CROWD SUPPLY

Signet

Physical security for your personal data

Signet is a compact, open hardware, and free and open source software USB device that safely stores your passwords, bookmarks, contacts, and other personal data in encrypted memory. It's compatible with MacOS, Linux, Windows, and Android so you can use it on any device with a USB port. The device is smaller than the average house key, making it easy to take with you wherever you go. This makes Signet a practical alternative to storing sensitive data in the cloud. Unlike cloud-based or proprietary solutions, Signet is fully auditable with no proprietary software, firmware, or binary blobs to potentially hide security flaws.

A Powerful Cross-Platform Application

Access your data through a cross-platform application that unlocks your data with your master password. Once unlocked, Signet acts as both a password manager and a general personal information database. Signet acts as a USB keyboard to allow you to easily enter data into web forms. Signet can also type both a username and password to log you into a website instantly. The application features an intuitive graphical interface as well as keyboard-based navigation to enable you to perform common tasks quickly.

Easily Access Your Data Anywhere

On desktop operating systems (Windows, GNU/Linux, MacOS), the Signet application software can run as a standalone executable with no driver installation needed, allowing you to quickly access your data at new locations. If you're away from a computer, you can still access your data on your Android device through a USB host adapter cable.

Physical Security for Peace of Mind

Unlike pure software solutions, Signet protects your data from any hostile software on the systems you use. Signet will not transmit, modify, or destroy any data without the command being confirmed by a button press when the device flashes. This physically secures the device because only the user can press the device's button. No system's security is absolute, but physically requiring a button press to confirm sensitive operations increases the complexity and decreases the potential effectiveness of any attack.

Flexible Data Storage

Signet's personal information database allows you to store whatever data you might want to keep with you and possibly off the cloud. It features built-in types for contacts, bookmarks, credit cards, and miscellaneous account numbers. You can add new data types to the database so you can keep track of whatever else is important to you and you can add fields to individual entries for notes and related data.

Personal Data Backups

Keeping your Signet with you comes with the risk of losing the device. You can configure Signet to regularly back up your data when connected to your primary computer, to either your computer's hard disk or a designated removable media device such as a USB stick or memory card. The Signet client can then read the backups when you provide the master password, giving you immediate access to your data and the option to upload the data to a replacement device.

To give you full control over your data the Signet application will also support conversions between Signet's internal database format and other popular formats. It will support import and export of login information into KeePass databases, and export of all data types to unenecrypted formats such as plaintext, CSV, XML, and JSON.

Who Needs It and Why?

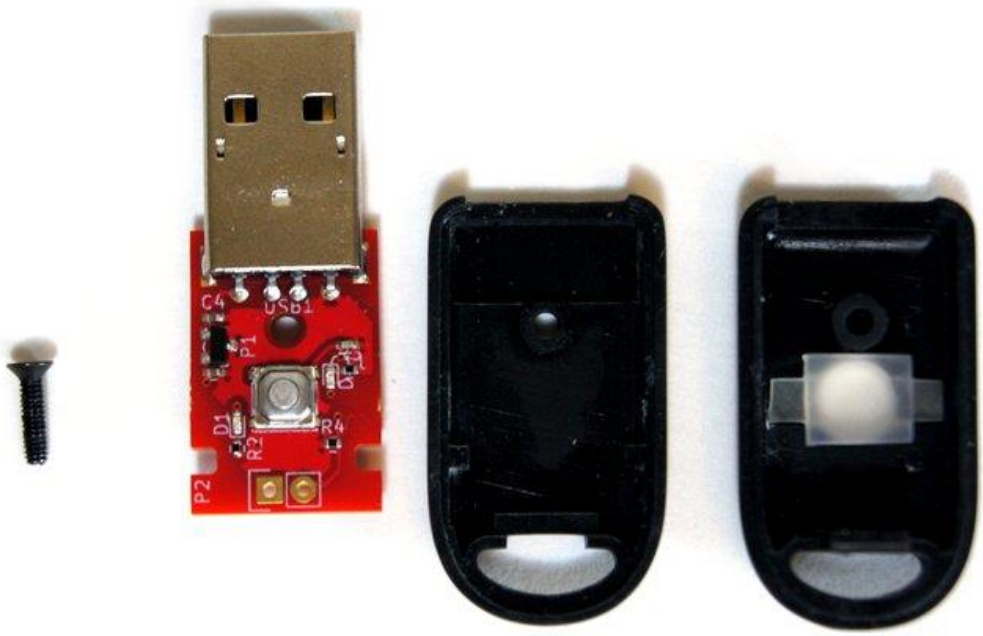
Signet is for anyone who wants the portability and convenience of storing passwords and other sensitive data on the cloud without having to trust closed source software or the security of third-party networks.

