The Making of a Secure Open Source Password Keeper

… from the electronics to the high-level software

Mathieu Stephan February 5, 2017

Hello!

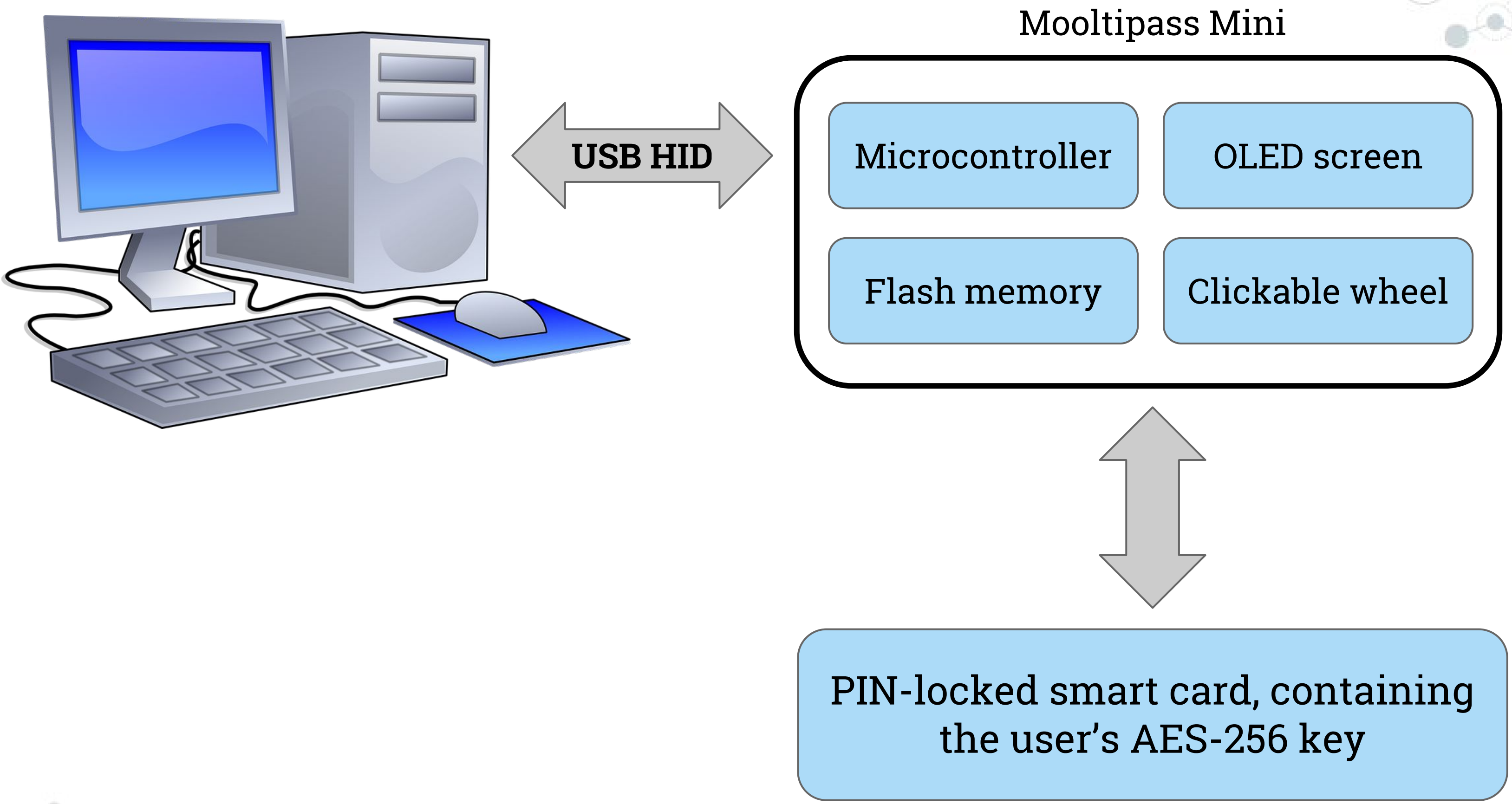
I am Mathieu Stephan

- Embedded systems engineer
- Former writer for Hackaday
- www.limpkin.fr
- Mooltipass project founder

What is the Mooltipass?

- Secure credential & file storage
- Native browser integration
- Recognized as a keyboard
- Aluminum case
- Multiple users
- Open software & hardware

