



NALBARI COMMERCE COLLEGE, NALBARI

Japarkuchi, P.O: Chowk Bazar, Nalbari, Assam - 781334

Submitted on partial fulfillment for the three years Degree
Course

Bachelor of Vocational (RMIT)

Of

GAUHATI UNIVERSITY

A PROJECT REPORT

ON

"DIGITAL SIGNATURE"

ACADEMIC GUIDE:

Dr. DEVAJIT MAHANTA
Asstt. Professor & HoD
Dept. of B.VOC (IT)
N.C.C, Nalbari

SUBMITTED BY:

RAJ KUMAR BAXLA
Reg. No: 21069043
Roll No: UA-211-200-0034
B.Voc (RMIT)

Nalbari Commerce College

Japarkuchi, P.O. Chowk Bazar, Nalbari, Assam-781334

CERTIFICATE OF GUIDANCE



This is to certify that **RAJ KUMAR BAXLA**, Student of **B.VOC (CBCS) 6th** Semester of **Retail Management & IT** and Roll No-**UA-211-200-0034** & Registration No-**2106943**, has prepared this Project titled "**Digital Signature**" study Under my guidance during the session 2023-24.

I wish him success in life.

Dept. of B.VOC (IT)



DR. DEVAJIT MAHANTA
Asstt. Professor & HoD
Nalbari Commerce College
Nalbari, Assam

Table of Contents

Page no

1. Abstract

2. Introduction

3. Information Technology Act

4. Objectives

Ensuring the Security and Integrity of Digitally Signed Documents

Providing a User-Friendly Interface for Signing and Verifying Documents

5. Aims of the project

Environmental Sustainability

Security Enhancement

Ease of Maintenance

Adherence to Standards

6. Methodology

Test Plan Development

Functional Testing

Performance Testing

Documentation Validation

Validation Against Standards

Data Integrity Testing

7. Digital Signature Overview

What is a Digital Signature?

How Does a Digital Signature Work?

Key elements of a digital signature process

Why Digital Signatures Matter

Applications of Digital Signatures

8. Technologies Used

Cryptographic Algorithms

Hash Functions

Cryptographic Libraries

User Interface (UI) Technologies

Database Technologies

Programming Languages

Digital Certificate Management
Security Protocols
Operating Systems
Cloud Services
Mobile Development Frameworks
Block chain Technology
Biometric Technologies

9. System Architecture

High-Level Components
Communication Channels
Cryptographic Operations
Security Measures
Scalability and Redundancy
Integration and Interoperability
User Experience (UX)
Compliance and Legal Aspects
Performance Optimization

10. Implementation

Coding and Development
Digital Signature Module
User Interface (UI)
Key Management
Database Integration
Security Features
Testing
Deployment
Integration
User Training
Documentation
Compliance and Legal Aspects
Monitoring and Maintenance
User Support
Post-Implementation Review

11. Digital signature generation

12. Digital Signature Verification and Validation

The Digital Signature Algorithm (DSA)

Selection of Parameter Sizes and Hash Functions for DSA

DSA Domain Parameters

Domain Parameter Generation

Domain Parameter Management

Key Pairs

DSA Key Pair Generation

Key Pair Management

DSA Per-Message Secret Number

The RSA Digital Signature Algorithm

RSA Key Pair Generation

Key Pair Management

Assurances

The Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA Domain Parameters

Domain Parameter Generation

Domain Parameter Management

Private/Public Keys

Key Pair Generation

Secret Number Generation

ECDSA Digital Signature Generation and Verification

APPENDIX A: Generation and Validation of FFC Domain Parameters

Generation of the FFC Primes p and q

Generation and Validation of Probable Primes

13. Validation of the Probable Primes p and q

14. Generation of the Probable Primes p and q

15. Validation of the Probable Primes p and q

Generating DSA Primes

Generating Primes for RSA Signatures

16. Conclusion

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to all those who have contributed to my understanding of the project on digital signatures. It is with immense pleasure that I acknowledge the invaluable support and guidance I have received throughout the duration of this project.

I have only studied and understood this project on digital signatures with the help of many individuals who shared their expertise, insights, and resources. Their willingness to share knowledge and offer assistance has been instrumental in my learning journey.

*I am particularly thankful to **Dr. Devajit Mahanta (Asstt. Professor & HOD)** Dept. of B.Voc (IT), whose guidance and mentorship proved invaluable in shaping my understanding of digital signatures. I also extend my appreciation to my fellow students and colleagues who engaged in insightful discussions and provided assistance when needed.*

Finally, I am grateful to my family and friends for their unwavering support and encouragement. This project would not have been possible without their understanding and encouragement.

Once again, I express my sincere thanks to everyone who played a role in my understanding of this project on digital signatures.

RAJ KUMAR BAXLA

Roll No: UA-211-200-0034

Reg. No: 21069043