Software Requirements Specification (SRS): Modern, Secure, AI Driven Document Management System

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) defines the requirements for a modern, secure, and AI-driven document management system that enables multiple users to edit documents, provides document verification through digital signatures, implements document versioning, and supports document scanning management. This document establishes the basis for subsequent design, implementation, verification, and validation activities.

1.2 Scope

The system and the covered by this SRS comprises software capabilities to: support multiple users editing documents; ensure a highly secure solution; verify documents using digital signatures; implement document versioning; and manage document scanning. The scope is limited to requirements directly supporting these capabilities.

1.3 Intended Audience

{{PLACEHOLDER: Intended audience roles and stakeholders}}

1.4 Intended Use

- Enable multiple users to edit documents.
- Provide a highly secure environment for document management.
- Verify document authenticity and integrity through digital signatures.
- Maintain and retrieve document versions.
- Support document scanning management.
- Provide AI-drriven capabilities applicable to document management tasks.

1.5 Definitions, Acronyms, and Abbreviations

- Document Management System (DMS): A software system for managing digital documents.
- AI-driven: Incorporating artificial intelligence capabilities in support of system functions. {{PLACEHOLDER: Specific AI capabilities}}
- Digital Signature: A cryptographic mechanism for verifying document origin and integrity. {{PLACEHOLDER: Supported digital signature schemes/formats}}

- Versioning: The capability to create, maintain, and retrieve successive states (versions) of a document over time.
- Scanning Management: Capabilities to ingest and manage scanned documents. {{PLACEHOLDER: Supported scan input methods/formats}}
- Multi-user Editing: The capability for more than one user to edit a document, potentially concurrently. {{PLACEHOLDER: Concurrency model and conflict resolution approach}}

1.6 References

See Section 2 for references applicable to this SRS.

1.7 Overview

Section 2 lists references. Section 3 describes the product at a high level. Section 4 specifies functional and non-functional requirements. Section 5 outlines verification approaches. Section 6 provides appendices. Section 7 contains an index. A final section explains placeholders required to complete an ISO/IEC/IEEE 29148:2018-compliant SRS.

2. References

- ISO/IEC/IEEE 29148:2018 — Systems and software engineering — Life cycle processes — Requirements engineering.
- {{PLACEHOLDER: Additional applicable references, if any}}

3. Overall Description

3.1 Product Perspective

The product is a document management system providing multi-user editing, high security, digital signature verification, document versioning, and document scanning management with AI-driven capabilities. {{PLACEHOLDER: System context diagram or description of external systems and integrations}}

3.2 Product Functions

- Enable multiple users to edit documents.
- Provide a highly secure solution for document management.
- Verify documents using digital signatures.
- Implement and manage document versioning.
- Support document scanning management.
- Provide AI-driven capabilities relevant to document management. {{PLACEHOLDER: Enumerated AI-driven functions}}

3.3 User Classes and Characteristics

{{PLACEHOLDER: User classes, roles, and characteristics}}

3.4 Operating Environment

{{PLACEHOLDER: Target operating systems, runtime platforms, and deployment environments}}

3.5 Design and Implementation Constraints

- Security: The system must be highly secure. {{PLACEHOLDER: Specific security constraints and objectives}}
- Digital Signature Support: Verification of digital signatures is required. {{PLACEHOLDER: Signature standards, certificate handling, and trust model}}
- {{PLACEHOLDER: Any additional constraints}}

3.6 Assumptions and Dependencies

- {{PLACEHOLDER: Assumptions about users, data, and operations}}
- {{PLACEHOLDER: External dependencies, if any}}

4. Specific Requirements

4.1 Functional Requirements

- FR-EDIT-001: The system shall support multiple users editing the same document.
- FR-EDIT-002: The system shall provide a method to handle simultaneous edits. {{PLACEHOLDER: Concurrency model and conflict resolution method}}
- FR-VERS-001: The system shall create and maintain versions of documents as they are edited.
- FR-VERS-002: The system shall allow retrieval of prior document versions.
- FR-VERS-003: The system shall associate each version with metadata sufficient to identify its state and history. {{PLACEHOLDER: Required version metadata}}
- FR-SIGN-001: The system shall verify the authenticity and integrity of documents using digital signatures.
- FR-SIGN-002: The system shall present the result of digital signature verification to the user.
- FR-SIGN-003: The system shall maintain the association between a document (or document version) and its digital signature(s). {{PLACEHOLDER: Signature storage approach}}
- FR-SCAN-001: The system shall support document scanning management, including ingestion of scanned documents. {{PLACEHOLDER: Supported scan sources and file formats}}
- FR-AI-001: The system shall provide AI-driven capabilities applicable to document management. {{PLACEHOLDER: Specific AI features and behaviors}}
- FR-SEC-001: The system shall provide mechanisms to achieve a highly secure solution for all document management operations. {{PLACEHOLDER: Security mechanisms and controls}}
- FR-DOC-001: The system shall persist documents and their version histories for subsequent access and editing.

