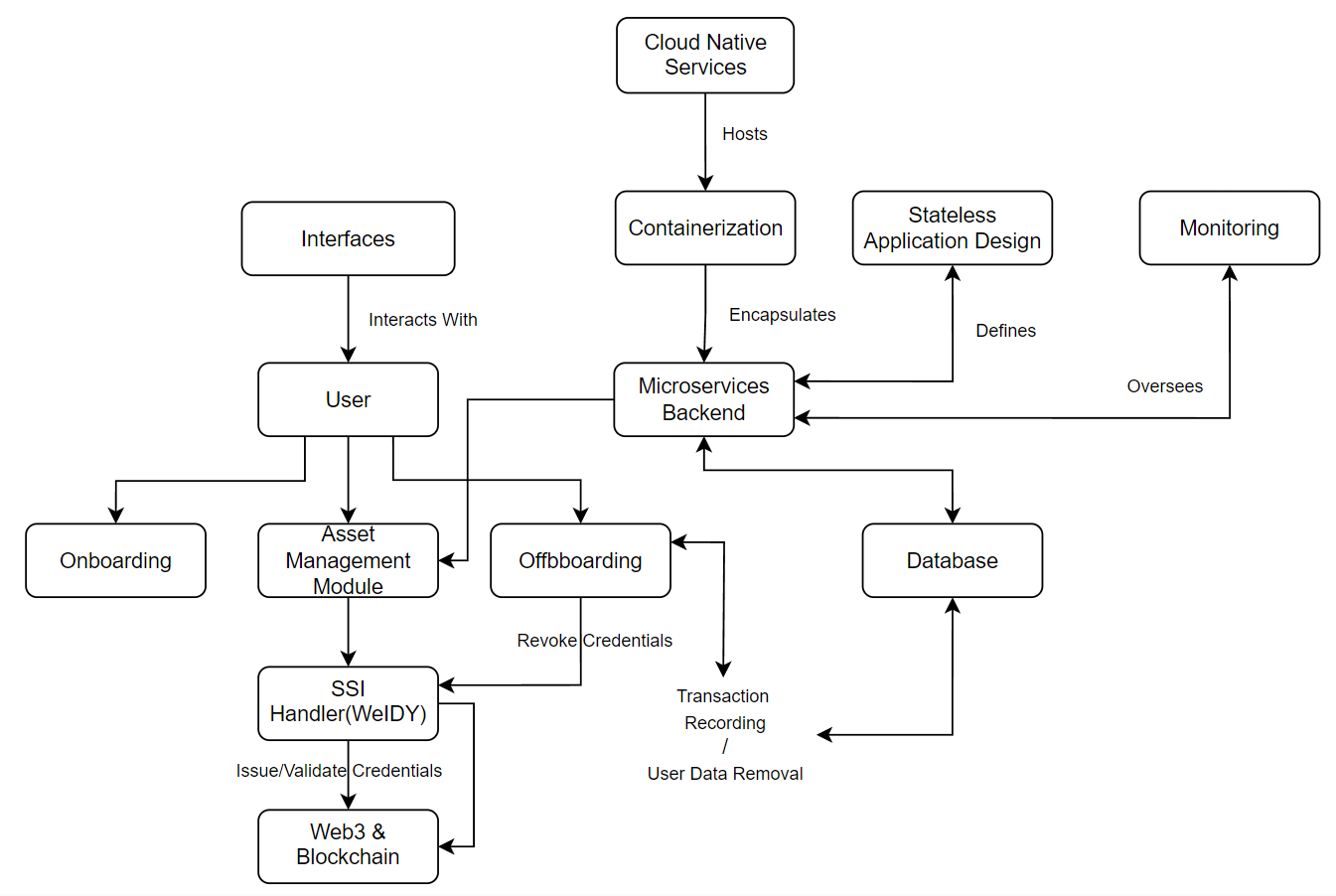
MTCT Web3 SSI System Technical Specification

**Overview**

The MTCT Web3 SSI system focuses on Web3 SSI-based customer onboarding, utilising verifiable credentials for asset management, and is designed for both on-premise and cloud-native deployment. As given in the below diagram.



**Layered Architecture**

Presentation Layer: Web interface, mobile applications.

Application Layer: API endpoints, business logic.

Integration Layer: Middleware for integrating SSI, WeIDY, other Web3 functionalities.

Data Layer: On-premise DB, cloud DB, data warehouses.

**Components and Services**

Web Browser: The primary interface for users to access the MTCT platform.

Load Balancer: Distributes incoming traffic across multiple instances to ensure optimal resource utilisation.

Express Server: Serves APIs and acts as the middleman between the frontend and backend.

SSI Handler (WeIDY):

Onboards users via verifiable credentials.

Integrates with Aries, Indy, etc.

Validates & issues verifiable credentials.

Provides the capability to prove, revoke, and verify credentials.

Web3 & Blockchain: Connects with Ethereum blockchain or other supported blockchain networks for smart contract deployments and interactions.

Asset Management Module: Handles CRUD operations for products, transaction recording, product ownership, and transfer.

Database: A hybrid architecture with both on-premise and cloud DBs. Ensures regular sync or real-time data replication between databases and sharding for scalability.

Microservices Backend: Supports the asset management module and other functionalities.

Interfaces: Various user interfaces to interact with the system.

Containerization: Encapsulates the micro-services backend for isolated deployments and scaling.

Cloud-native Services: Hosts the containerized applications on platforms like AWS, Azure, or GCP.

Stateless Application Design: Ensures easy scalability of the system.

Centralised Logging: Tools like ELK Stack for monitoring and logging system activities.

Monitoring: Tools like Prometheus and Grafana for system health checks and alerts.

**Rationale**

**Web3 Integration**: Provides a decentralised approach to identity management, ensuring security and privacy.

**SSI Handler (WeIDY)**: Enables a trustable and secure transactional environment using verifiable credentials.

**Asset Management Module**: Ensures seamless management of assets with the added security of verifiable credentials.

**Database Design**: The hybrid architecture ensures data availability, redundancy, and scalability.

**Microservices Architecture**: Provides flexibility, scalability, and ease of maintenance.

**Containerization & Cloud-native Services**: Ensures efficient resource utilisation, scalability, and high availability.

**Stateless Design**: Enhances the system's scalability by ensuring that each request from a client to a server is treated as a new request.

**Centralised Logging & Monitoring**: Provides insights into system performance, potential issues, and ensures system health.

**Best Practices**

**Security & Compliance**

End-to-end Encryption: Ensures data security at rest and in transit.

Role-based Access Control: Manages application access.

Web3 Wallet Integration: Allows users to interact with the blockchain.

Regular Audits & Penetration Testing: Identifies and fixes vulnerabilities.

**Backup & Disaster Recovery**

Periodic Data Backups: Ensures data safety.

Redundancy: Provides infrastructure redundancy.

Failover Mechanisms: Ensures system availability during failures.

**Scalability**

Stateless Application Design: Ensures easy scalability.

Load Balancers: Distributes traffic across multiple instances.

Data Partitioning: Manages data efficiently at scale.

**Implementation Flow**

1. A user accesses the MTCT platform.
2. For onboarding, they're directed to WeIDY, where they create/submit their SSI credentials.
3. WeIDY interacts with Web3 to validate and store these credentials on the blockchain.
4. Post-validation, the user is granted access to the MTCT platform.
5. For asset management, verifiable credentials ensure a trustable and secure transactional environment.
6. On offboarding, the user's SSI credentials can be revoked or retained for future interactions.