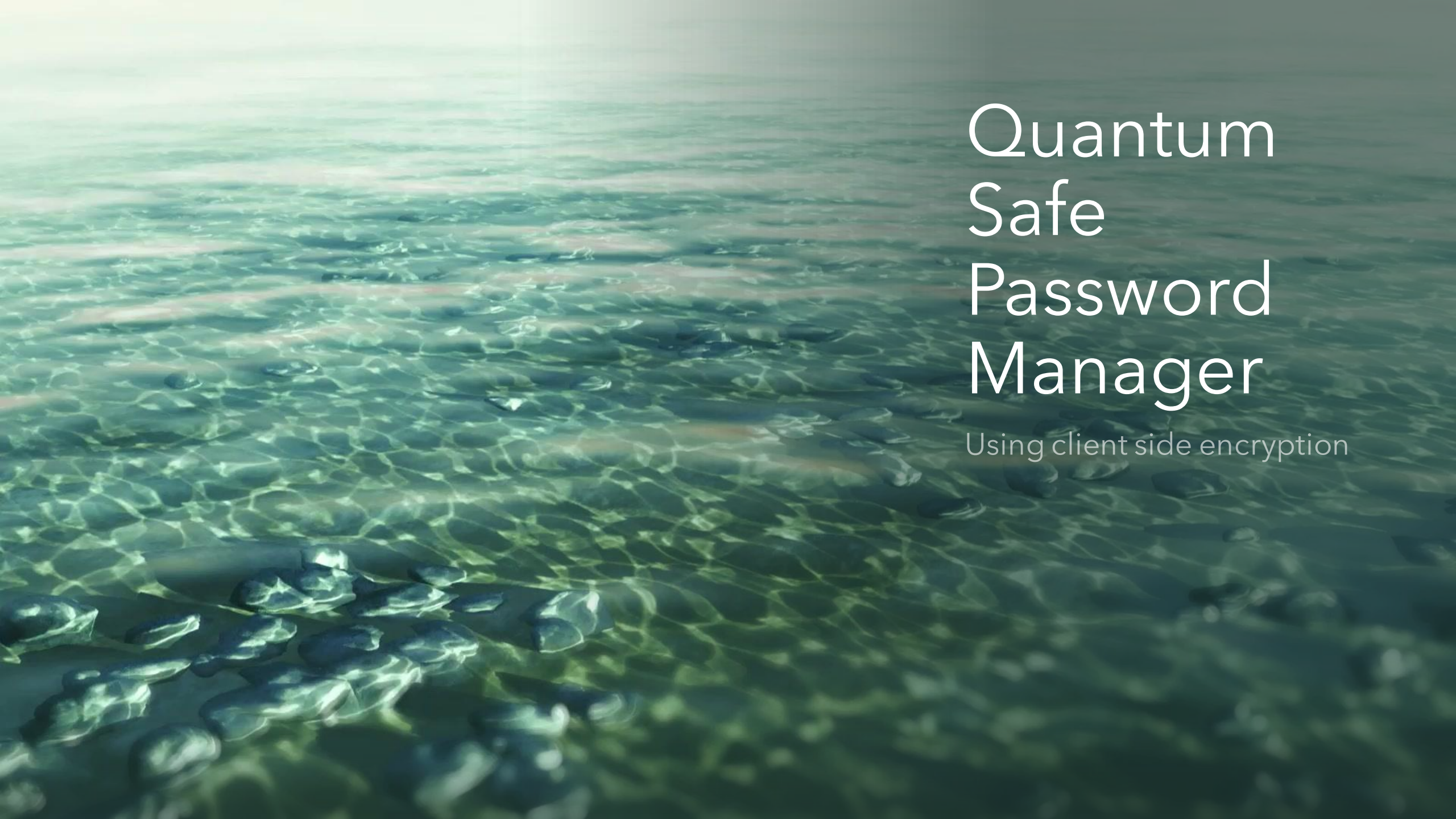


Quantum Safe Password Manager

Using client side encryption

Agenda

- Server Side
- Client Side
- Summary

Server Side Encryption

- Traditional approach
- Data is stored securely on the server
- Application accesses the encrypted and decrypted data via TLS

