Privacy and Security is matter
Trust is like the air we breathe--when it's present, nobody really notices; when it's absent, everybody notices.

— Warren Buffett —
How to build the Trust?
Rebuilding trust, one phone at a time – **EXODUS**

Security Architected enclave secure your keys -- **Zion**
LET MY DATA GO

Rebuilding the Internet: We believe we can rebuild the Internet together by empowering the people to own their own identities, personal data and assets.

Own Your Own Keys
Why have someone else hold your keys when you have the Zion private vault.

Security Architected
The same military-grade cryptographic scheme that protects your assets.

Key Management API/Vault SDK
Extending the security from the vault to web 3.0 DApps.
Features

**Zion Vault**
When activating your Zion, both 12-word recovery phrase and signing transaction will be operate in trusted execution environment (TEE). It is an isolated area that runs free from malware.

**All-in-one Private Vault**
View your BTC, LTC, ETH and other popular ERC-20 tokens and ERC-721* on Zion. Manage your crypto asset is simple!

**Social Key Recovery (SKR)**
Zion breaks, encrypts and shares your recovery phrase to your trusted contacts. They can help you recover your key when your phone is lost.

**Own your own keys**
Keep your own key in the Trusted Execution Environment. No login required. Zion won’t collect your personal data.

**SDK API**
Provide Zion service, API, Exchange service and SKR API. 3rd party integrate who care more security.

**Zion Trusted UI**
Provide a Trusted UI (include Secure Display and Secure Touch event) to avoid monitor by hacker or tamper when using popular application such as payment, bank account transaction, privacy information for KYC, or your Wallet.
Zion Trusted UI
Zion SDK
Curve list:
- ECDSA signing/verifying (supports secp256k1 and nist256p1 curves, uses RFC6979 for deterministic signatures)
- ECDSA public key derivation
- Ed25519 signing/verifying (also SHA3 and Keccak variants)
- Chacha20-Poly1305

Hash:
- AES/Rijndael encryption/decryption
- Big Number (256 bit) Arithmetics
- BIP32 Hierarchical Deterministic Wallets
- BIP39 Mnemonic code
- Base32 (RFC4648 and custom alphabets)
- Base58 address representation
- ECDH using secp256k1, nist256p1 and Curve25519
- HMAC-SHA256
- HMAC-SHA512
- PBKDF2
- RIPEMD-160
- SHA1
- SHA2-256/SHA2-512
- SHA3/Keccak
- BLAKE2s/BLAKE2b
Open source to be the trustworthy thing
Gathering energy of research in the world to construct trustworthy thing

-- HTC Exodus
Open Source

Zion
htczion

hTC, Inc
Taiwan

Block or report user

Overview | Repositories 4 | Projects 0 | Stars 3 | Followers 17 | Following 0

Popular repositories

**ZKMS**
Zion Key Management Service
- Java
- ★ 16
- ☆ 3

**ZKMA**
Zion Key Management Api
- Java
- ★ 12
- ☆ 1

**ZionVaultSDK**
Integration guide for the cryptocurrency exchange service provider
- ★ 10

**Zion-SKR-SDK**
SDK for social seed recovery
- ★ 2
- ☆ 1

76 contributions in the last year

[https://github.com/htczion](https://github.com/htczion)
Bug Bounty Program

Coming soon 2019  HTC EXODUS bounty

https://www.htcexodus.com
Future Plan

- Full node on Exodus
- More chain/token support on line.
- SKR2.0 next generation
- Embedded secure element (possible with RISC-V?)
Here we are!!

Contact Us

exodus@htc.com
@htcexodus
www.facebook.com/htcexodus