The Internals



USB HID

Mooltipass Mini

Microcontroller

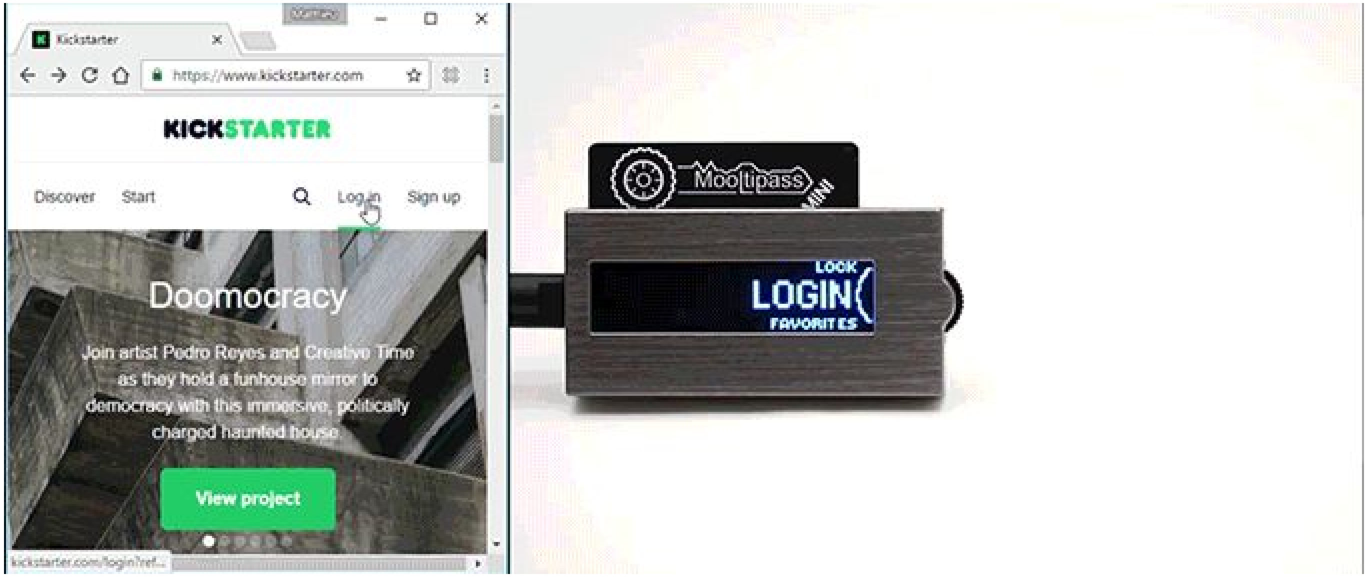
OLED screen

Flash memory

Clickable wheel

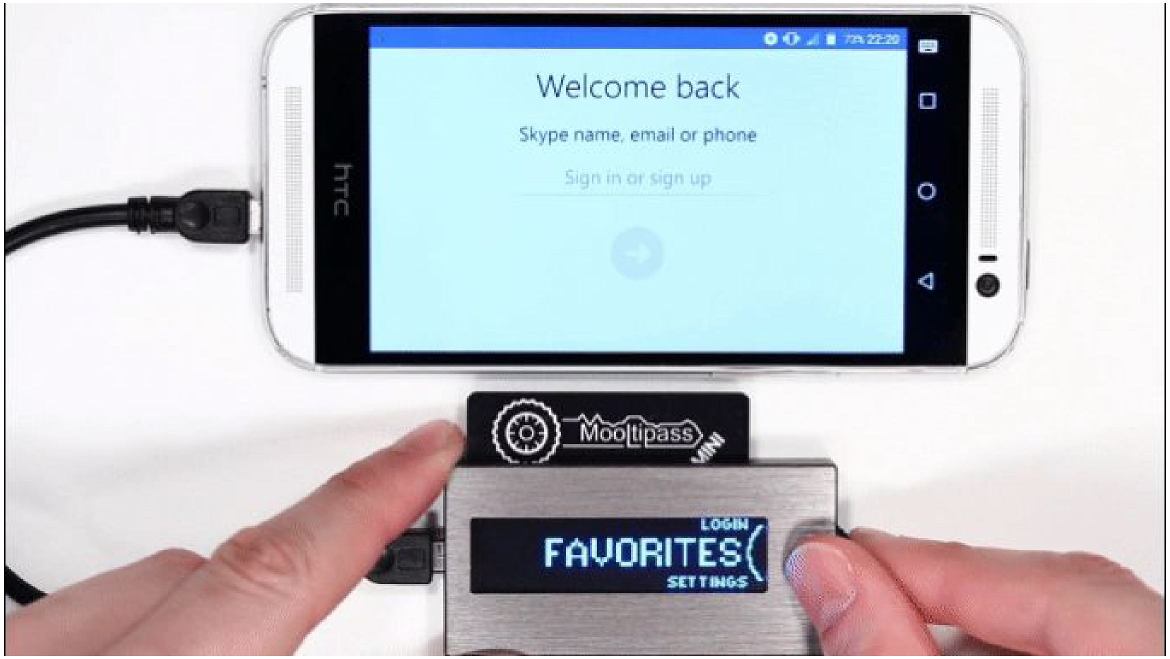
PIN-locked smart card, containing the user’s AES-256 key

Usage Example



Join artist Pedro Reyes and Creative Time as they hold a funhouse mirror to democracy with this immersive, politically charged haunted house.

Usage Example



Presentation Outline

Here’s how…

… this adventure started

… 20 people collaborated without meeting each other

… we produced two devices from the ground up

… the Mooltipass software was designed

… we successfully raised ~$290k

… so you can do the same for your project!

1.

Starting The Project

Getting contributors and setting up the project infrastructure

Beginning The Mooltipass Adventure

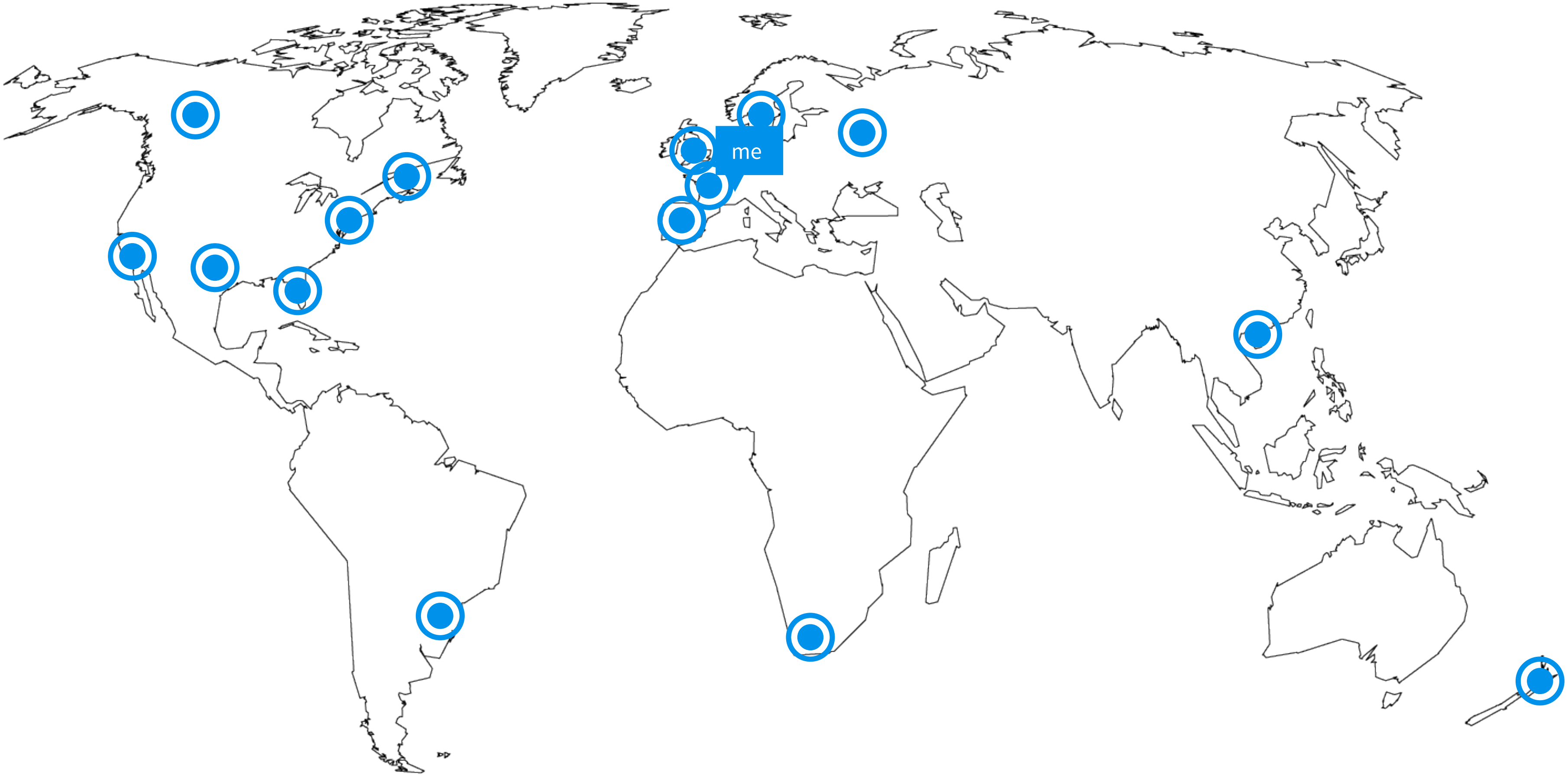
First call for contributors was in December 2013

- First article on hackaday.com describing the concept
- “Developed on Hackaday” but not associated with it
- Received 30 applications!

