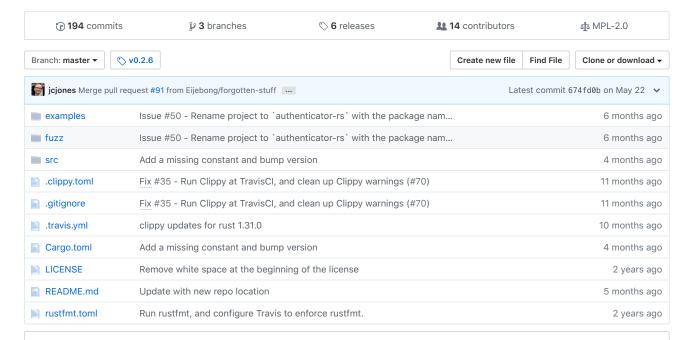
☐ mozilla / authenticator-rs ✓

Rust library to interact with Security Keys, used by Firefox

#u2f #hid #rust



A Rust library for interacting with CTAP1/CTAP2 Security Keys



This is a cross-platform library for interacting with Security Key-type devices via Rust.

- Supported Platforms: Windows, Linux, FreeBSD, and macOS.
- Supported Transports: USB HID.
- Supported Protocols: FIDO U2F over USB. CTAP2 support is forthcoming, with work being done in the unstable ctap2 branch.

This library currently focuses on USB security keys, but is expected to be extended to support additional transports.

Usage

There's only a simple example function that tries to register and sign right now. It uses env_logger for logging, which you configure with the RUST_LOG environment variable:

cargo build --example main
RUST_LOG=debug cargo run --example main

Proper usage should be to call into this library from something else - e.g., Firefox. There are some C headers exposed for the purpose.

Tests

There are some tests of the cross-platform runloop logic and the protocol decoder:

cargo test

1 of 2 28.09.19, 18:20

Fuzzing

There are fuzzers for the USB protocol reader, basically fuzzing inputs from the HID layer. There are not (yet) fuzzers for the C API used by callers (such as Gecko).

To fuzz, you will need cargo-fuzz (the latest version from GitHub) as well as Rust Nightly.

```
rustup install nightly
cargo install --git https://github.com/rust-fuzz/cargo-fuzz/

cargo +nightly fuzz run u2f_read -- -max_len=512
cargo +nightly fuzz run u2f_read_write -- -max_len=512
```

2 of 2