VKX Wallet Security Architecture v1.0

Technical Specification

Date: February 6, 2026
Subject: Incremental Security Layer, Hybrid Signing, and Post-Quantum Readiness
Version: 1.0
Status: Implementation Complete / Public Record

---

1. Introdução

Este documento detalha a arquitetura de segurança da VKX Wallet, uma carteira não-custodial multichain desenvolvida pela VKx Tech. O objetivo é descrever a implementação de uma camada de segurança incremental que introduz prontidão pós-quântica (Post-Quantum Readiness) e integridade de dispositivo sem alterar os protocolos fundamentais das blockchains suportadas ou o fluxo padrão de derivação de chaves via BIP-39.

2. Arquitetura Geral da Wallet

A VKX Wallet opera sob o padrão de autocustódia, onde a frase mnemônica (Seed Phrase) é armazenada localmente e criptografada. A arquitetura é dividida em três pilares:

1. **Core Layer:** Manipulação de chaves BIP-32/BIP-44, assinatura ECDSA/Ed25419 nativa.
2. **Security Layer (Orchestrator):** Gerenciamento de PIN, biometria e integridade de runtime.
3. **Post-Quantum Readiness Layer:** Geração e gestão de chaves assemétricas baseadas em algoritmos resistentes a computação quântica.

3. Security Layer

A camada de segurança atua como um middleware entre a interface do usuário e as funções de execução de transação. Ela é responsável por:

- Validação de estado de desbloqueio (PIN/Biometria).
- Monitoramento de integridade do sistema operacional.
- Orquestração do processo de assinatura híbrida.

4. Post-Quantum Readiness Layer

Diferente das wallets tradicionais que dependem exclusivamente de curvas elípticas (secp256k1 e ed25519), a VKX implementa chaves secundárias baseadas em algoritmos Lattice-based.

- **Algoritmo Utilizado:** ML-DSA-65 (conhecido como Dilithium3), selecionado pelo NIST para padronização pós-quântica.
- **Geração de Chave:** Realizada localmente no dispositivo. A chave privada pós-quântica (PQ-SK) é gerada de forma independente ou derivada deterministicamente de uma semente segura.
- **PQ-PK (Public Key):** Registrada opcionalmente no servidor de backend para verificação de provas de autenticidade.

5. Assinatura Híbrida

O modelo de assinatura da VKX é "Híbrido Off-Chain".

- **Processo:** Ao aprovar uma transação, o dispositivo gera a assinatura ECDSA/Ed25419 necessária para a blockchain e, simultaneamente, gera uma assinatura ML-DSA da carga útil da transação (TX Payload).
- **Resultado:** Um objeto `HybridSignatureProof` contendo o hash da transação, a assinatura quântica e o ID do dispositivo.
- **Objetivo:** Estabelecer um rastro de auditoria que prova que a transação foi originada por um dispositivo de alta integridade usando criptografia resistente a ataques futuros.

6. Device Integrity Model

Sistema de pontuação de integridade (Integrity Score) que avalia:

- **Runtime Environment:** Presença de Debuggers, Emuladores ou Hooks de interceptação.
- **Platform Status:** Verificação de Root (Android) ou Jailbreak (iOS).
- **Storage Integrity:** Disponibilidade de Secure Enclave / TEE (Trusted Execution Environment).
  Atividades críticas e recursos do Quantum Shield são bloqueados se o score de integridade for inferior ao limite de segurança definido.

7. Quantum Shield (Premium Security Layer)

O Quantum Shield é uma camada de serviço por assinatura que habilita recursos avançados:

- **Gating de Integridade:** Bloqueio mandatório de transações em dispositivos comprometidos.
- **Proof Registry:** Armazenamento persistente de assinaturas híbridas no ProofVault da VKX.
- **Backup Gerenciado:** Habilita a exportação criptografada da chave pós-quântica.

8. Proof Registry Model

As assinaturas geradas pela camada de prontidão quântica são registradas no **VKX Proof Registry**.

- **Local:** Cache seguro no dispositivo para acesso offline.
- **Cloud (Premium):** Sincronização com o backend para preservação histórica, permitindo que o usuário comprove a autoria de suas transações mesmo após trocar de dispositivo.

9. Secure Storage Strategy

O armazenamento de chaves segue uma política de isolamento:

- **Chaves Privadas (Nativas):** Armazenadas via Keystore/Keychain com criptografia AES-256GCM.
- **Chaves Pós-Quânticas:** Armazenadas em slots separados no Secure Storage, protegidas por entropia adicional derivada do PIN do dispositivo.

10. Segurança e Limitações

- **Não-Custodial:** A camada de segurança não dá à VKx Tech acesso aos fundos do usuário.
- **Independência da Rede:** A assinatura quântica é incremental e off-chain; não depende de suporte nativo das blockchains atuais.
- **Limitação:** A proteção quântica aplica-se à integridade da transação e prova de autoria, não impedindo ataques de engenharia social (phishing).

11. Conclusão

A arquitetura v1.0 da VKX Wallet estabelece um novo paradigma para wallets mobile, movendo-se além da segurança criptográfica básica para um modelo de defesa em profundidade, preparando a base de usuários para a transição para padrões criptográficos pós-quânticos.

VKx Tech Engineering