Work was assigned based on the applicants’…

1) Preferences
2) Available spare time
3) Area of expertise

Globally Distributed Contributors



The Ground Rules

- Implement features as determined by consensus
- Use GitHub for code versioning and source control
- **Document** the produced code (doxygen)
- Work in a dedicated file or folder
- Follow the chosen coding convention

Group Communications

Constraint: people have different availabilities!

- Separate general and development discussion groups
- Direct contact via IM service (sparingly)

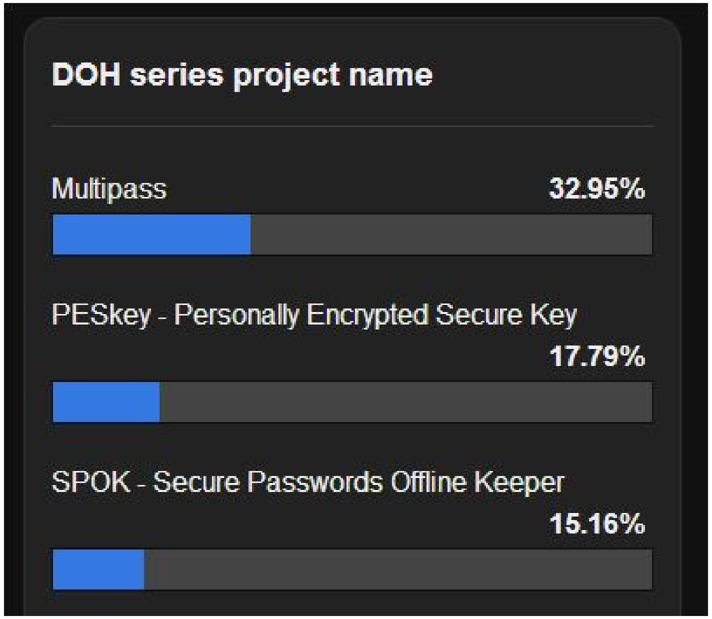
Challenge: keep the momentum going!

- Show off contributors’ progress
- Ensure the community feels involved

Keeping Everyone Involved

Publish monthly progress articles on Hackaday

to get readers' input…



DOH series project name

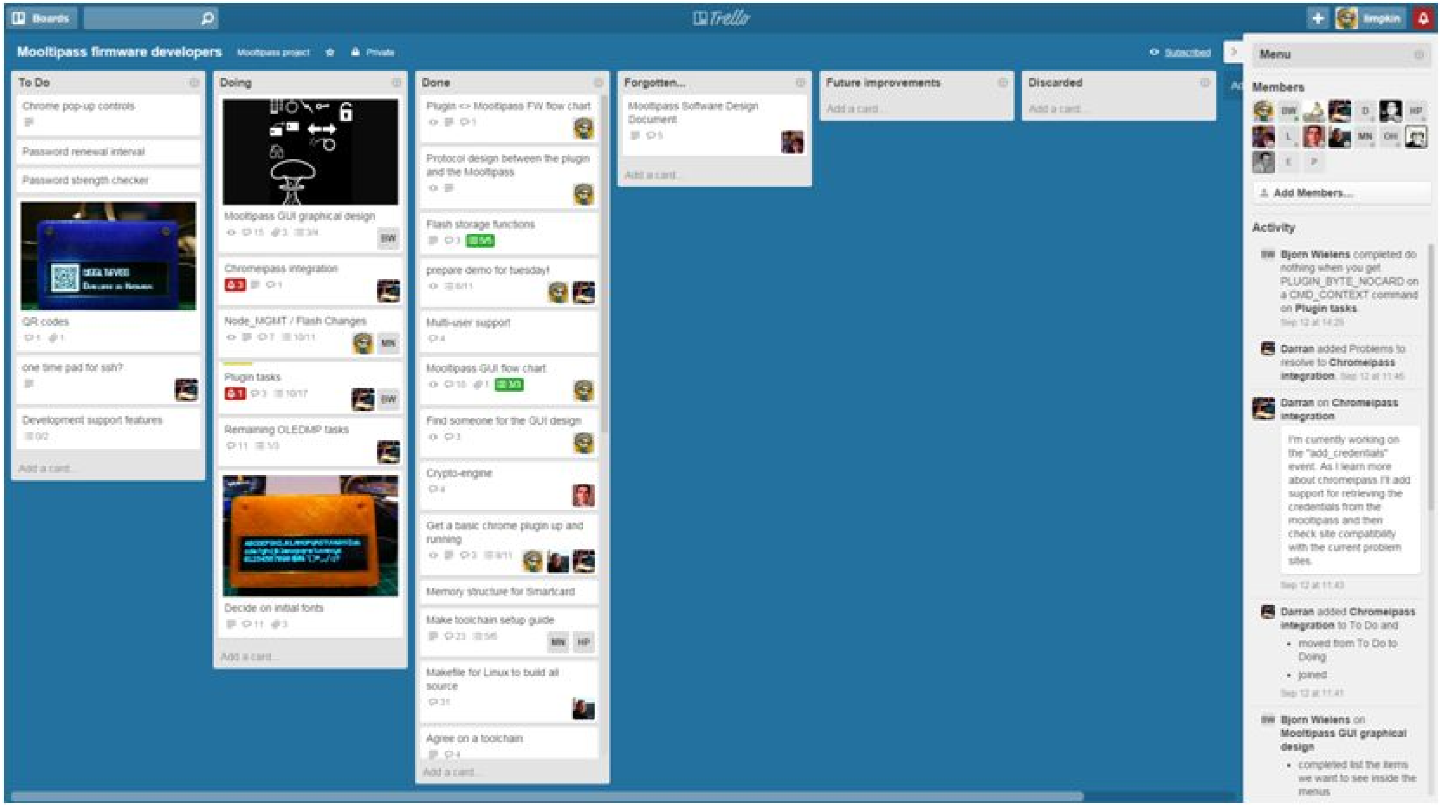
Multipass 32.95%

PESkey - Personally Encrypted Secure Key 17.79%

SPOK - Secure Passwords Offline Keeper 15.16%

… and to spread brand recognition

Management Infrastructure



Boards

Trello

limpkin

Mooltipass firmware developers Mooltipass project Private

Subscribed

To Do

- Chrome pop-up controls
- Password renewal interval
- Password strength checker
- QR codes — 1 1
- one time pad for ssh?
- Development support features — 0/2

Add a card...

Doing

- Mooltipass GUI graphical design — 15 3 3/4 BW
- Chromeipass integration — 3 1
- Node_MGMT / Flash Changes — 7 10/11 MN
- Plugin tasks — 1 3 10/17 BW
- Remaining OLEDMP tasks — 11 5/3
- Decide on initial fonts — 11 3

Add a card...