Server Side Issues

TLS transfers sensitive data

TLS is secure today but not quantum safe

TLS will be quantum safe in the future

Any data collected today could be vulnerable

PITM (Person-In-The-Middle) Attack

Could capture sensitive data

Server side security

Depends on how well the server administration manages security

Client Side Encryption

Data is encrypted and decrypted in the browser

Only encrypted data is transferred

Can use symmetric key encryption

Client Side Issues

Depends on browser sandbox security

Master password is not recoverable

Vulnerability Summary

SERVER SIDE

- Browser
- Lost master password
- Stored TLS
- PITM
- Server security

- CLIENT SIDE
- Browser
- Lost master password

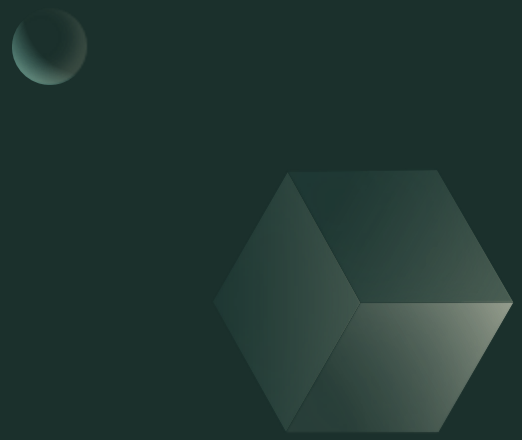
qspm

WEB APP WRITTEN IN HTML, CSS, JAVASCRIPT

WASM MODULE WRITTEN IN RUST

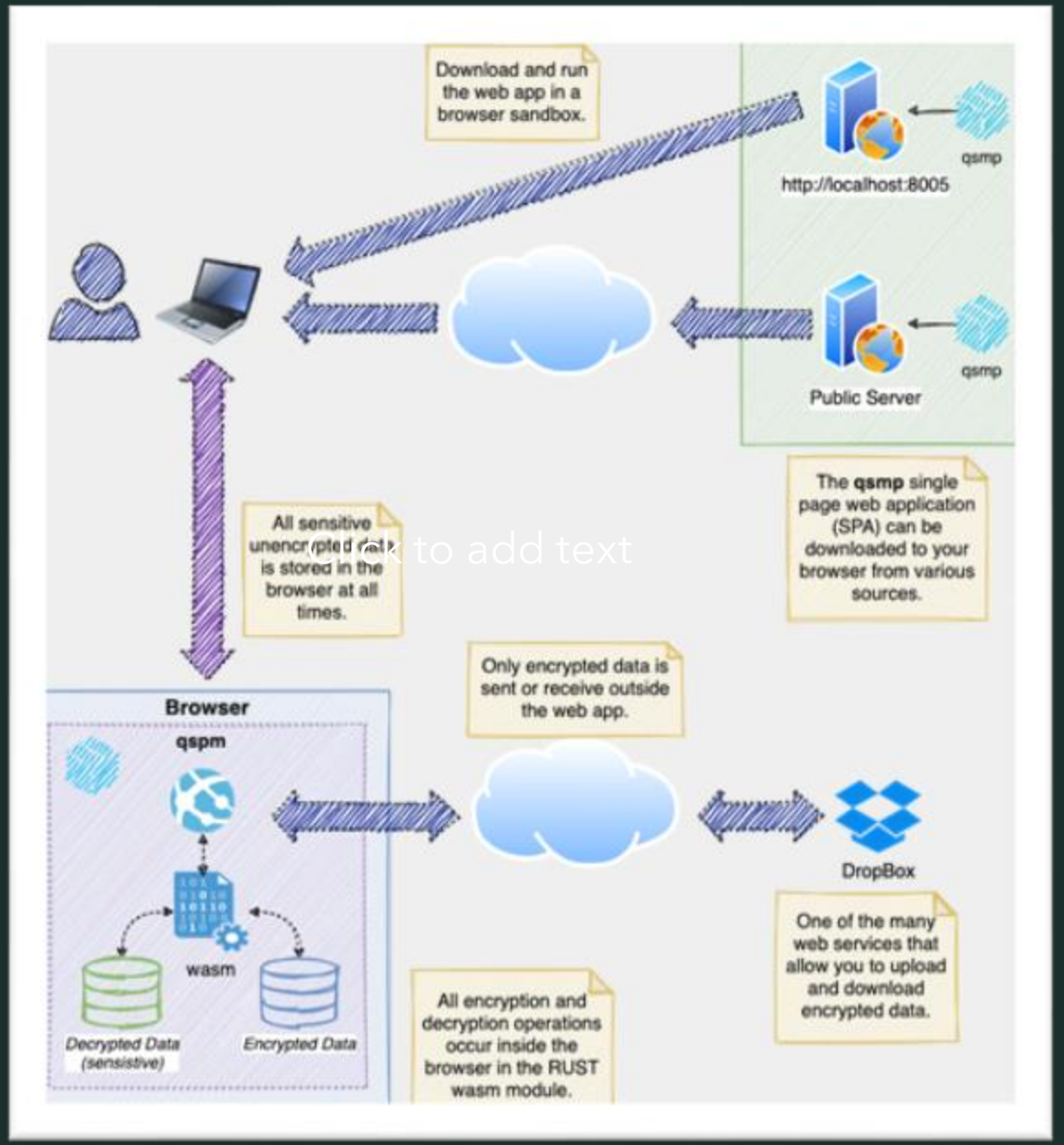
SCAFFOLDING WRITTEN IN MAKE AND PYTHON

SPA Web App

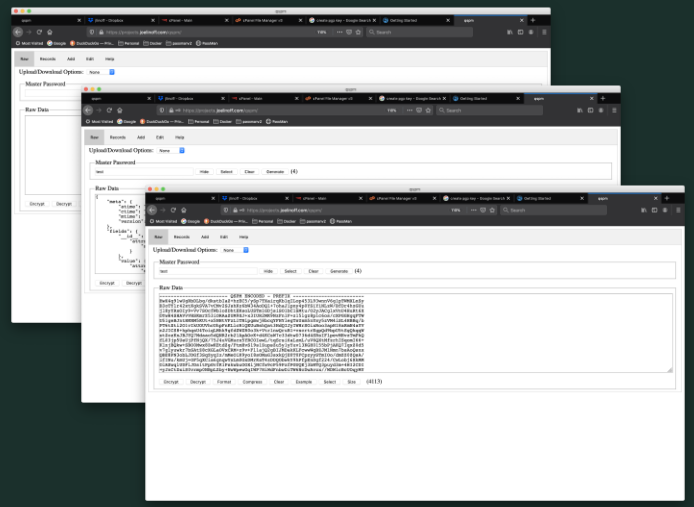


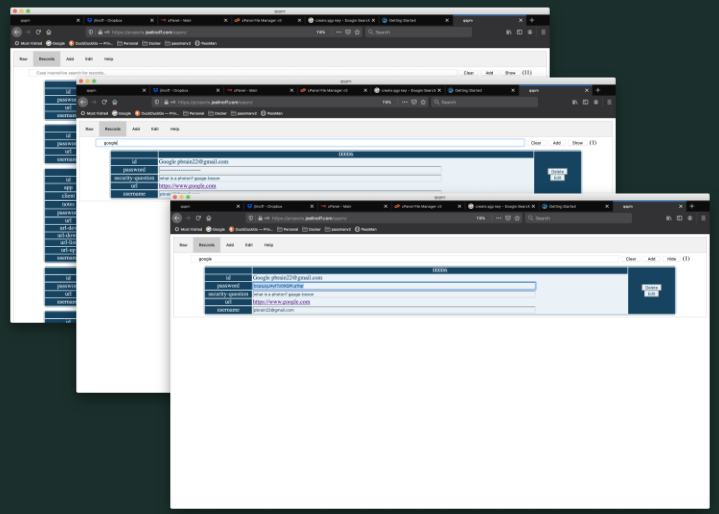
- Simple single page web application
- Web Assembly (wasm) module to do encryption/decryption
- Only allows the export of encrypted data
- Ties into common cloud storage systems
  - AWS
  - DropBox
  - Google Drive
  - Microsoft OneDrive

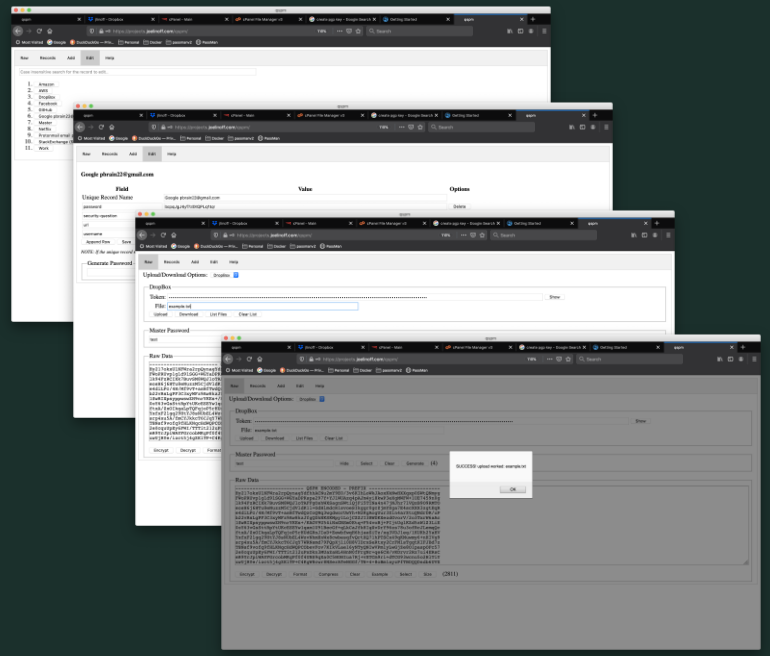
Flow

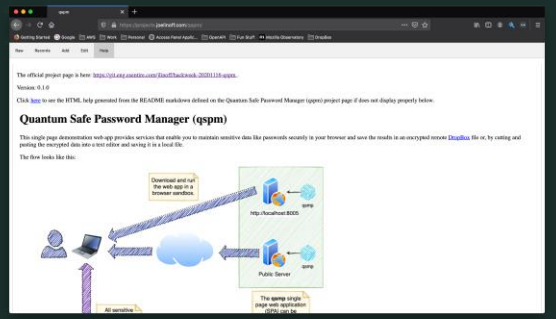

Download and run the web app in a browser sandbox.
http://localhost:8005
qsmp
Public Server
qsmp
The qsmp single page web application (SPA) can be downloaded to your browser from various sources.
All sensitive unencrypted data is stored in the browser at all times.
Only encrypted data is sent or receive outside the web app.
Browser
qspm
wasm
Decrypted Data (sensistive)
Encrypted Data
DropBox
One of the many web services that allow you to upload and download encrypted data.
All encryption and decryption operations occur inside the browser in the RUST wasm module.

Demo








Quantum Safe Password Manager (qspm)
Download and run the web app in a browser sandbox.
http://localhost:8005
Public Server

Next Steps

01

This is FOSS

02

Publish initial version

03

Add support for additional cloud storage services