Zcash
FROST UniFFI SDK

A walkthrough

Pacu - Dev Rel Engineer (ZCG Grantee)

pacu@zecdev.org

FROST UniFFI SDK (PoC)

URL: https://github.com/pacu/frost-uniffi-sdk

Goals:

Bring Randomized FROST Rust crates to other languages without porting or rewriting

- Languages:
    - GoLang (infrastructure)
    - Kotlin (JVM and Android)
    - Swift (Apple Platforms like iOS and Mac)

GitHub Repo QR

https://github.com/zecdev/frost-uniffi-sdk

What’s UniFFI?

A multi-language bindings generator for Rust

Expectation

What’s UniFFI?

A multi-language bindings generator for Rust

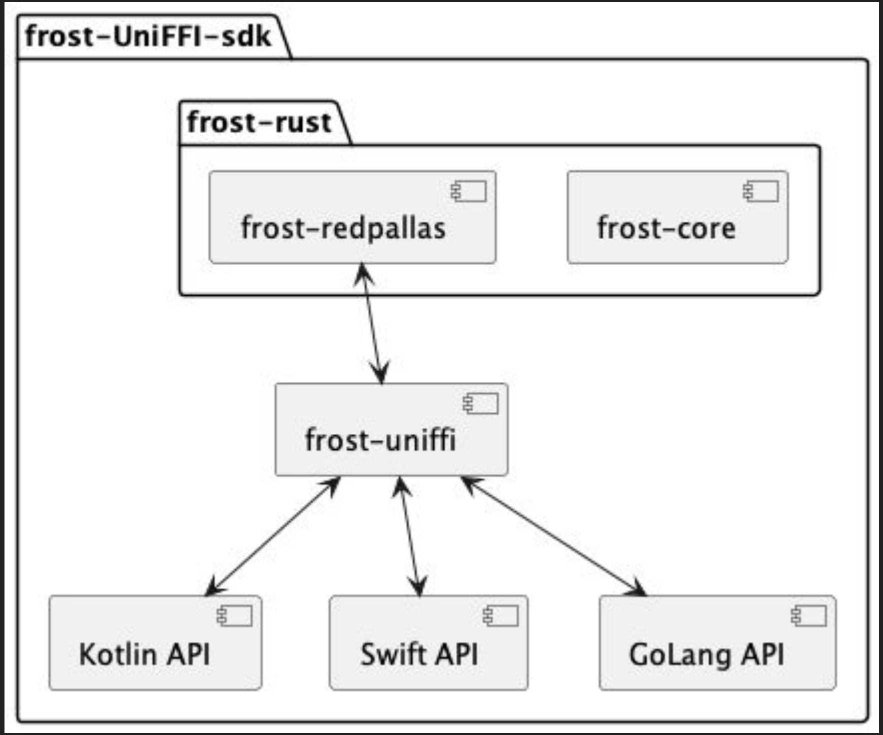
Expectation

Reality

Architecture

The Mozilla UniFFI framework allows having 1 different FFI per language.

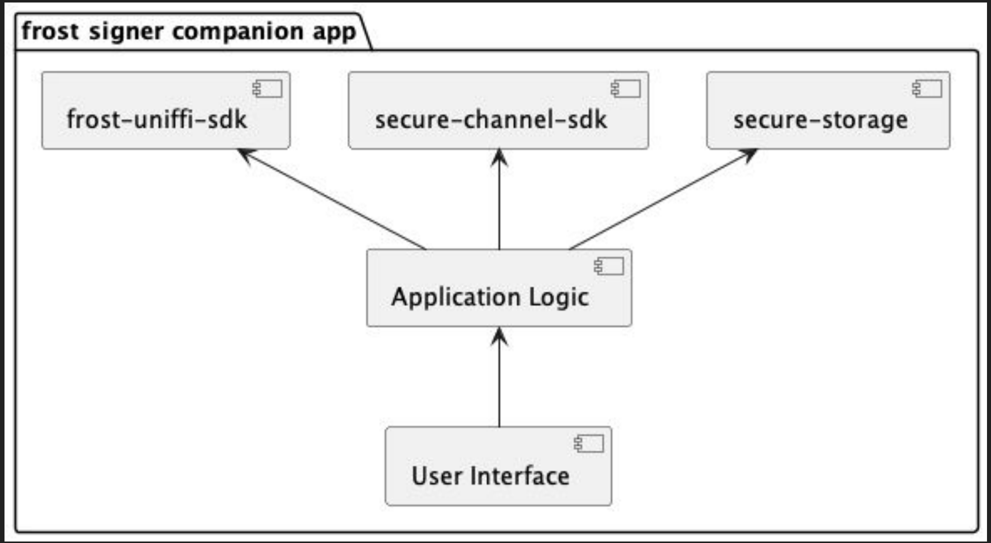
The target languages call the frost-uniffi primitives.



Use case: FROST companion application

A Mobile companion Application that helps Signing UX

- Can create
  - Trusted Setup
  - DKG
- Can participate in TSS or DKG signature
- Can backup own or restore other shares



Let’s walk!

Code walkthrough screen share

Thank You!

Contributions are welcome!

GitHub Repo QR

https://github.com/zecdev/frost-uniffi-sdk

Ping me!

pacu{at}zecdev.org