Done

- Plugin <> Mooltipass FW flow chart — 1
- Protocol design between the plugin and the Mooltipass
- Flash storage functions — 3 5/5
- prepare demo for tuesday! — 8/11
- Multi-user support — 4
- Mooltipass GUI flow chart — 18 1 3/3
- Find someone for the GUI design — 3
- Crypto-engine — 4
- Get a basic chrome plugin up and running — 3 8/11
- Memory structure for Smartcard
- Make toolchain setup guide — 23 5/6 MN HP
- Makefile for Linux to build all source — 31
- Agree on a toolchain — 4

Add a card...

Forgotten...

- Mooltipass Software Design Document — 5

Add a card...

Future improvements

Add a card...

Discarded

Add a card...

Menu

Members

BW D HP L MN OH E P

Add Members...

Activity

Bjorn Wielens completed do nothing when you get PLUGIN_BYTE_NOCARD on a CMD_CONTEXT command on **Plugin tasks**
Sep 12 at 14:28

Darran added Problems to resolve to **Chromeipass integration**. Sep 12 at 11:46

Darran on **Chromeipass integration**

I'm currently working on the "add_credentials" event. As I learn more about chromeipass I'll add support for retrieving the credentials from the mooltipass and then check site compatibility with the current problem sites.

Sep 12 at 11:43

Darran added **Chromeipass integration** to To Do and

- moved from To Do to Doing
- joined

Sep 12 at 11:41

Bjorn Wielens on **Mooltipass GUI graphical design**

- completed list the items we want to see inside the menus

Trello - a free online Kanban board

Management Infrastructure

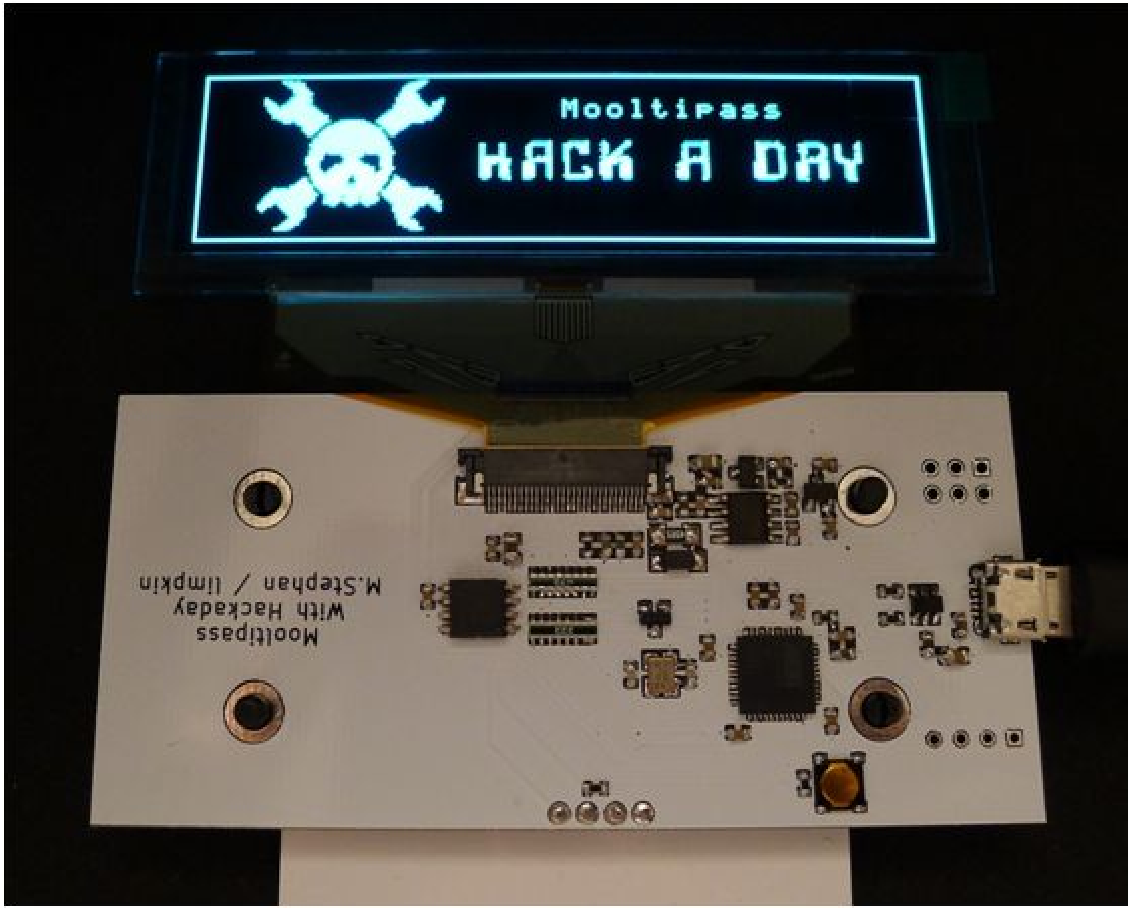
Based on the Japanese kanban process

- Respect the roles, responsibilities and titles
- Leadership at all levels
- Document & encourage evolutions
- Maintain a community atmosphere
- Obtain & manage ETAs without contributors feeling pressured

2.

The Mooltipass Hardware

Functional Prototype



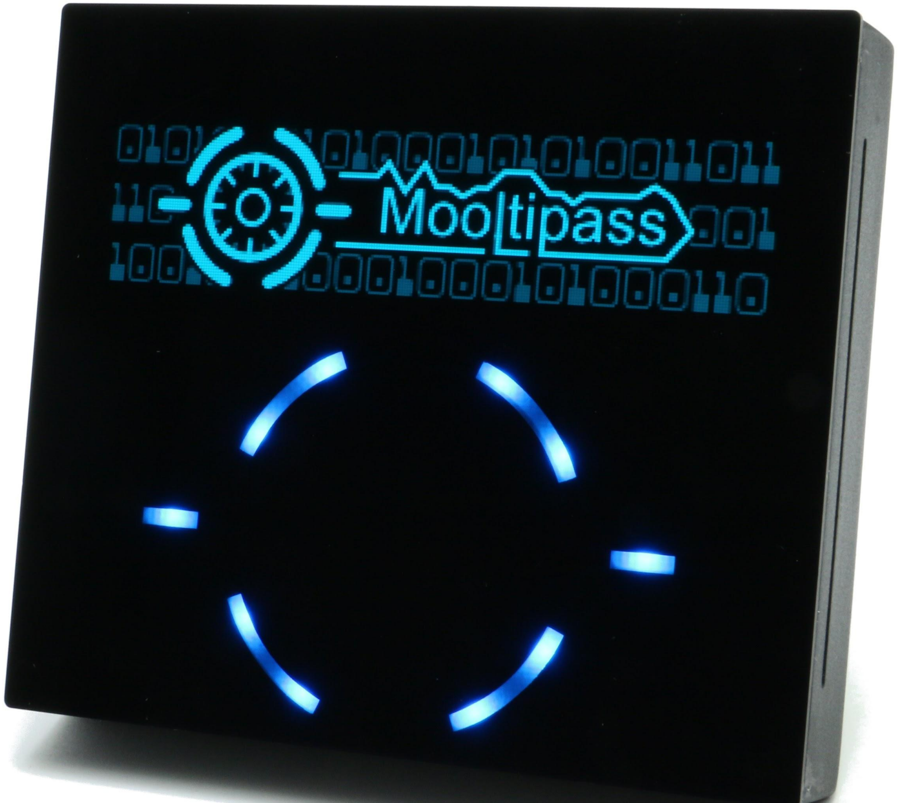
Hand soldered and shipped to contributors

