**Software requirements specification [SRS] content**

**1) SRS Overview**

This Software Requirements Specification (SRS) document defines the functional and technical aspects of a decentralized online meeting platform aimed at enhancing security, privacy, and usability. The platform integrates blockchain technology for immutable logging, decentralized storage via IPFS, and blockchain-based role-based access control. Key features include end-to-end encryption, real-time video conferencing powered by WebRTC, and robust user authentication mechanisms. The system is designed to be scalable, user-friendly, and adaptable for diverse industries while ensuring compliance with privacy regulations and data integrity standards.

**2) Purpose**

The purpose of this SRS is to outline the requirements for developing a decentralized online meeting platform that ensures secure, private, and robust communication for stakeholders in institutes, organizations, and government bodies. By leveraging blockchain technology, the platform aims to protect sensitive data, ensure transparency through immutable logging, and enable secure decentralized storage. The document serves as a guide for developers, testers, and stakeholders to align on the system's features, functionality, and architecture.

**3) Scope**

The following software products will be identified and integrated into the decentralized online meeting platform:

* **WebRTC**: Enables real-time video and audio communication between participants, providing low-latency, high-quality conferencing capabilities.
* **IPFS (InterPlanetary File System)**: Facilitates decentralized storage for meeting recordings and shared files, ensuring data integrity and availability across distributed nodes.
* **Blockchain (Ethereum/Hyperledger)**: Ensures secure, immutable logging of meeting activities, implementing role-based access control and decentralized identity verification for participants.
* **End-to-End Encryption (AES-256, TLS)**: Encrypts all communication (video, audio, file transfers) to ensure that meeting data remains confidential and protected from unauthorized access.
* **OAuth/OpenID**: Handles secure user authentication and authorization, integrating with blockchain for secure, tamper-proof identity verification.

The platform will deliver:

* **Decentralized Security and Security**: Leverage blockchain technology for secure, immutable logging of meeting data and actions.
* **End-to-End Encryption**: Ensure all communications, including video, audio, and file sharing, are encrypted in transit and at rest.
* **Role-Based Access Control**: Utilize blockchain-based identity verification for secure authentication and controlled access to resources.
* **Scalable Architecture**: Build a system that is adaptable for varied use cases, including education, healthcare, and business environments.
* **User-Friendly Design**: Provide intuitive interfaces for scheduling, joining meetings, managing settings, and accessing recordings.

**4) Product Perspective**

The decentralized online meeting platform is a standalone system but integrates seamlessly with larger organizational IT ecosystems. It interacts with other related products such as user management systems, blockchain networks, and video conferencing tools, forming a cohesive and secure collaboration environment.

**4.1) System Interfaces**

* APIs for interaction with blockchain, IPFS, and external identity providers.
* Data exchange through REST/GraphQL APIs, ensuring secure and efficient communication.

**4.2) User Interfaces**

* Web and mobile applications with intuitive designs, accessible through browsers and native apps.

**4.3) Hardware Interfaces**

* Requires devices with a camera, microphone, and stable internet connectivity.

**4.4) Software Interfaces**

* Interacts with WebRTC, IPFS, blockchain SDKs, and authentication frameworks like OAuth/OpenID.

**4.5) Communication Interfaces**

* Secure communication protocols (e.g., HTTPS, TLS) for data transmission.
* Peer-to-peer communication for video and audio streaming via WebRTC.

**4.6) Memory**

* Minimal local storage, leveraging cloud and decentralized networks for scalability.

**4.7) Operations**

* Real-time meeting setup, scheduling, and logging.
* Blockchain ensures tamper-proof logs and secure operations.

**4.8) Site Adaptation Requirements**

* Adaptable to organizational environments with minor configuration for branding, user roles, and compliance needs.

**5) Product Functions**

The decentralized online meeting platform will perform the following major functions:

* **User Management**: User registration, authentication, and role-based access control using blockchain-based identity verification.
* **Meeting Scheduling and Management**: Schedule, start, and manage online meetings with role-based participation and access rights.
* **Real-Time Communication**: Enable high-quality video, audio, and text-based interactions using WebRTC.
* **File Sharing**: Allow secure, encrypted sharing of documents during meetings.
* **Immutable Logging**: Use blockchain to maintain a tamper-proof record of meeting actions and events.
* **Meeting Recordings**: Store recordings and files on decentralized storage systems like IPFS for secure, scalable access.
* **Security and Privacy**: Provide end-to-end encryption for communication and ensure compliance with privacy regulations.
* **User Interface**: Intuitive web and mobile interfaces for managing settings, accessing recordings, and participating in meetings.
* **Notifications and Alerts**: Send reminders and updates for scheduled meetings and changes.

**6) User Characteristics**

The platform targets the following user groups with varying levels of technical expertise:

* **Administrative Users**: System administrators, IT staff.
* **Organizational Users**: Faculty, managers, professionals.
* **General Participants**: Students, employees, stakeholders.
* **Users with Disabilities**: Any user requiring accessibility features.

**7) Limitations**

* **Scalability**:
  + While the system is designed to be scalable, increased blockchain transaction volume and IPFS storage usage may lead to higher latency and costs.
  + Hosting a large number of concurrent users may require significant infrastructure scaling.
* **Internet Availability**:
  + The platform requires stable, high-speed internet for seamless video conferencing and real-time communication. Users in regions with poor connectivity may face disruptions.
* **IPFS Storage Costs**:
  + Decentralized storage via IPFS, while secure, can incur additional costs as storage requirements grow due to meeting recordings and file sharing.
* **Blockchain Transaction Latency**:
  + Blockchain operations, such as logging actions or verifying identities, may introduce delays due to network congestion or transaction confirmation times.
* **Resource Constraints**:
  + Devices with low processing power or outdated hardware may struggle to handle WebRTC-based real-time communication and blockchain operations effectively.

**8) Assumptions and Dependencies**

1. **Platform Availability**: Assumes access to blockchain networks, IPFS, and WebRTC-compatible devices.
2. **Third-Party Integrations**: Dependence on stable APIs for OAuth and decentralized storage.
3. **Infrastructure**: Availability of reliable internet and cloud services for seamless operations.
4. **Regulatory Stability**: Assumes no major changes in compliance requirements like GDPR or HIPAA.
5. **User Expertise**: Assumes users have basic familiarity with online meeting tools and devices.
6. **Device Compatibility**: Assumes hardware capabilities to support video conferencing and encryption mechanisms.

**9) Apportioning of Requirements**

The major requirements are allocated to the following software elements:

|  |  |
| --- | --- |
| **Requirement** | **Software Element** |
| User Authentication | Blockchain, OAuth |
| Real-Time Communication | WebRTC |
| Decentralized Storage | IPFS |
| Meeting Scheduling & Management | Backend APIs, Database |
| Role-Based Access Control | Blockchain, Middleware |
| End-to-End Encryption | WebRTC, Encryption Libraries |
| Logging and Auditing | Blockchain, Backend APIs |
| User Interface | Frontend (Web and Mobile Apps) |

**10) Specified Requirements**

**Functional Requirements**:

1. Authenticate users with OAuth and blockchain; output access tokens.
2. Schedule/manage meetings and store details in the database.
3. Enable real-time communication with WebRTC and support encrypted streams.
4. Allow file sharing via IPFS with secure access.

**Cross-References**: OAuth for authentication, IPFS for storage, WebRTC for communication.

Each requirement is uniquely identifiable and traceable.