1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document describes the requirements for a modern, secure, and AI-driven Document Management System (DMS) that enables multiple-users edit functionality, ensures document verification through digital signatures, maintains document versioning, and supports document scanning management.

The purpose of this document is to provide a detailed and comprehensive description of the system requirements to all stakeholders involved in the design, development, testing, and deployment of the system.

1.2 Scope

The Document Management System will provide a platform that allows creation, editing, storing, versioning, verifying, and managing scanned documents securely with AI-enhanced capabilities, including multi-user editing and digital signature verification.

The primary scope of the system is to improve document collaboration and security in a multi-user environment while supporting scanned document management workflows.

The system will be deployed {{PLACEHOLDER}}

1.3 Intended Audience

- Project Managers
- Software Engineers and Developers
- Quality Assurance/Testers
- End Users (document creators, editors, and approvers)
- Security Analysts
- System Administrators

Additional stakeholders: {{PLACEHOLDER}}

1.4 Intended Use

The system is intended to be used by organizations requiring secure document creation,

collaborative editing, version control, digital signature verification, and scanned document management within regulated or security-conscious environments.

Users will interact with the platform to upload, edit, verify, and manage documents securely.

1.5 Definitions, Acronyms, and Abbreviations

- DMS: Document Management System
- AI: Artificial Intelligence
- Digital Signature: An electronic signature that verifies the authenticity and integrity of a document
- Versioning: System capability to maintain and manage multiple iterations of a document
- Multi-user editing: Ability for multiple users to concurrently edit the same document
- {{PLACEHOLDER}} (other terms as applicable)

1.6 References

The list of reference documents, standards, and technologies used or consulted during the requirements formulation is provided in Section 2.

1.7 Overview

This SRS document is organized according to the ISO/IEC/IEEE 29148:2018 standard. Section 2 lists the applicable references. Section 3 provides an overall description of the system environment and constraints. Section 4 details specific requirements including functional and non-functional aspects. Section 5 discusses verification strategies. Sections 6 and 7 include appendices and an index respectively.

2. References

- ISO/IEC/IEEE 29148:2018 - Systems and software engineering — Life cycle processes — Requirements engineering
- {{PLACEHOLDER}} (Additional relevant standards, protocols, or documents)

3. Overall Description

3.1 Product Perspective

The Document Management System is a standalone, AI-enhanced platform intended to

operate in an enterprise IT environment. It integrates document editing, versioning, secure storage, digital signature verification, and scanning management functionalities.

The system will interface with existing authentication services and hardware scanners {{PLACEHOLDER}}.

3.2 Product Functions

- Allow multiple users to concurrently edit documents.
- Maintain document version history for rollback and auditing.
- Perform document verification via digital signatures.
- Support document scanning imports and management.
- Provide AI-driven features related to document management {{PLACEHOLDER}}.

3.3 User Classes and Characteristics

- Document Editors: Users responsible for creating and editing documents concurrently.
- Approvers/Reviewers: Users who verify and digitally sign documents.
- Administrators: Users managing system configuration, security settings, and user permissions.
- Scanner Operators: Users managing document scanning and import.
- {{PLACEHOLDER}} (Other user roles if applicable)

3.4 Operating Environment

The system will run on {{PLACEHOLDER}}, supporting integration with existing document repositories, authentication/authorization infrastructure, and hardware scanners.

3.5 Design and Implementation Constraints

- Must comply with organizational security policies to ensure highly secure document management.
- Must support AI-driven functionalities using approved AI frameworks {{PLACEHOLDER}}.
- Must support concurrent multi-user editing with data consistency guarantees.
- Must implement digital signature verification following accepted cryptographic standards.
- {{PLACEHOLDER}} (Further constraints)

3.6 Assumptions and Dependencies

- Availability of existing authentication and directory services.
- Availability of digital signature infrastructure compliant with regulations.
- Users have access to document scanning hardware compatible with the system.
- {{PLACEHOLDER}} (Other assumptions or dependencies)

4. Specific Requirements

4.1 Functional Requirements

- FR-1: The system shall allow multiple users to edit the same document concurrently with real-time conflict resolution.
- FR-2: The system shall maintain complete document version history accessible to authorized users.
- FR-3: The system shall provide document verification functionality leveraging digital signatures to authenticate documents.
- FR-4: The system shall support import and management of scanned documents.
- FR-5: The system shall provide AI-driven features to enhance document management operations {{PLACEHOLDER}}.

