Audit of Tangem's Smartcard Wallet Code

Independent Security Audit - Summary of Findings

Client	Tangem
Auditor	Kudelski Security
Date	August 6, 2018
Scope	Smartcard wallet firmware source code (internal logic)
Firmware version	v1.28

Overview

Tangem provides smart banknotes for digital assets - smart card storage media for Bitcoin private keys with basic wallet functionality. Tangem hired Kudelski Security to perform a security audit of the source code written by Tangem to offer these features.

Key Findings

✓ **Security risks identified and mitigated**

A number of security risks were identified during the audit. All identified risks were subsequently mitigated by the Tangem engineering team to the satisfaction of Kudelski Security.

✓ **Adequate defenses confirmed**

The implemented countermeasures provide adequate defenses against counterfeiting and cloning of cards, and against theft of blockchain assets.

✓ **No backdoors or malicious code**

No backdoor, malicious, or suspicious undocumented feature was found in the firmware.

✓ **Firmware integrity verification**

Firmware v1.28 was compiled and a binary fingerprint was stored. This fingerprint can be embedded into users' host (NFC) applications to verify the integrity of the firmware in each banknote.

Scope and Limitations

The audit covered the internal logic of the cards as defined by the source code. Physical attack resistance was not assessed as part of this engagement. The cards include a number of protections against physical attacks, including those provided by EAL6+ certified components.

Note: *The full audit report is not published because it contains numerous references to proprietary information, such as snippets of the firmware source code. This document summarizes the publicly available conclusions.*