
CIS	Centre for Internet Security
CMA	Crypto Misuse Analyzer
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certification Revocation List
DES	Data Encryption Standard
DMAIC	Define, Measure, Analyse, Improve and Control
ESP	Entrust Intelligence Security Provider
GLBA	Gramm-Leach-Bliley Act
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
ID	Identification Number
IP	Internet Protocol
ISO	International Standards Organization
ISSAF	Information Systems Security Assessment Framework
KKESH	King Khaled Eye Specialist Hospital
NIST	US National Institute of Standard and Technology
OSSTMM	Open Source Security Testing Methodology
OWASP	Open Web Application Security Project

PA	Policy Administrator
PACMAD	People at the Centre of Mobile Application Development
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTES	Penetration Testing Execution Standard
RA	Registration Authority
SAC	SafeNet Authentication Client
SCR	Certificate Signing Request
SDLC	Software Development Life Cycle
SEQ	Single Ease Question
SMEQ	Subjective Mental Effort Questionnaire
UME	Usability Magnitude Estimation
USB	Uniform Resource Locator.
VA	Validation Authority
VBA	Visual Basic for Applications
VPN	Virtual private network
WWW	World Wide Web