M5Dex Wallet Requirements Specification

1. Product Overview

M5Dex Wallet is a groundbreaking Web3 hardware wallet system that combines a three-card sharding architecture with MPC and Shamir's Secret Sharing (SSS) technology. Each package includes three smart security cards the size of standard bank cards, delivering a revolutionary balance between security and usability through innovative key sharding and joint signing mechanisms.

Core value proposition:

- ☑ Single-card operation: Daily transfers require just one card and NFC pairing via the mobile app
- ☑ Dual-card recovery: If either card is lost or damaged, you can safely restore your wallet using the remaining two cards
- ☑ Physical Security: Card-grade CC EAL5+ security chip, portable design, anti-counterfeiting and anti-side-channel attacks
- ☑ Seamless Experience: Say goodbye to mnemonics with NFC 'tap-to-sign'

product orientation：

M5Dex Wallet is not just an asset management system, but also a gateway for users to explore the Web3 ecosystem, resolving the security-convenience paradox of traditional wallets through hardware innovation.

2. Problem Statement

2.1 Safety Issues

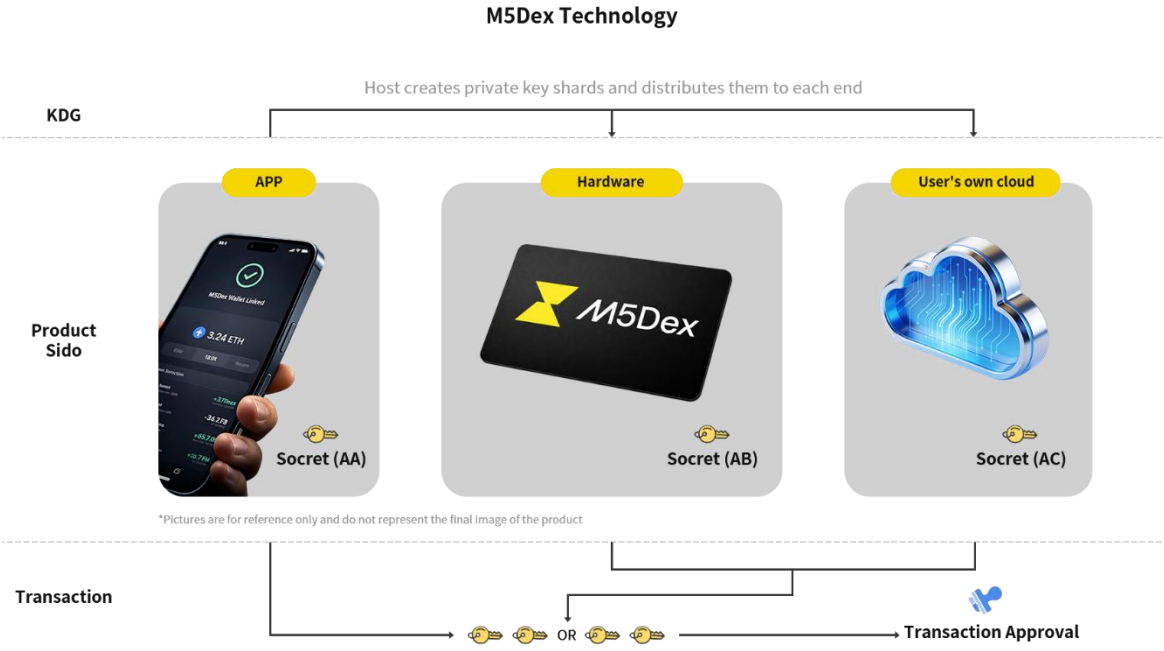
- Single point of failure in mnemonic words: Traditional mnemonic schemes have a risk of single point of failure. If lost or leaked, assets cannot be recovered.
- Physical device loss risk: Permanent asset loss due to hardware wallet loss
- Network Attack Vulnerability: Software Wallet Vulnerable to Phishing and Malware Attacks
- Insecure signature: Traditional wallets have security vulnerabilities during the signing process

2.2 Practical Issues

- High usage threshold: Users need in-depth Web3 knowledge to effectively use the wallet
- Difficult to manage mnemonic phrases: Users need special methods to store them, making them harder to use
- Complex cross-chain interactions: The cumbersome process of cross-platform communication between different blockchains leads to a poor user experience.
- Inconvenient to carry: Traditional hardware wallets require separate carrying, increasing the burden of use

3. Solutions

3.1 Core Technology Architecture



Integration of MPC and SSS technologies:

- Doubly prevent single point of failure: By storing private keys in three different devices, eliminate the risk of single point of failure.
- No mnemonic required: Users don't need to remember or keep mnemonics, making the experience more natural
- Secure transmission: Uses fully homomorphic encryption to ensure secure data transfer

3.2 Product Features

Function	Superiority	Compared with traditional solutions
MPC private key management	Prevent single point of failure and improve security	Better than traditional mnemonic scheme
amnesia for word operations	Lower user barriers	Better than traditional wallets
three-card sharding architecture	Rebuild the wallet with any two cards	Superior to single-device hardware wallets
NFC contactless interaction	Tap to sign	Superior to USB/Bluetooth connection solutions
cross-chain support	Supports multiple blockchains with good scalability	Superior to a single blockchain wallet

4. Product Specifications

4.1 Product Portfolio

M5Dex Wallet product line:

- **M5Dex Wallet App: iOS and Android versions support over 2,300 cryptocurrencies**
- M5Dex Cold Wallet Card: A hardware wallet containing 3 bank-sized security cards per set, packaged in a gift box.