Mooltipass - Case Choice

Mooltipass
HACK A DAY
laser cut
tinted acrylic top
mooltipass
rotary encoder
large hardware
protects the device
injection molded bottom

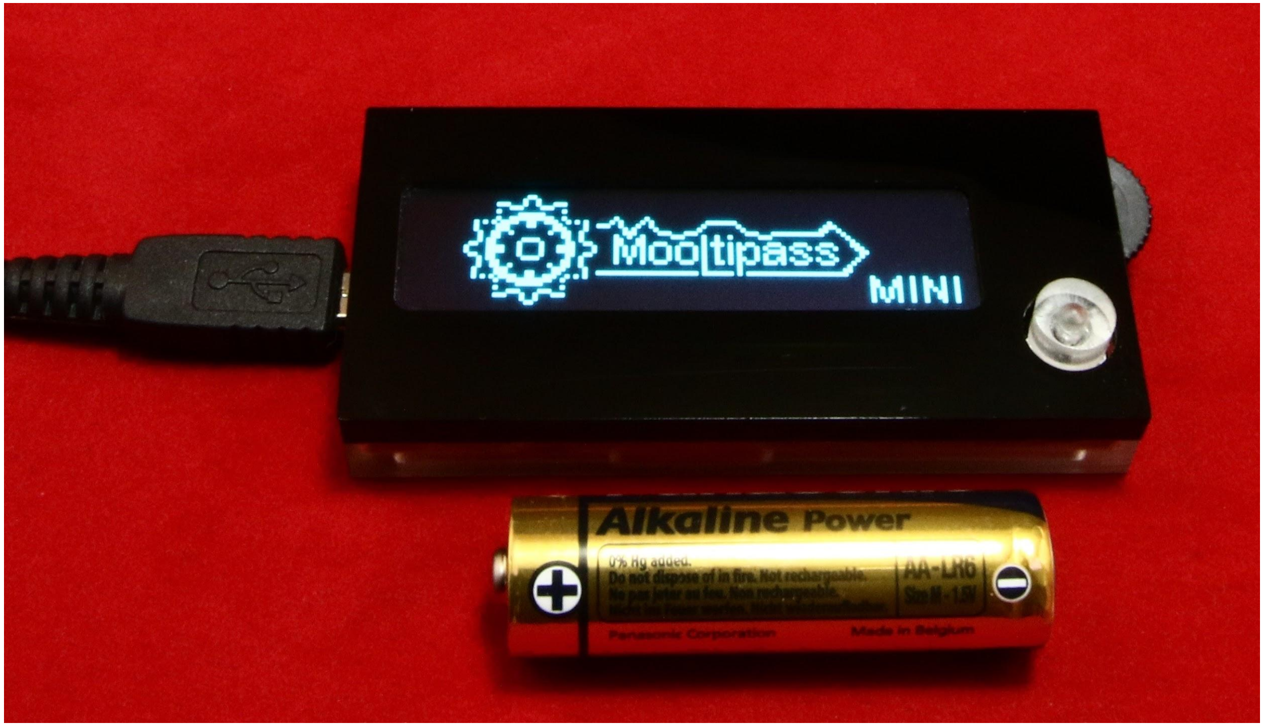
Designs made by the community

Mooltipass - Final Design



