STATEMENT OF WORK PERFORMED

FIREFLY AND STRONGHOLD

IOTA Foundation

April 28, 2021

F-Secure

1 Introduction

The purpose of this document is to provide a statement of work performed by F-Secure during an assessment of the Firefly wallet application and the Stronghold secret management engine for the IOTA Foundation.

The results of the assessment are to be considered in the context of effort, time and budget spent, and within the context of the threat model and constraints in use during the assessment. Additionally, the listed results apply as a snapshot in time against a particular version of the audited code base, future code changes might introduce vulnerabilities not covered under this assessment. As such, it is possible that certain vulnerabilities have not been identified during the time allocated for the project.

This document does not serve as a certification of the results or the security of the application, and solely as a statement that F-Secure has performed a certain amount of security assessment work for the IOTA Foundation.

2 Scope

Target

The following table identifies the version of the audited codebase.

Target Identifier	Description and Characteristics	Component versions
Firefly	Firefly wallet is an Electron based application implementing the wallet user interface.	branch `develop` [1]
Stronghold	Stronghold is a secret management engine.	branch `dev` [2]

[1] The branch was at commit `1e4f3b67` during the assessment and at commit `ca739570` during the verification test.

[2] The branch crates have been evaluated at commits `65ec786` (snapshot, runtime), `5490f0a` (store) and `1443973` (vault, client) during the assessment.

Assessment Approach

The assessment was conducted based on the parameters described below.

Location	Off-site
Effort	25 days source code review + 3 days verification review
Timespan	February 8, 2021 - April 28, 2021
Target Lifecycle State	Development
Attacker View	Anonymous and trusted user (unauthenticated and authenticated as a regular user)
Methodology	White-box, F-Secure had full insight into all details regarding the target(s) such as source code, etc

Assessment Constraints

The audit has been conducted under the following assumptions:

- Adversary has not compromised the underlying operating system
- Adversary has the same level of privileges as the one using the wallet
- Adversary is not root or does not have administrator rights on the system
- Adversary has not instrumented or modified the binary

Attack scenarios depending on any of the conditions listed above, or a combination of them, have not been covered by this audit.

3 Summary of results

The purpose of this security assessment was to analyse the Firefly wallet application and Stronghold secret management engine developed by the IOTA Foundation and attempt to use it in a way not specified during the design process. The project focused on identifying security vulnerabilities with the goal of establishing the current security level of the audited application.

This report is meant as a statement that this application underwent an assessment by F-Secure and only provides a summary overview of the findings made during the assessment and does not describe full technical details.

A verification test of the findings against the Firefly wallet has been conducted to evaluate the validity of the fixes deployed by IOTA Foundation: this report includes the results of this further testing activity, giving an indication of the efficiency of the implemented mitigations.

As several constraints affected the assessment, directly influencing the results and achieved coverage, F-Secure recommends readers of this report to take the constraints, described in the Assessment Constraints section, into account to ensure a proper understanding of the findings within their context and the overall security level.

Summary of Vulnerabilities

The following table presents all the issues that were identified, ordered by severity and prevalence and their status after the verification test conducted to verify the mitigations deployed by the IOTA Foundation. The status applies to the application version available during the verification tests indicated in the Target section.

Target	Vulnerability Description	Status
Firefly	Wallet PIN leaked on local filesystem	FIXED
Firefly	Wallet PIN not wiped from the Local Storage	FIXED
Firefly	Weak protections against evil node operator	RISK ACCEPTED [3]
Firefly	Isolation of multiple Firefly application users cannot be guaranteed under a single application install	RISK ACCEPTED [3]
Firefly	Insufficient verification of certificate chains	FIX IN PROGRESS [4]
Firefly	Insufficient zeroization of sensitive data	FIXED
Firefly	Outdated PBKDF2 dependency	FIXED
Firefly	Errors not checked on account deletion	FIXED
Firefly	Multiple unhandled error conditions in Firefly UI	FIXED
Firefly	Debugging options enabled in Firefly UI	FIXED
Stronghold	Guarded vector escape for external use of contents	RISK ACCEPTED [5]
Stronghold	Lack of protection for command line arguments	RISK ACCEPTED [5]
Stronghold	Redundant encrypted key storage	INFORMATIONAL[6]
Stronghold	Incomplete memory initialization	INFORMATIONAL[6]
Stronghold	Inconsistent memory caching documentation	INFORMATIONAL[6]

[3] This finding has been addressed but not fixed, the residual risk has been evaluated and accepted by IOTA Foundation.

[4] This fix proposal discussed with IOTA Foundation developers appears to be consistent with the recommendation. Nevertheless, the actual remediation was not deployed yet in the application version that was available during the verification test.

[5] These findings are current limitation already known, and commented, within the code base.

[6] These findings concerns style, documentation, consistency, code quality or abstraction aspects that have no practical impact on security or security vulnerabilities identified on dead code.

F-Secure