4.2 System Requirements

• SR-CONC-001: The system shall support concurrent editing sessions. {{PLACEHOLDER: Maximum number of concurrent editors per document}}

• SR-SIGN-001: The system shall process digital signatures for verification. {{PLACEHOLDER: Accepted signature formats and certificate sources}}

• SR-SCAN-001: The system shall accept input from scanning management. {{PLACEHOLDER: Input interfaces and ingestion workflows}}

• SR-AI-001: The system shall provide AI capabilities as part of the product functions. {{PLACEHOLDER: AI runtime and model management requirements}}

• SR-SEC-001: The system shall enforce security controls to satisfy the “highly secure” requirement. {{PLACEHOLDER: Security policy and assurance level}}

4.3 Interface Requirements

• IR-UI-001: The system shall provide a user interface for multi-user document editing.

• IR-UI-002: The system shall provide a user interface to view and retrieve document versions.

• IR-UI-003: The system shall provide a user interface to initiate and view the results of digital signature verification.

• IR-UI-004: The system shall provide a user interface for document scanning management. {{PLACEHOLDER: UI workflows for scanning management}}

• IR-API-001: The system shall provide programmatic interfaces to access core functions (editing, versioning, signature verification, scanning management). {{PLACEHOLDER: API protocols and endpoints}}

• IR-EXT-001: The system shall interface with sources of scanned documents. {{PLACEHOLDER: External interface specifications}}

4.4 Performance Requirements

• PR-EDIT-001: Editing operations shall complete within {{PLACEHOLDER: Target latency}} under {{PLACEHOLDER: Load conditions}}.

• PR-SIGN-001: Digital signature verification shall complete within {{PLACEHOLDER: Target time}} for documents up to {{PLACEHOLDER: Document size}}.

• PR-VERS-001: Version creation and retrieval shall complete within {{PLACEHOLDER: Target latency}}.

• PR-SCAN-001: Scanned document ingestion shall process at {{PLACEHOLDER: Throughput}}.

• PR-AI-001: AI feature responses shall complete within {{PLACEHOLDER: Target response time}}.

4.5 Logical Database Requirements

• LDR-ENT-001: The system shall maintain logical entities to represent documents and their versions. {{PLACEHOLDER: Entity attributes}}

• LDR-ENT-002: The system shall maintain associations between documents (and/or versions) and digital signatures. {{PLACEHOLDER: Association model}}

• LDR-ENT-003: The system shall store metadata necessary to support multi-user editing and versioning. {{PLACEHOLDER: Metadata fields}}

• LDR-ENT-004: The system shall store records needed for scanning management. {{PLACEHOLDER: Scanning metadata and indexing}}

• LDR-DATA-001: The system shall define constraints to ensure data integrity across documents, versions, and signatures. {{PLACEHOLDER: Integrity rules}}

4.6 Design Constraints

• DC-SEC-001: The design shall incorporate security to achieve “highly secure” operation. {{PLACEHOLDER: Security design constraints}}

• DC-SIGN-001: The design shall accommodate digital signature verification workflows. {{PLACEHOLDER: Cryptographic dependency constraints}}

• DC-EDIT-001: The design shall support multi-user editing concurrency. {{PLACEHOLDER: Concurrency control constraint}}

• DC-SCAN-001: The design shall support scanning management ingestion and processing. {{PLACEHOLDER: Input constraints}}

• DC-AI-001: The design shall support AI-driven capabilities. {{PLACEHOLDER: AI design constraints}}

4.7 Software System Attributes

• Reliability: {{PLACEHOLDER: Reliability objectives and measures}}

• Availability: {{PLACEHOLDER: Availability targets}}

• Security: The system shall be highly secure. {{PLACEHOLDER: Security objectives, threat model, and controls}}

• Maintainability: {{PLACEHOLDER: Maintainability objectives}}

• Portability: {{PLACEHOLDER: Portability objectives and target platforms}}

• Usability: {{PLACEHOLDER: Usability objectives}}

• Scalability: {{PLACEHOLDER: Scalability objectives}}

5. Verification

• V-EDIT: Verify FR-EDIT-001 and FR-EDIT-002 by test and demonstration under concurrent editing scenarios. {{PLACEHOLDER: Test conditions}}

• V-VERS: Verify FR-VERS-001 and FR-VERS-002 by inspection and test of version creation and retrieval. {{PLACEHOLDER: Acceptance criteria}}

• V-SIGN: Verify FR-SIGN-001 through FR-SIGN-003 by test using documents with valid and invalid signatures. {{PLACEHOLDER: Test datasets}}

