Token2

PIN+ FIDO2 Security Keys Series Review

Version:	v1.0
Project Number:	89781
Date of Delivery:	September 9th, 2024

Compass Security Schweiz AG, Werkstrasse 20, CH-8645 Jona
T +41 58 510 36 00, team.csch@compass-security.com, www.compass-security.com

Executive Summary

In August 2024, Compass Security Schweiz AG (Compass) conducted a security review of the Token2 PIN+ FIDO2 Security Keys Series firmware. This document is intended to provide a high-level summary of the assessment results. Further details have been reported to Token2 in a separate document.

Scope

The firmware in scope and its version is listed in the following table:

Target	Git Commit	Effort
The firmware of the PIN+ FIDO2 Security Keys Series was in scope (https://github.com/token2/pin_plus_firmware). The review focused on the following key areas: ▪ Analysis of code related to PIN complexity requirements. ▪ Spot checks of the most important functionality that the security key exposes to the platform (CTAP interface), including PIN configuration/change, credential generation (createCredential), and using credentials (makeCredential). ▪ Spot checks of security relevant implementation details (e.g., key material generation and storage, usage of key material and cryptographic functionality).	8461a9331a9172767ac75d478cc102f8eb53432e	3.00 PD

The statements made in this document are only applicable to the exact firmware version listed above.

Only FIDO2 functionality was in scope. Other features such as TOTP were explicitly taken out of scope. Also, the assessment solely focused on the firmware (i.e., software); the hardware components (e.g., secure elements) were not tested.

Procedures

The firmware of the security key is primarily based on a third-party GitHub project. Token2 have implemented a few modifications, the most significant being stricter PIN policy enforcement. The primary objective of the assessment was to review these modifications, particularly the code where the PIN policy is implemented. In addition, the interface exposed by the security key to the outside world (i.e., the platform) and some security key internals were reviewed. The review was mainly conducted through source code analysis, supplemented by practical tests to verify PIN policy enforcement and PIN verification.

Weakness Rating

Compass classifies findings into four categories: low, medium, high, and critical. The ratings are based on their intrinsic technical properties and are not a risk score. Other factors such as a threat actor's motivation or financial loss incurred by a successful exploitation of a vulnerability have not necessarily been considered.

Results

The analysis of the PIN policy implementation has not revealed any critical or high severity vulnerabilities that would have a significant impact on the security of the security keys. Only a single medium and a low rated issue were found that concern the FIDO2 pin policy compliance. It would be desirable to have the PIN policy allow Unicode characters to not restrict the key space and to ensure proper PIN termination.

The existing source code is highly complex, consisting of low-level Java code. Therefore, the source code review only focused on the most critical code components of the security key, including PIN verification, credential creation, and credential usage for authentication, though it was constrained to a three-day assessment. No security vulnerabilities have been found. In particular, the security key generates and stores credentials (i.e., cryptographic key material) securely. It is ensured that they are never exposed outside the security key.

About

Compass Security Schweiz AG is a Swiss IT security company specializing in providing tailored high-quality attack simulations, security assessments and forensic investigations to customers. Founded in 1999, Compass has over 25 years of experience working on national and international projects with Fortune 500 companies, small and medium-sized companies, as well as with start-ups operating in the financial, medical, industrial, and pharmaceutical industries. The diverse training and specializations of our security analysts, as well as close cooperation with leading Swiss universities, ensure that our analysts are always informed about the latest developments in the security industry.