4.2 Technical Specifications

Class	**Specification parameters**
Key scheme	(2,3) SSS threshold + MPC joint signature protocol
Hardware card	Key Sharding Scheme: (2,3) Shamir's Secret Sharing Threshold Scheme Physical form: dimensions 85.6×53.98×0.76 mm; operating temperature range-25℃ to 70℃; erase/write cycle life ≥100,000 cycles Communication method: NFC Type A/B (ISO/IEC 14443), encrypted channel for signature transmission Security chip: CC EAL5+ security chip

NFC communication	Distance ≤4 cm; Encryption protocol: AES-256-GCM; Authentication speed <800ms
Recovery mechanism	Rebuild with dual SIM in <1 minute; supports exporting mnemonic backup (optional)
Compatibility	Supports iPhone RX+/Android 10.0+ (NFC-enabled models)

4.3 User Experience Specifications

User type	Requirement	Size of product
Web3 beginner	Low threshold, high usability	No mnemonics, intuitive interface, built-in tutorials
asset security requirement user	High security, hacker-proof	MPC technology, AI risk control, hardware signature
Multi-chain user	Convenient cross-chain interaction	Supports multiple blockchains with a unified interface
Professional users	Advanced Functional Requirements	API interfaces, customized services, and complete data views
Daily users	Convenient payment experience	Touch payment with single-card NFC completes transactions in 1 second

5. Competitive Analysis

5.1 A Comprehensive Comparison of Major Wallet Solutions in the Market

Contrast dimension	M5Dex three-card hardware wallet	Ledger/Trezor	MetaMask	MPC software solution	exchange custody wallet
private key storage method	Three-card physical partitioning (2,3) SSS threshold	Full private key for a single device	Device local storage	Cloud/Multi-device Sharding	third party full control
single point of failure risk	Zero risk (1 card lost, recoverable)	High risk (device loss = asset loss)	High risk (phone lost/infected)	Medium risk (shards may leak collectively)	platform-dependent
Ease of daily operations	1 card + NFC (1 second)	Connect USB/Bluetooth + and confirm	One-click signature (high risk)	Multi-device collaboration (requires network)	Minimalist (but not self-hosted)
disaster recovery capability	Dual SIM Rebuild (<1 minute, no Mnemonics)	Back up with a mnemonic (easy to lose or remember incorrectly)	Use Mnemonics/Cloud Backup	Restore process depends on email verification	Depends on customer service (days)

physical portability	Bank card size (fits in a regular wallet)	Special equipment (to be carried separately)	No hardware	No hardware	No hardware
Offline security	Offline signature for the entire process (NFC only sends commands)	Offline signature	High risk of online environment	network dependent communication	Fully online
loss-proof design	active disaster recovery (loss of data scenario considered in design)	passive protection	No protection	Partial protection	No user control
user learning cost	Very low (touch to use)	Medium (requires hardware operation understanding)	Low (but high safety awareness required)	Medium (understand MPC concept)	Very low (but not autonomous)

5.2 Key Scene Depth Comparison

Scenario 1: User lost wallet device

Scheme	Restore process	M5Dex superiority
Traditional hardware wallet	1. Find paper mnemonics 2. Purchase new equipment 3. Manual input of 24 words	☑ No Mnemonics Required ☑ Rebuild in 1 minute with 2 remaining cards ☑ Auto-expire of old cards to prevent duplicate risks
Digital Wallet	1. Use backup files or mnemonics 2. Reinstall the app and import	☑ No risk of digital backup leakage ☑ Physical isolation and sharding enhance security
Exchange Wallet	1. Contact customer service 2. Submit identification 3. Wait for review (3-7 days)	☑ User autonomy ☑ No third-party involvement

Scenario 2: Daily small payments

Scheme	Operating steps	M5Dex superiority

Traditional hardware wallet	1. Remove the device 2. Connect to the computer via USB 3. Confirm the transaction on the screen	☑ Card in Wallet, Always with You ☑ Pay with Phone Touch ☑ No Screen, No Confirmation Frustration
Mobile wallet app	1. Unlock your phone 2. Open the App 3. Confirm the signature	☑ Private keys never connect to the internet ☑ Offline signing protects against network attacks