• V-SCAN: Verify FR-SCAN-001 by test with sample scanned documents. {{PLACEHOLDER: Test inputs and expected results}}

• V-AI: Verify FR-AI-001 by test and analysis of AI feature outputs. {{PLACEHOLDER: Evaluation metrics}}

• V-SEC: Verify FR-SEC-001 and SR-SEC-001 by analysis, inspection, and security testing. {{PLACEHOLDER: Security verification scope}}

• V-PERF: Verify performance requirements by performance testing. {{PLACEHOLDER: Performance test plan}}

• V-DB: Verify logical database requirements by inspection and test of data constraints. {{PLACEHOLDER: Data validation procedures}}

6. Appendix

• {{PLACEHOLDER: Data dictionary and additional definitions}}

• {{PLACEHOLDER: Document versioning policy}}

• {{PLACEHOLDER: Digital signature handling and operational procedures}}

• {{PLACEHOLDER: Scanning management operational procedures}}

• {{PLACEHOLDER: AI feature description and limitations}}

7. Index

Placeholder Explanations

• Intended audience roles and stakeholders: Needed to tailor requirements to the needs of each stakeholder class, as required by ISO/IEC/IEEE 29148:2018 for clarity of audience.

• Specific AI capabilities: Required to define the AI-driven features explicitly to ensure verifiable and unambiguous requirements.

• Supported digital signature schemes/formats: Necessary to implement and verify signature handling; without this, verification cannot be fully specified or tested.

• Supported scan input methods/formats: Required to define ingestion compatibility for scanning management.

• Concurrency model and conflict resolution approach: Essential to specify how multi-user editing operates (e.g., locking vs. real-time merge) to avoid ambiguity and enable verification.

• Additional applicable references, if any: Required by the standard to cite normative and informative sources that constrain or inform requirements.

• System context diagram or description of external systems and integrations: Needed to

define external interfaces and boundaries per the standard’s product perspective guidance.

• Enumerated AI-driven functions: Needed to scope AI features and define testable behaviors.

• User classes, roles, and characteristics: Required to tailor requirements and interfaces to distinct user groups per the standard.

• Target operating systems, runtime platforms, and deployment environments: Necessary to constrain design and supportability per operating environment requirements.

• Specific security constraints and objectives: Needed to concretize the “highly secure” requirement into actionable, testable constraints.

• Signature standards, certificate handling, and trust model: Required to implement and validate digital signature verification correctly.

• Any additional constraints: Placeholder for constraints such as regulatory, licensing, or tooling that affect design/implementation.

• Assumptions about users, data, and operations: Required to state conditions considered true to avoid misinterpretation and scope creep.

• External dependencies, if any: Needed to identify reliance on external services, devices, or libraries.

• Required version metadata: Needed to ensure retrievability and traceability of versions (e.g., timestamp, editor identity, change note).

• Signature storage approach: Required to specify how signatures are stored/linked to documents or versions.

• Supported scan sources and file formats: Needed to define compatibility and testing scope for scanning management.

• Security mechanisms and controls: Required to translate “highly secure” into implementable and verifiable controls.

• Maximum number of concurrent editors per document: Needed to set performance and capacity expectations for concurrency.

• Accepted signature formats and certificate sources: Needed for interoperability and correct verification.

• Input interfaces and ingestion workflows: Required to define how scanned documents enter the system.

• AI runtime and model management requirements: Needed to specify how AI features are executed and maintained.

• Security policy and assurance level: Required to define the security baseline and verification rigor.

• UI workflows for scanning management: Needed for user interface completeness and usability testing.

• API protocols and endpoints: Required to define integration points and enable interface testing.

• External interface specifications: Needed for interoperability with scanning sources or other systems.

• Target latency, load conditions, time, document size, throughput, response time: Required to make performance requirements measurable and testable.

• Entity attributes, association model, metadata fields, scanning metadata and indexing: Needed to define the logical data model supporting the stated functions.

• Integrity rules: Required to ensure data consistency across documents, versions, and signatures.

• Security design constraints, cryptographic dependency constraints, concurrency control constraint, input constraints, AI design constraints: Needed to guide architecture and design decisions aligned with required capabilities.

• Reliability, availability, security, maintainability, portability, usability, scalability objectives: Required to quantify quality attributes for design trade-offs and verification.

• Test conditions, acceptance criteria, test datasets, test inputs and expected results, evaluation metrics, security verification scope, performance test plan, data validation procedures: Required to plan and execute verification consistent with the standard’s emphasis on testable requirements.

• Data dictionary and additional definitions; document versioning policy; digital signature handling and operational procedures; scanning management operational procedures; AI feature description and limitations: Needed to provide supporting detail that operationalizes requirements and ensures consistent implementation and use.