SOFTWARE REQUIREMENTS SPECIFICATION

Blockchain-based skill credentialing system

NANDINI CHAHAR

23BCE5096

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document provides a complete and detailed description of the requirements for the **Blockchain-Based Skill Credentialing System**. The purpose of this document is to clearly define the system's functionality, constraints, and interfaces so that developers, evaluators, testers, and future maintainers have a common understanding of the system. This document acts as a formal reference throughout the system development lifecycle.

1.2 Document Conventions

This document follows the IEEE Software Requirements Specification standards. The following conventions are used:

- The word **"shall"** indicates a mandatory requirement.
- The word **"should"** indicates a recommended but optional feature.
- All technical terms are defined in the glossary section.
- Diagrams such as use case diagrams and data flow diagrams are used where required for clarity.

1.3 Intended audience and reading suggestions

This document is intended for:

- **Project Developers** – to understand functional and technical requirements
- **Faculty Evaluators** – to assess completeness and feasibility
- **Testers** – to design test cases based on requirements
- **Future Maintainers** – to understand system behavior and constraints

Readers are advised to first read the overall description before proceeding to detailed requirements.

1.4 Project scope

The Blockchain-Based Skill Credentialing System aims to provide a secure, decentralized, and tamper-proof platform for issuing, storing, and verifying vocational skill credentials.

The system replaces traditional paper-based and centralized digital certificates with blockchain-backed digital credentials. Authorized training institutions can issue credentials, learners can store and control their credentials through digital wallets, and employers or regulatory bodies can instantly verify credential authenticity without intermediaries. The system enhances trust, transparency, and portability of vocational certifications.

1.5 Definitions, acronyms and abbreviations

Term	Description
Blockchain	A distributed, immutable digital ledger
Smart Contract	Self-executing contract deployed on blockchain
Credential	Digitally verifiable skill certificate
DID	Decentralized Identifier
NCVET	National Council for Vocational Education and Training
MSDE	Ministry of Skill Development and Entrepreneurship

1.6 References

- IEEE Software Requirements Specification Standard
- Ministry of Skill Development and Entrepreneurship (MSDE)
- National Council for Vocational Education and Training (NCVET)
- Smart India Hackathon Problem Statement

2. Overall description

2.1 Product perspective

The Blockchain-Based Skill Credentialing System is a standalone decentralized application that operates on a blockchain network. It integrates a web-based interface with blockchain infrastructure and smart contracts. The system interacts with multiple external entities such as training institutions, learners, employers, and regulatory authorities.

2.2 Product functions

The major functions of the system include:

- Issuing digital skill credentials by authorized institutions
- Storing credential hashes securely on the blockchain
- Providing learners with lifelong ownership of credentials
- Enabling instant credential verification
- Preventing certificate forgery and duplication
- Maintaining immutable audit logs

2.3 User Classes and Characteristics

User class	Description
Training Institution	Authorized body that issues credentials
Learner	Individual who receives and owns credentials
Employer	Verifies credentials during hiring
Regulator	Audits and oversees credential authenticity
System Administrator	Manages system access and policies

2.4 Operating Environment

- Web browsers (Chrome, Firefox)
- Blockchain network (Ethereum / Hyperledger)
- Backend server (Node.js / Python)
- Smart contracts (Solidity)
- Secure digital wallets

2.5 Design and Implementation Constraints

- Blockchain transaction costs
- Network latency
- Compliance with Indian data protection laws
- Scalability limitations of public blockchains

2.6 Assumptions and Dependencies

- Institutions are verified before issuing credentials
- Users have access to internet-enabled devices
- Blockchain network remains available and operational

3. System Features

3.1 Credential Issuance

Description: Enables authorized institutions to issue blockchain-backed digital credentials.

Functional Requirements:

- The system shall allow only authorized institutions to issue credentials.
- The system shall generate a cryptographic hash for each credential.
- The system shall store the credential hash on the blockchain.
- The system shall associate the credential with a learner's decentralized identity.

3.2 Learner Credential Wallet

Description: Provides learners with a secure digital wallet to store and manage credentials.

Functional Requirements:

- The system shall allow learners to view all issued credentials.
- The system shall allow learners to selectively share credentials.
- The system shall ensure learner ownership and control over credentials.

3.3 Credential Verification

Description: Allows employers and regulators to verify credentials instantly.

Functional Requirements:

- The system shall allow verification without contacting issuing institutions.
- The system shall validate credentials using blockchain records.
- The system shall display verification results clearly.

3.4 Credential Revocation

Description: Supports revocation of invalid or expired credentials.

Functional Requirements:

- The system shall allow institutions to revoke credentials.
- The system shall maintain an immutable revocation log on blockchain.

4. External Interface Requirements

4.1 User Interfaces

- Institution dashboard for credential issuance
- Learner wallet interface
- Employer verification portal

4.2 Hardware Interfaces

User devices such as desktops, laptops, and smartphones

4.3 Software Interfaces

- Blockchain APIs
- Smart contract interfaces
- Wallet SDKs

4.4 Communication Interfaces

- HTTPS protocol
- RESTful APIs
- Blockchain peer-to-peer communication

5. Non-Functional Requirements

5.1 Performance Requirements

- Credential verification response time shall be less than 5 seconds.
- The system shall support multiple concurrent verification requests.

5.2 Security Requirements

- The system shall use public-key cryptography for authentication.
- The system shall ensure data integrity using blockchain immutability.
- The system shall enforce role-based access control.

5.3 Reliability Requirements

- The system shall maintain high availability.
- The system shall recover gracefully from failures.

5.4 Scalability Requirements

- The system shall support a large number of institutions and learners.
- The backend shall support horizontal scaling.

5.5 Legal and Compliance Requirements

- The system shall comply with applicable data protection regulations.
- The system shall align with government credentialing standards.

6. Other Requirements

6.1 Audit and Logging

The system shall maintain logs for credential issuance, verification, and revocation activities.

6.2 Future Enhancements

- Cross-border credential verification
- Integration with government portals
- Advanced analytics for skill tracking