4.2 System Requirements

- The system shall enforce access control mechanisms to ensure only authorized users can edit or verify documents.
- The system shall use encryption for data at rest and in transit.
- The system shall provide audit logs for document access and modifications.
- {{PLACEHOLDER}} (Additional system-level requirements)

4.3 Interface Requirements

- User Interface: The system shall provide a web-based interface for document editing, version browsing, signature verification, and scan management.
- Hardware Interface: The system shall interface with document scanners supporting {{PLACEHOLDER}} protocols/standards.
- Software Interface: The system shall integrate with authentication systems such as

{{PLACEHOLDER}}.

4.4 Performance Requirements

• The system shall support concurrent editing of documents by up to {{PLACEHOLDER}} users without degradation.

• Document verification via digital signature shall complete within {{PLACEHOLDER}} seconds.

• The system shall maintain document version history with retrieval times not exceeding {{PLACEHOLDER}} seconds per version.

4.5 Logical Database Requirements

• The system shall maintain metadata and version histories for all documents.

• The system shall store digital signatures and verification metadata securely.

• The database shall support scalable storage to accommodate {{PLACEHOLDER}} documents.

4.6 Design Constraints

• The system design must comply with applicable data protection regulations.

• The system shall employ AI models trained on {{PLACEHOLDER}} datasets only.

• The system shall prevent unauthorized access through multi-factor authentication.

• {{PLACEHOLDER}} (Additional constraints)

4.7 Software System Attributes

• Reliability: The system shall have an uptime of {{PLACEHOLDER}} % to ensure availability.

• Availability: The system shall provide failover mechanisms to maintain service continuity.

• Security: The system shall employ end-to-end encryption and comply with {{PLACEHOLDER}} security standards.

• Maintainability: The system design shall support modular updates without system downtime.

• Portability: The system shall be deployable on {{PLACEHOLDER}} platforms.

5. Verification

Verification of requirements will be performed through the following methods:

- Unit and integration testing of multi-user editing, versioning, and signature verification features.
- Security testing including penetration tests and vulnerability assessments to validate high security requirements.
- Performance testing to confirm system responsiveness and concurrency support.
- AI component validation for document management features.
- User acceptance testing (UAT) with designated user groups.
- {{PLACEHOLDER}} (Additional verification methods)

6. Appendix

{{PLACEHOLDER}} (Supporting information, diagrams, or supplemental material)

7. Index

{{PLACEHOLDER}} (Index of key terms and sections)

Placeholder Explanations

- Scope Deployment Context: To properly identify target deployment environments and ecosystems to capture relevant constraints and requirements.
- Additional Stakeholders: To ensure all relevant user groups and stakeholders are accounted for, guiding requirement completeness.
- Other Definitions and Acronyms: Necessary for clarity and shared understanding of domain-specific terms.
- Additional References: To give authoritative backing for standards, protocols, or technologies influencing requirements.
- System Interfaces and Integrations: Precise details on existing systems and protocols are needed for interface design.
- AI Features Detail: Specification of AI capabilities and scope is essential to clarify functional and design requirements for AI-driven features.
- User Roles Expansion: To cover all operational roles interacting with the system for tailored requirements.

• Operating Environment Details: Information about hardware, OS, network, and software environment is essential for compatibility and performance planning.

• Design and Implementation Constraints: Details about technologies, policies, and standards that constrain design need specification to avoid conflicts and ensure compliance.

• Assumptions and Dependencies: Essential to clarify what external factors affect system development and operation, reducing risk of missed conditions.

• System-level Requirements and Security Standards: Needed to enforce compliance with organizational or legal security and data protection requirements.

• Interface Protocols and Authentication Systems: To ensure seamless integration, verification, and system interoperability.

• Performance Metrics: To allow measurable acceptance criteria for system responsiveness and scalability.

• Database Scaling and Capacity: Helps design the data storage solution to meet expected volumes and growth.

• Legal and Data Protection Compliance: To avoid legal liabilities and to align design with mandatory controls.

• AI Training Dataset Constraints: Needed to maintain model quality and compliance within data governance limits.

• Reliability and Availability Targets: Essential to define service levels and validate system robustness.

• Security Standards Reference: Specific standards will guide implementation of cryptographic and access control features.

• Platform Portability: To determine deployment and distribution requirements applicable for the system.

• Additional Verification Methods: To ensure all system facets are validated for compliance and fitness-for-purpose.

• Appendix Content: To provide supplementary material supportive of requirements understanding; diagrams, glossary, or detailed explanations.

• Index Content: A comprehensive index supports document navigation and usability.