110% funded in Dec. 2014

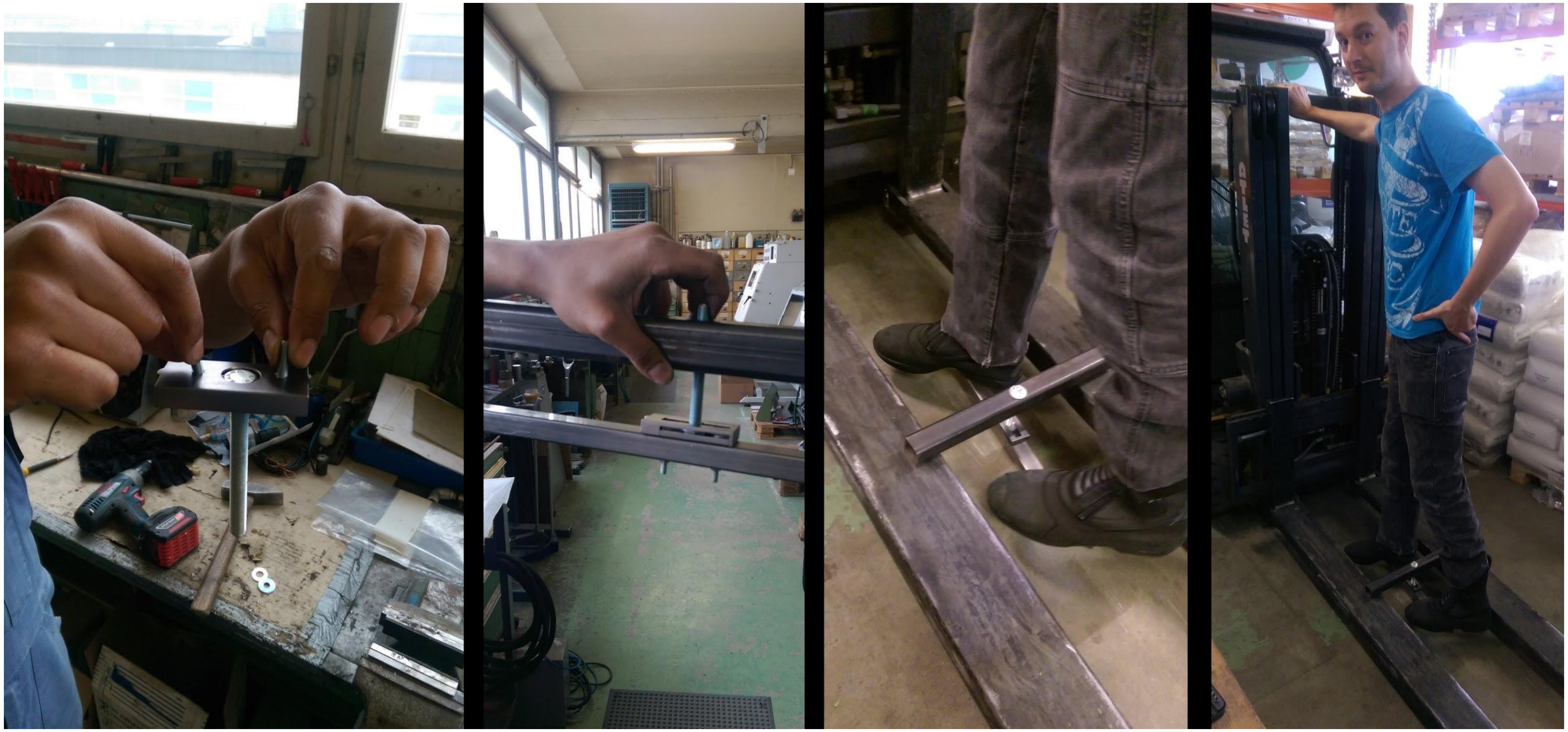
Mooltipass Mini



Mooltipass Mini

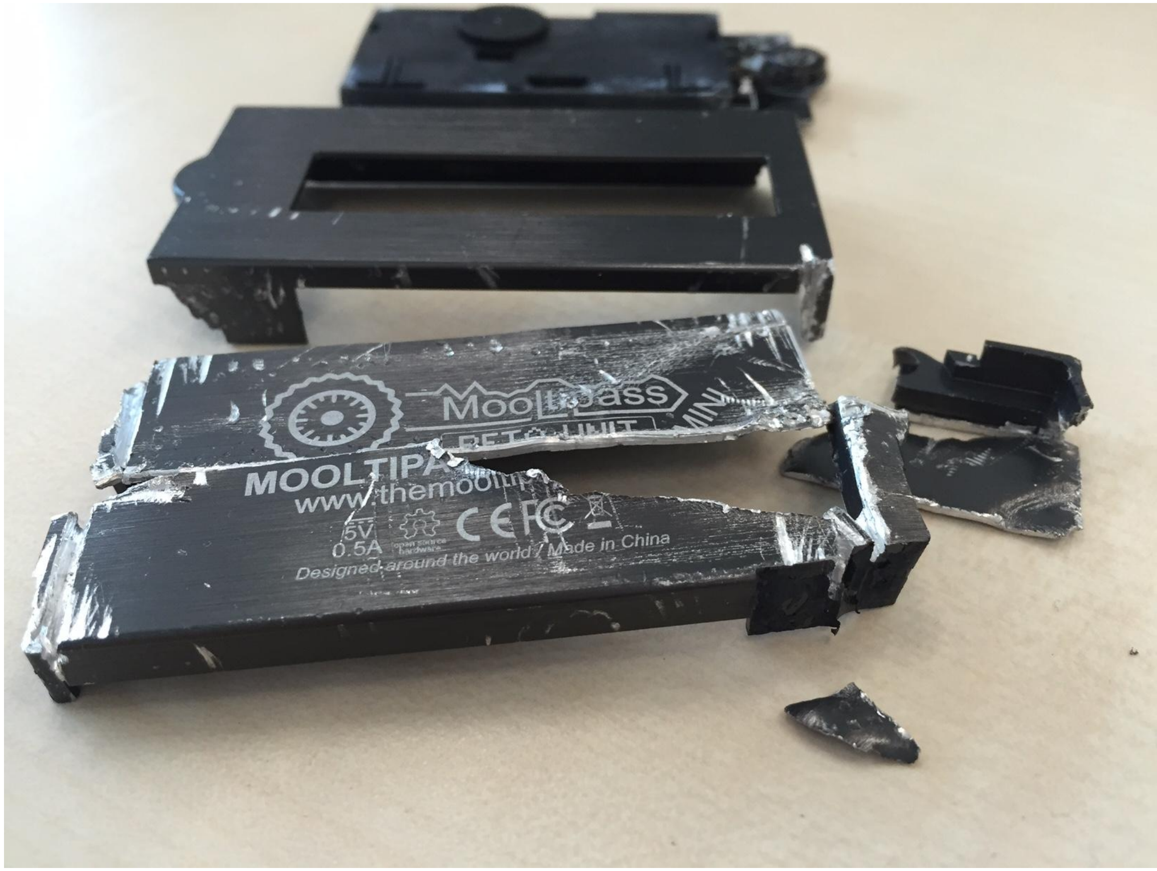
300% funded in Oct. 2016

Mooltipass Mini - Tests



Testing the adhesive strength

Mooltipass Mini - Tests



…but some people double checked!

