Trust Through Open Hardware

Open Hardware Authentication with the Tillitis Key

PA4 Project - Team 4303

Eliza.K - Nathan.H - Michael.A - Sofien.E - Aboubakar.B - Paul.A

ESILV DE VINCI ENGINEERING SCHOOL

Problem Statement

- Most hardware security keys are closed-source and non-auditable
- Users cannot verify firmware integrity or device behavior
- Security relies on trust rather than transparency

Objective

- Evaluate the robustness of the key through security analysis
- Identify vulnerabilities and propose strategies to strengthen the security

Benchmark

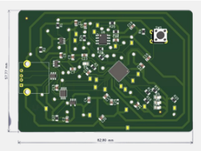
Feature	Tillitis Key	YubiKey 5
Open Hardware	Yes	No
Open Source Firmware	Yes	No
Verifiable Firmware	Yes	No
Cryptographic Operations	Yes	Yes
Hardware Isolation	Yes	Yes
Transparency / Auditability	High	Low
Developer Friendly	High	Medium

Tillitis Key Study

Official TKey

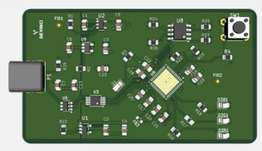
- Reference & Testing
- Benchmarking

Local Prototype



- Learning & PCB Reproduction
- Experimental Build

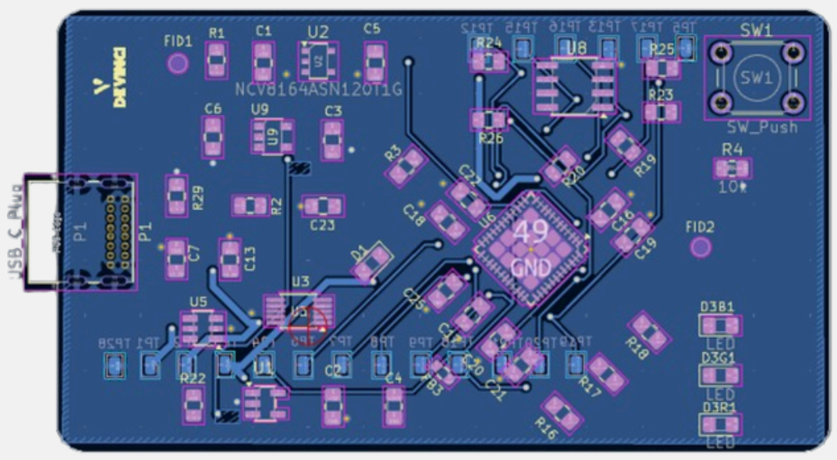
Compact Version



- Smaller Form Factor
- Future Production

Work & Research

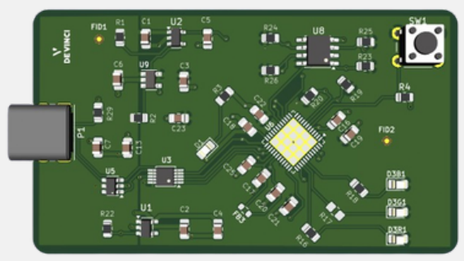
- Studied existing hardware authentication systems
- Tested the pre-built Tillitis Key
- Analyzed and replicated open hardware security models
- Examined the Tillitis Key firmware to configure it in our environment



KiCad project made to build the Tillitis Key

Results Obtained

- Functional authentication prototype implemented using the Tillitis Key
- Successful implementation of hardware-based cryptographic signing
- Verification workflow successfully integrated and tested
- Demonstrated secure authentication using a trusted hardware device



Kicad 3D view of the key

Workflow

User - Authentication Request

↓

Application generates challenge

↓

Challenge Sent to the Tillitis Key

↓

Key signs Challenge using Ed25519 + Private Key (stored in the device)

↓

Signed Response Returned

↓

Application verifies the signature using the public key

↓

Authentication Successful

Conclusion

- Open hardware enhances trust and transparency
- Tillitis Key enables secure cryptographic operations

Futur Perspectives

- Investigate quantum-resistant cryptographic mechanisms to anticipate future threats
- Study human factors and secure usage practices to mitigate risks related to user behavior

Learn More:

GitHub

Security Analysis

- Threat model and attack surface analysis of the authentication workflow