



ANASTASIA LABS

Technical Specifications for Each Component

Version 1.4 – October 2024

Contents

1. Bridging Contract	1
2. Mithril Integration Module	1
3. User Interface (Optional Component)	1
4. Security Modules	1

Technical Specifications for Each Component

1. Bridging Contract

- Language: Plutus (Haskell)
- Features:
 - Asset Locking Mechanism: Securely lock assets on Cardano.
 - Minting and Burning Functions: Manage token representation of assets.
 - Mithril Signature Verification: Validate certificates for transaction inclusion.
- Interfaces:
 - User Interaction: Functions callable by users to initiate transfers.
 - Mithril Integration: APIs to interact with Mithril aggregators and signers.
- Security Considerations:
 - Input validation to prevent malicious data.
 - Safe handling of UTXOs and prevention of double-spending.

2. Mithril Integration Module

- Purpose: Facilitate communication between the bridging contract and Mithril protocol components.
- Components:
 - Certificate Request Handler: Automates requests for transaction certificates.
 - Metadata Request Handler: Automates requests for transaction metadata.
 - Verification Engine: Validates Mithril certificate and metadata

3. User Interface (Optional Component)

- Type: Web-based Decentralized Application (DApp)
- Technologies: React.js, Web3.js (or equivalent libraries compatible with Cardano)
- Features:
 - Wallet integration for transaction signing.
 - Real-time status updates on bridging transactions.
 - User-friendly forms for inputting transaction details.

4. Security Modules

- Audit Logging:
 - Comprehensive logging of all transactions and certificate verifications.

- Secure storage of logs for auditing purposes.
- Encryption and Secure Communication:

Use of TLS/SSL for all communications between nodes and modules.

- Secure key management practices for handling private keys.