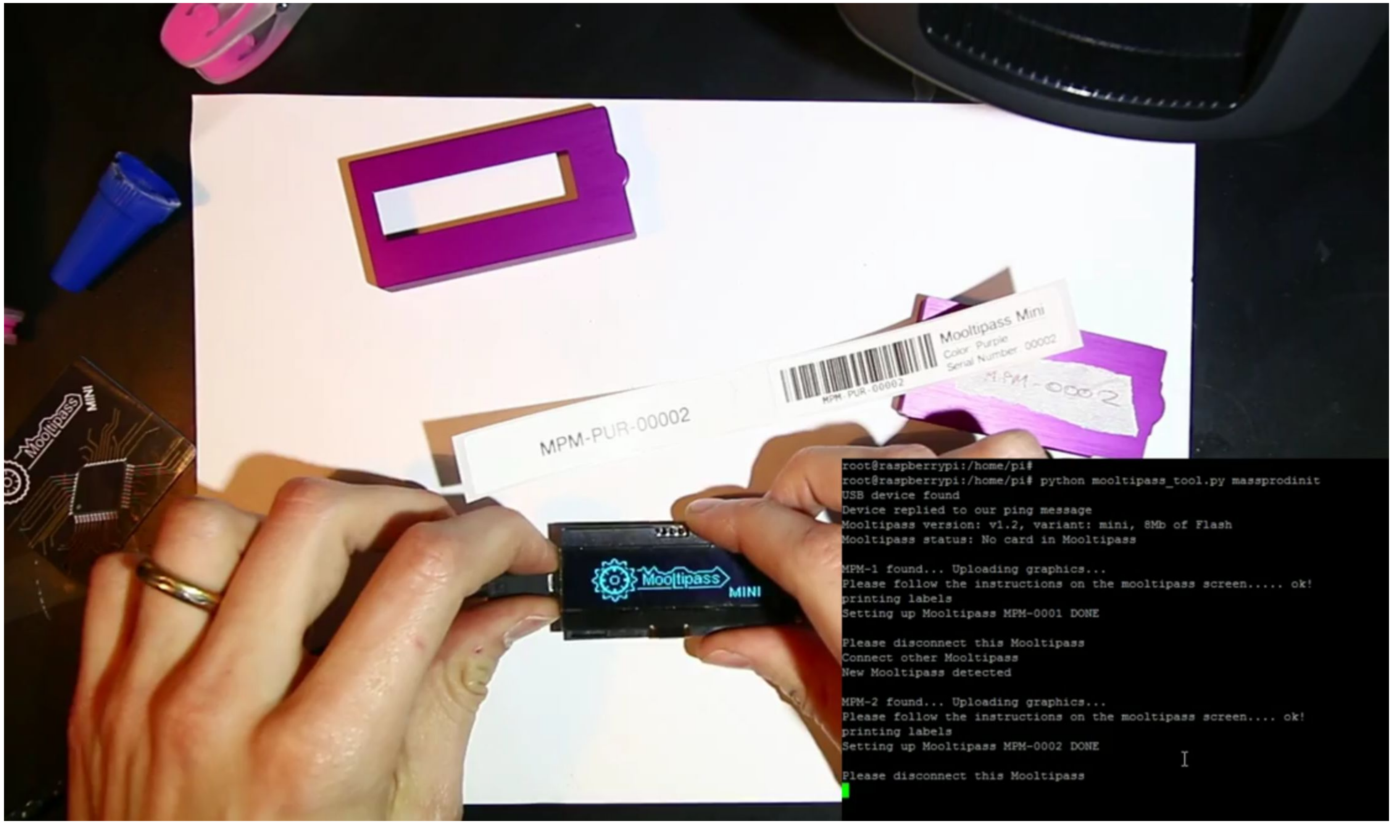
Mooltipass Mass Production

Chinese assembly lines

Mooltipass Mass Production

CNC shops

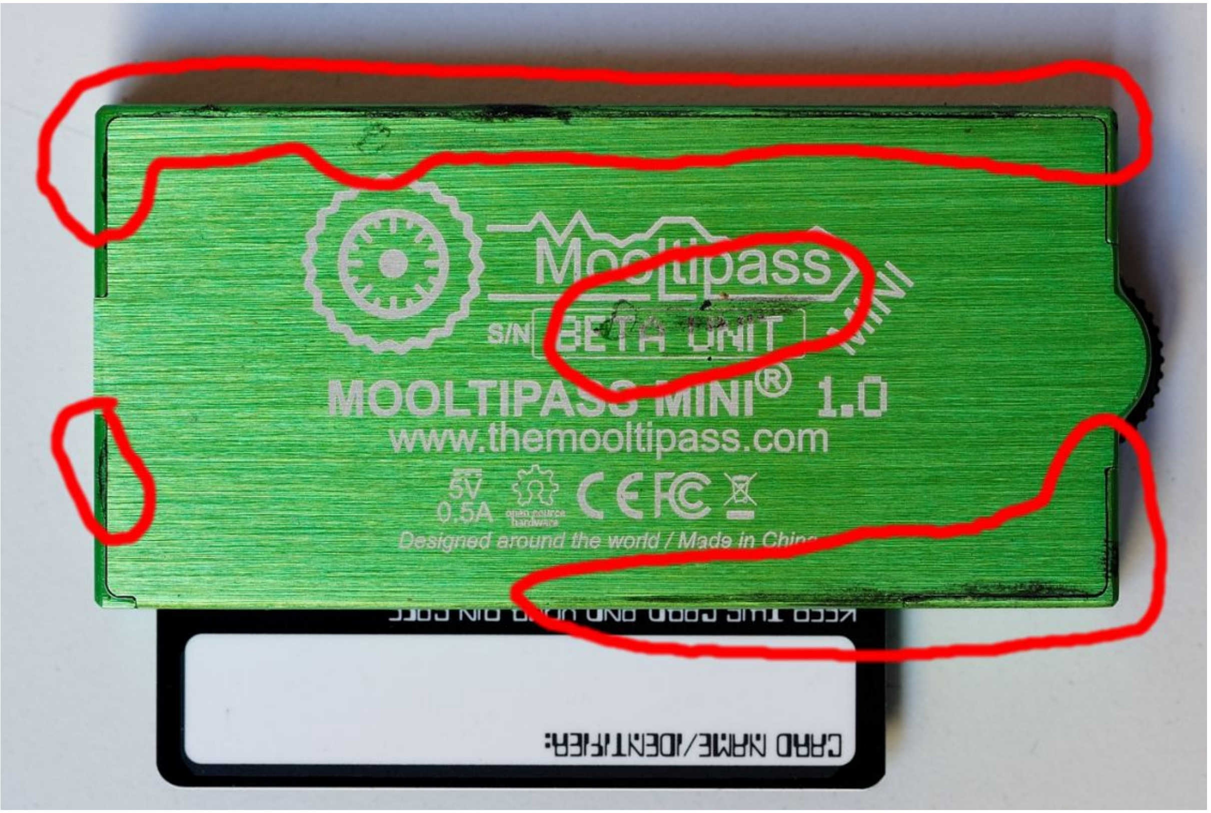
Mooltipass Mass Production



```
root@raspberrypi:/home/pi#
root@raspberrypi:/home/pi# python mooltipass_tool.py massprodinit
USB device found
Device replied to our ping message
Mooltipass version: v1.2, variant: mini, 8Mb of Flash
Mooltipass status: No card in Mooltipass

MPM-1 found... Uploading graphics...
Please follow the instructions on the mooltipass screen..... ok!
printing labels
Setting up Mooltipass MPM-0001 DONE

Please disconnect this Mooltipass
Connect other Mooltipass
New Mooltipass detected

MPM-2 found... Uploading graphics...
Please follow the instructions on the mooltipass screen.... ok!
printing labels
Setting up Mooltipass MPM-0002 DONE

Please disconnect this Mooltipass
```

Video instructions for the assembler

Mooltipass Mass Production



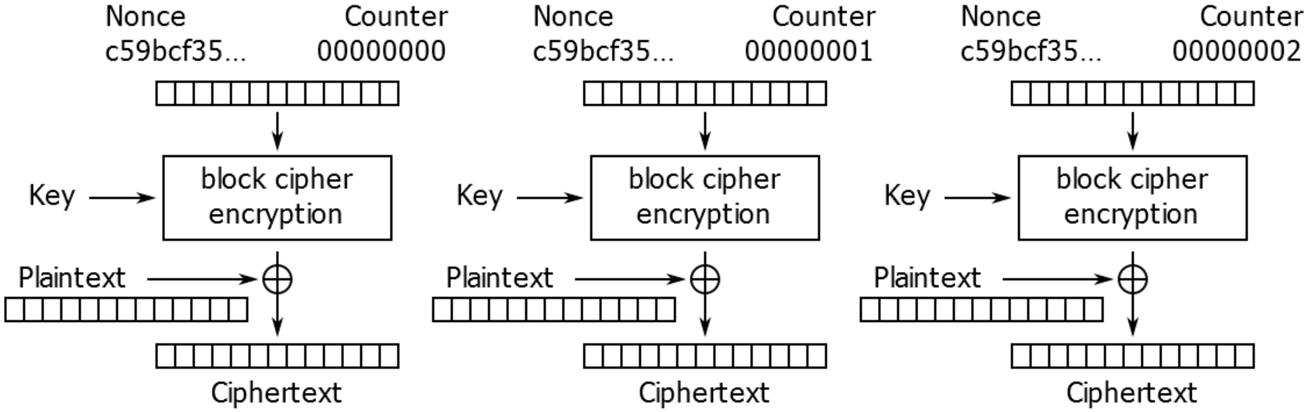
… and a lengthy quality control document

3.

