

**UNIVERSITY TEKNOLOGI MARA**

**DIGITAL SIGNATURE IN E-  
CERTIFICATE**

**MUHAMMAD IQHUAN HARIIRIE BIN  
SUHAIMI**

**BACHELOR OF COMPUTER SCIENCE (Hons.)**

**JANUARY 2025**

## **ACKNOWLEDGEMENT**

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thanks go to my supervisor, Muhammad Atif Bin Ramlan, for his invaluable guidance, support, and patience throughout this project. Your insights and expertise were instrumental in the completion of this research.

Special appreciation also goes to my beloved parents for their unwavering support, encouragement, and prayers, which have been a constant source of strength for me.

Lastly, I'd like to express my heartfelt gratitude to my friends for their unwavering support, understanding, and encouragement. Their kindness and belief in me played a huge role in helping me complete this research.

## ABSTRACT

The project implements RSA digital signatures to tackle authenticity and integrity issues with e-certificates at Universiti Teknologi MARA Kuala Terengganu's activity clubs. Users generate and sign e-certificates securely through a Next.js and Firebase-built web-based platform that provides verification capabilities. The system uses RSA digital signatures to ensure e-certificate integrity and authenticity. The system enables automatic e-certificate generation and batch signing and provides secure email distribution through the Resend API in addition to online and PDF-native verification options. Nine participants from the activity club committee with students took part in the evaluation by completing System Usability Scale (SUS) tests which yielded a score of 70.3 showing good usability. Test results from comprehensive functionality evaluation showed that essential system features operated successfully for e-certificate generation and digital signing followed by verification and distribution. Self-signed certificates used for internal university purposes successfully prevent unauthorized changes which protects e-certificates from alteration and confirms their integrity and authenticity. The practical implementation offers a usable approach toward digital credential management in educational institutions while new features can be developed in the future.

## TABLE OF CONTENTS

CONTENT	PAGE
SUPERVISOR APPROVAL	ii
STUDENT DECLARATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	xi

### CHAPTER 1 INTRODUCTION

1.1	Background of Study	1
1.2	Problem Statement	2
1.3	Objective	4
1.4	Project scope	4
1.5	Project Significance	5
1.6	Overview of Research Framework	6
1.7	Conclusion	7

### CHAPTER 2 LITERATURE REVIEW

2.1	Introduction	8
2.2	Background on E-certificates and Verification Mechanisms	9
2.2.1	E-certificates: Definition and Importance	9
2.3	Overview of Hash Functions and SHA-256	10
2.3.1	Introduction to Hash Functions	10
2.3.2	Cryptographic Hash Functions	10
2.3.3	The SHA Family	12
2.3.4	Detailed Explanation of SHA-256	14
2.4	Digital Signature and RSA	16
2.4.1	Introduction to Digital Signatures	16
2.4.2	Public Key Infrastructure (PKI)	17
2.4.3	Rivest Shamir Adleman (RSA)	18
2.5	Implementation digital signature in Various Problems	19
2.6	Similar Works	28
2.7	The Implication of Literature Review	39
2.8	Conclusion	40

## **CHAPTER 3 METHODOLOGY**

3.1	Overview of Research Methodology	41
3.1.1	Research Methodology Phases	41
3.2	Preliminary Phase	43
3.2.1	Domain Requirement and Literature Study	43
3.3	Design Phase	44
3.3.1	System Architecture	44
3.3.2	Entity Relationship Diagram	45
3.3.3	Use Case Diagram	47
3.3.4	Flowchart	48
3.3.5	User Interface Design	51
3.3.6	Pseudocode	53
3.3.7	Prototype Implementation	56
3.3.7.1	Hardware Specification	57
3.3.7.2	Software Specification	58
3.4	Project Testing	58
3.4.1	User Evaluation	59
3.5	Gantt Chart	60
3.6	Conclusion	60

## **CHAPTER 4 RESULT AND DISCUSSION**

4.1	Logical Design	62
4.1.1	Key Generation Process in Local Development	63
4.1.2	Signing Process	65
4.1.3	Online Verification Process	66
4.1.4	Digital Signature Verification Process	67
4.1.5	Distribution Process	68
4.2	Program Codes	69
4.2.1	Key Generation Process	69
4.2.2	Signing Process	73
4.2.3	Verification Process	82
4.3	User Interfaces	85
4.4	Usability and User Functionality Testing	109
4.4.1	Usability Testing	109
4.4.2	Functionality Testing	111
4.5	Conclusion	116
4.6	Research Summary	117

## **CHAPTER 5 CONCLUSION**

5.1	Project Summary	120
5.2	Project Limitations	121
5.3	Future Recommendations	122
5.4	Conclusion	124

## **REFERENCES 125**