## Enno Wallet iOS Mobile App Threat Model v1.0

## Internet Waves Blockchain Mobile Phone (PIN or Biometrics - Authenticated) C05 TA05 -TA06 -TA07 TA01 Enno Wallet (PIN or Biometrics - Authenticated) A05 User Stake C05 C04 C02 C02 Login / Wallet/Dapp € C04 A05 Onboarding 3rd Party Services C03 TA02 **Fransactions** Cloud Provider C06 C02 C03 C06 TA02 C04 A02 A04 Authorization A03 Waves Blockchain TA02 C03 C04 C03 A05 TA04 **API** Server TA02 Defo A06 C07 C01 TA03 TA04 C04 Mobile/Storage (Rest/ricted) OS Keychain (Encrypted) A05 Waves Matcher C03 C01 TA02 TA02 Swap / Swop C03 TA04 Database C02 C07 A02 A01 A05 User Data RAM Secret Keys A05 A05 C02 C06 TA02 C03 C06 Ticker Server C05 Enno Cash Binance Ticker (Web Socket) C07 Security Controls Assets **Threat Agents** A01 - Account Seeds (Private Key) - Data Encryption Malicious App Users - Integrity Check - User Email Address TA02 **Network Attackers** - User Generated PIN - TLS/Certificate Verification Malicious Employees TA03 - Account Public Data - Certificate Pinning Malicious Cloud/Server Provider TA04 - Public Blockchain Data - Pin or Biometrics (Mobile Phone) TA05 Malicious Apps (Sandboxed) A06 - Device Data (Brand/Model/ID) - Pin or Biometrics (Enno Wallet App) Malicious Apps (Root Priv.) TA06 C07 - Commands/Server Logging/Monitoring User w/ physical access to device