Software Requirements Specification (SRS)

Digital Document Verification System (Group D)

University of Peradeniya

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document outlines the functional and non-functional requirements for a Digital Document Verification System designed for the University of Peradeniya. The primary purpose of the system is to manage the creation, flow, signing, tracking, and verification of official university documents such as academic transcripts and degree certificates, ensuring their integrity and confidentiality.

1.2 Scope

The system will support the digital management of official documents within the university, automating document workflows and providing secure access based on user roles. It includes functionalities for document creation, approval, signing, tracking, and external verification.

1.3 Intended Audience

This document is intended for developers, testers, project managers, university administrators, and other stakeholders involved in the development and deployment of the system.

1.4 Definitions, Acronyms, and Abbreviations

VC: Vice Chancellor
DVC: Deputy Vice Chancellor
HOD: Head of Department
DMS: Document Management System
PDF: Portable Document Format
2FA: Two-Factor Authentication

2. Overall Description

2.1 Product Perspective

The system is a new, standalone system designed to replace existing manual or semi-digital document handling processes.

2.2 Product Functions

• Document creation and management
• Document forwarding and tracking
• User authentication and authorization
• Document signing and commenting
• Workflow management
• External document verification

2.3 User Classes and Characteristics

• Vice Chancellor (VC)

• Deputy Vice Chancellor (DVC)

• Deans

• Heads of Departments (HODs) Professors, Senior Professors, Senior Lecturers, Lecturers, Probationary Lecturers, Junior Lecturers, Temporary Staff

• Programme Coordinators

• Assistant Registrars (Faculty and Student Registration)

• Authorized Clerks (Student Registration)

• Registrar

• Bursar, Assistant Bursars, Accountants, Clerks (Finance)

• Technical Officers, Lab Attendants, Work Aids, Management Assistants

• External Parties

2.4 Operating Environment

Web-based application compatible with major browsers, hosted on university , with Linux backend and PostgreSQL/MySQL database.

2.5 Design and Implementation Constraints

Must comply with university IT security policies, prefer open-source tech, integrate with Single Sign On, and ensure responsive design.

3. System Features and Requirements

3.1 Functional Requirements

3.1.1 User Authentication and Authorization

• Users shall log in using university credentials.
• The system shall support two-factor authentication (2FA).
• The system shall restrict access based on user roles.

3.1.2 Document Creation and Management

• Users shall create documents using templates or upload them.
• Support for PDF, DOCX formats.
• Users can edit documents with version control enabled.
• Authorized users can add digital signatures and comments.

3.1.3 Document Forwarding and Tracking

• Documents can be forwarded to individuals or role groups.
• The system shall track document status and movement.
• Users shall receive notifications of updates and pending actions.
• A detailed audit trail shall be maintained.

3.1.4 Workflow Management

• Admins can create and assign document workflows.
• The system supports both sequential and parallel workflows.
• Workflows enforce document processing rules.

3.1.5 External Document Verification

• External verifiers can check authenticity using secure methods (e.g., QR codes, unique hashes).
• System returns verification status based on a hash comparison.

3.1.6 Reporting and Analytics

• The system shall generate reports on document flow, user activity, and turnaround times.

3.2 Non-Functional Requirements

• Performance: The system shall respond to user actions within a few seconds under normal load.
• Security: All data shall be encrypted at rest and in transit, with strict access control.
• Usability: The interface shall be intuitive and user-friendly.
• Reliability: System uptime shall be at least 99.5%.
• Maintainability: Modular design to allow easy updates and extensions.

4. External Interface Requirements

4.1 User Interfaces

- Web dashboard for internal users with role-based visibility
- Mobile-friendly version for on-the-go access
- Verification portal for external verifiers

4.2 Hardware Interfaces

- Servers hosting the application

4.3 Software Interfaces

- Support for MS Word (.docx) and PDF (.pdf) document formats.
- Digital signature integration for signing and verifying documents.
- Interface with relational databases for data storage and retrieval.
- Hashing interface for generating and comparing document hashes.
- Secure API or web portal for external verifiers to check document authenticity.
- Email system integration for sending user notifications.
- Web-based user interface for different user roles.

4.4 Communication Interfaces

- HTTPS protocol for all communications
- Email/SMS gateways for notifications

5. Other Requirements

5.1 Data Requirements

- All document versions and metadata will be stored.
- Data backup to be performed frequently

5.2 Security Requirements

- Role-based access control and 2FA
- Digital signatures and tamper-proof document hashes
- Logs of access and modifications

5.3 Legal and Regulatory Requirements

- Adherence to university data policies
- Compliance with national IT security regulations
- Data privacy per local laws (e.g., Data Protection Act)

6. Glossary

- Audit Trail: Record of changes made to a document.
- Document Hash: Unique fingerprint of a document used for verification.
- Two-Factor Authentication (2FA): Additional layer of security during login.
- Workflow: Predefined process for handling documents.

7. Future Enhancements

- AI-based document classification and auto-routing
- Blockchain integration for immutable document verification