

trust wallet app security review

prepared for SIX DAYS LLC

prepared by Viktor Miroshnikov [iOS] , Sergei Buterin [Android]



Turning our expertise into your profit

Stateful sp. z o.o.

Company reg no: 0000456299

Ksawerow 3,

Warsaw, Poland

hi@stateful.eu

USA: +1 (415) 870 66 99

EU: +48 532 070 757

Executive Summary

Six Days LLC engaged Stateful sp. z o.o. to analyze Trust cryptocurrency wallet applications for Android and iOS during October and December, 2017.

Stateful performed a comprehensive review of architecture and codebase and tested both Android and iOS applications. The review focused on code quality and security of handling sensitive data such as private keys along with a set of recommendation inline with current best practices.

Stateful made and Six Days LLC implemented several recommendations regarding encryption of private keys at rest and in transit, secret key generation and key derivation, private key backup and recovery, handling of sensitive data in RAM.

Project Goals and Scope

The goal of this engagement was to review the state of security in Trust Wallet Android and iOS Apps. The research team used an adaptation of OWASP Mobile Application Security Verification Standard(MASVS) v.0.9.3 for review. Adapted version excluded

Included areas of OWASP MASVS requirements sections:

- Architecture and design
- Data Storage and Privacy
- Cryptography
- Network Communication
- Environmental Interaction
- Code Quality and Build Settings
- Handling private keys (storage, load, usage)

Explicitly excluded the following areas

- Authentication and Session Management (OWASP MASVS)
- Resiliency Against Reverse Engineering
- External libraries included in project

The review also included used a combination of automated testing tools, code statical analysis, manual test techniques and manual source code review.

Appendix A: App Security Checklist





An excerpt of what has been checked in iOS app.

Checklist: General Security Measures

| Check | Response | OK |
|--|--|----|
| Does application attempt to detect jailbreak? | <ul style="list-style-type: none"> Jailbreak trace checks are performed at every application initialization | ✓ |
| Does application warn user if jailbreak is detected? | <ul style="list-style-type: none"> If jailbreak is detected a warning message is displayed | ✓ |
| Is incoming data is validated and sanitized? | <ul style="list-style-type: none"> No data sanitization found for external API use cases | ✗ |
| Are SSL certificates pinned for TLS connections? | <ul style="list-style-type: none"> No certificate pinning implemented | ✗ |
| Are compile security features enabled? | <ul style="list-style-type: none"> Enabled PIE Enabled fstack-protector-all | ✓ |

Checklist: Ethereum Wallet Private Key Usage and Storage

| Check | Response | OK |
|--|---|----|
| Where private keys are stored while at rest? | <ul style="list-style-type: none"> Every key is: <ul style="list-style-type: none"> stored in application local folder encrypted by Geth only readable if device is unlocked protected with random password | ✓ |
| How can user fetch private keys? | <ul style="list-style-type: none"> Can only be done by using "export keys" feature via application user interface | ✓ |
| Can user restore or backup private keys with iTunes or iCloud backups? | <ul style="list-style-type: none"> File that keeps key data is excluded from iTunes and iCloud backups There is no way to fetch file with keys using conventional tools like iTunes or iFunBox, unless device is jailbroken | ✓ |
| How exported keys are protected? | <ul style="list-style-type: none"> Exported keys are encrypted with user provided password | ✓ |

| Check | Response | OK |
|--|---|---|
| How exported keys are encrypted? | <ul style="list-style-type: none">• Encryption is done with :<ul style="list-style-type: none">• PKBDF2(10,000 iterations)• AES256 in CBC mode with random IV and no padding |  |
| Where Geth wallet passwords are stored? | <ul style="list-style-type: none">• Stored in Keychain with<ul style="list-style-type: none">• disabled backup synchronization• accessible only when device is unlocked |  |
| How are Geth wallet passwords generated? | <ul style="list-style-type: none">• 16 byte cryptographically secure random string is generated using iOS native RandomizationServices |  |
| Does app zero memory where private keys were stored after usage? | <ul style="list-style-type: none">• No memory zeroing in Geth or app itself |  |

Appendix B: Android App Security Checklist

An excerpt of what has been checked in Android app.

Checklist: General Security Measures

| Check | Response | OK |
|--|--|----|
| Does application attempt to detect rooted Android? | <ul style="list-style-type: none"> Rooting trace checks are performed at every application initialization | ✓ |
| Does application warn user if root is detected? | <ul style="list-style-type: none"> If root is detected a warning message is displayed | ✓ |
| Is incoming data is validated and sanitized? | <ul style="list-style-type: none"> No data sanitization found for external API use cases | ✗ |
| Are SSL certificates pinned for TLS connections? | <ul style="list-style-type: none"> No certificate pinning implemented | ✗ |

Checklist: Ethereum Wallet Private Key Usage and Storage

| Check | Response | OK |
|--|---|----|
| Where private keys are stored while at rest? | <ul style="list-style-type: none"> Every key is: <ul style="list-style-type: none"> stored in application local folder encrypted by Geth only readable if device is unlocked protected with random password | ✓ |
| How can user fetch private keys? | <ul style="list-style-type: none"> Can only be done by using "export keys" feature via application user interface | ✓ |
| How exported keys are protected? | <ul style="list-style-type: none"> Exported keys are encrypted with user provided password | ✓ |
| Where Geth wallet passwords are stored? | <ul style="list-style-type: none"> Stored in Android Keystore | ✓ |
| How are Geth wallet passwords generated? | <ul style="list-style-type: none"> UUID 122 bit key from cryptographically secure random generator | ✓ |
| Does app zero memory where private keys were stored after usage? | <ul style="list-style-type: none"> No memory zeroing in Geth or app itself | ✗ |