Signet could be useful to anyone who has:

- Reused passwords in order to have fewer to remember and has had to change passwords on many accounts because one account was compromised.
- Wanted to store private information (such as Social Security numbers) on their person but hesitated because of the risks of the information being stolen.
- Resorted to using simplistic passwords to make them easy to remember despite the risks of password cracking.
- Needed to access sensitive data (passwords, credit cards, account numbers, etc) on multiple computers outside their home (school, work, etc).
- Wanted to move away from using hand written notes and stray text files for remembering important data and switch to using a self-contained digital system.

Features & Specifications

- **Dimensions:** 46 mm x 18 mm x 10.5 mm
- **Compatibility:** Windows, Linux, MacOS, Android
- **Firmware Software License:** GPLv3 (https://github.com/nthdimtech/signet-firmware)
- **Client Software License:** GPLv3 (https://github.com/nthdimtech/signet-desktop-client)
- **KiCAD Files License:** CC-BY-3.0 (https://github.com/nthdimtech/signet-cad)
- **Enclosure:** Injection molded ABS plastic fastened with a screw and an external snap
- **Microcontroller:** STM32L442 Cortex M4 processor
- **Database Capacity:** 192 KB. Enough space for thousands of data fields
- **Database Storage Type:** On-chip flash memory
- **Encryption Method:** AES-256 with cypher block chaining
- **Encryption Key Derivation:** PBKDF2 based hash function with a per-device randomized salt
- **Firmware Program Size:** 64 KB



Comparisons

	Open source	Non-password data	Cost	Physical portability	Physical security	Offline
Signet	Yes	Yes	$39	High	Yes	Yes
Mooltipass	Yes	No	$79	Limited	Yes	Yes
KeePass	Yes	No	Free	N/A	No	Yes
Lastpass	No	Yes	$12/year	N/A	No	No

Demonstration Videos

Learn about Signet's implemenation and features from these videos.

Password Management

Device Management

Manufacturing Plan

MacroFab will manufacture the PCBs. I'm choosing MacroFab since I have worked with them throughout Signet's prototyping process, have received good service, and the most recent prototype runs have met all of my production requirements.

ICOMold will make the enclosure using an injection mold. I have a competitive, confirmed quote with ICOMold for the final enclosure model and have been in discussions with them for several months. I will order the injection mold before the campaign ends to reduce the risk of delay.

The button parts will be 3D printed in resin and contain a diffusing film. The button parts need little to no processing after printing and many button parts can be printed in a single run cheaply. If more than 500 orders are made, I will have the buttons injection molded by ICOmold at the same time as the enclosures.

Once high-quality injection-molded part samples come back, the mold will be finalized and the first volume batch of 500 or fewer enclosure parts, buttons, and PCBs will be made.

I will personally assemble and test the final units if fewer than 500 units are ordered. For higher quantities, I will arrange for testing and assembly to be done by MacroFab. Once assembled and tested, the final units will be sent to Crowd Supply for shipping from Portland, OR.

Risks & Challenges

The biggest risk is that the parts that make the enclosure don't fit correctly with each other or the PCB. I will double check all fit tolerances before making the injection mold order. ICOmold will receive sample 3D printed buttons and PCB samples so that they can test the fit on site before sending first samples. If there are fit problems in the first samples I can work with ICOmold to correct the problems before a full production run of parts is done at the cost of a delay. If the buttons are resin printed the button fit can be calibrated after the mold is finalized to eliminate that risk.

Another possibility is that some of the PCBs in the production run will have faults. This risk is relatively low since I will be doing my production run with MacroFab, which is same company that has been manufacturing my prototype PCBs. I will make a pre-production order of a dozen PCBs before the campaign ends in preparation for the production run in order to identify manufacturing problems. I will also order 10% more PCBs than needed for the production run so I can have the option to discard some PCBs and still complete assembly on time.