The Mooltipass Firmware

Firmware - AES Encryption

- Using AVR-Cryptolib, CTR mode
- Checked against NESSIE vector sets



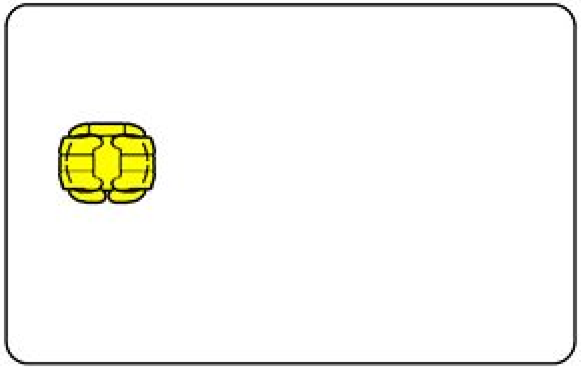
Counter (CTR) mode encryption

Firmware - Encrypted Storage

- Dedicated flash memory used for storage
- 2 types of data
  - Credentials
  - Encrypted blobs
- Sorted linked list data structure
- Encryption key stored inside the smart card

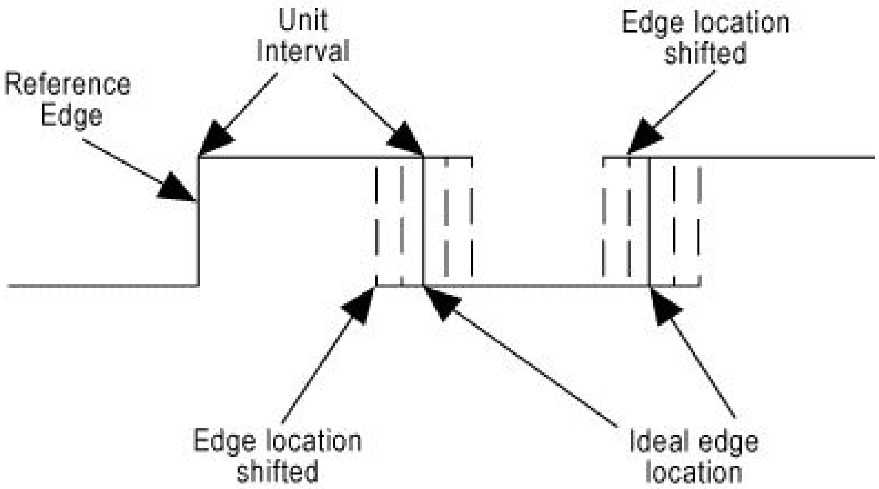
Firmware - Smartcard Use

- Ubiquitous form of read-protected memory
- 16-bit PIN code (“0000” to “FFFF”)
- Permanently locked after 4 incorrect PINs
- Cheap (<$1) in volume



Firmware - RNG

- Uses watchdog timer’s natural jitter
- Generate 8 bytes per second (!)



Firmware - USB

- USB composite: HID keyboard & HID ‘proprietary’
- USB Keyboards are natively supported by all OSes…
  - …but LUTs needed for different locales
- Keyboard channel for manual password recall
- Proprietary channel for integration plugins

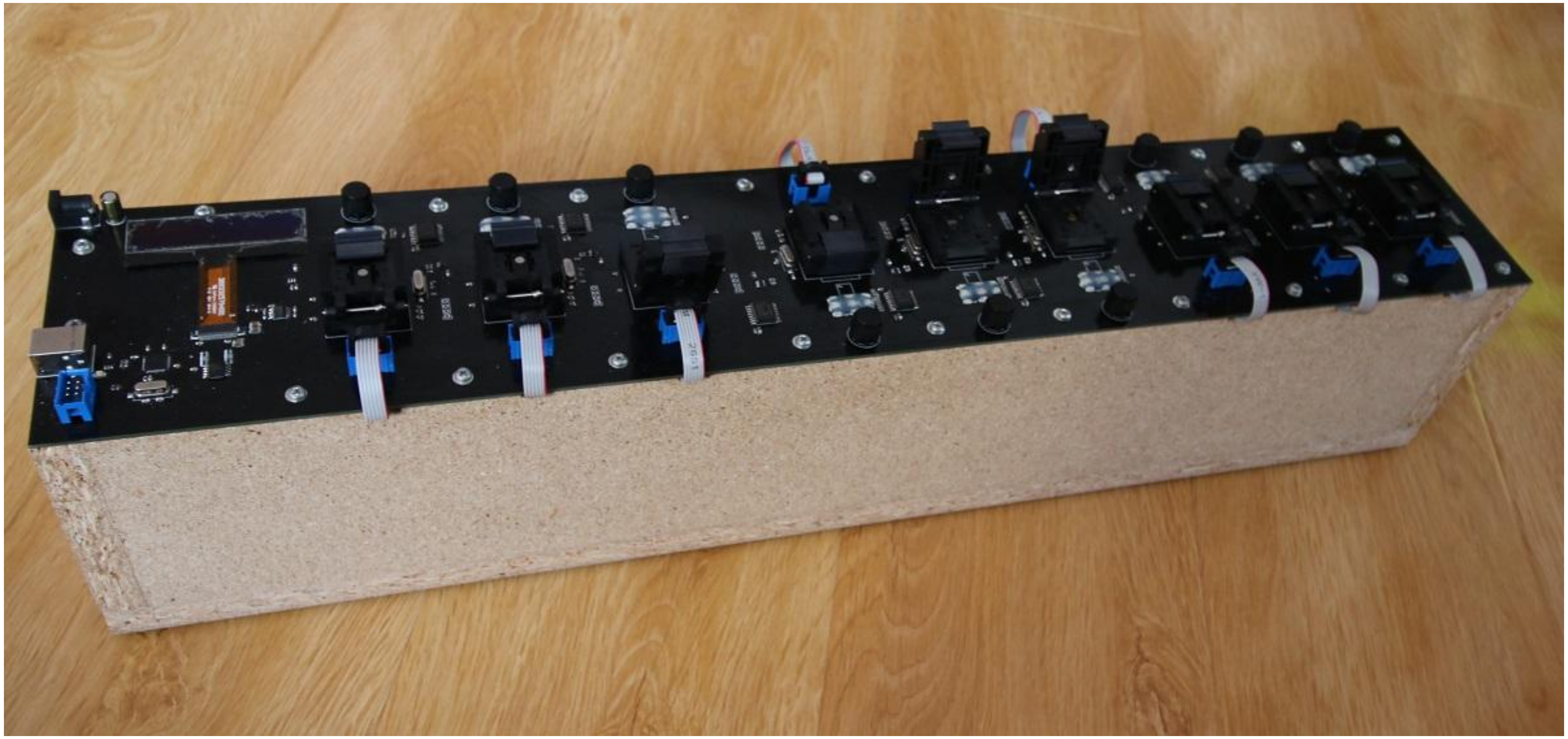
Firmware - Graphics Library

- Designed from the ground up
- Optimized for speed
- Features:
    - RLE compression for bitmaps
    - Bitmaps, fonts stored inside the external flash
    - Python scripts to generate the graphics bundle
    - Can be updated securely

Firmware - Bootloader

- Signed firmware updates
- Stored on the device:
    - One unique AES key for firmware signing
    - One unique AES key for hash generation
    - Read-protected UID for device identification

Flashing the Firmware



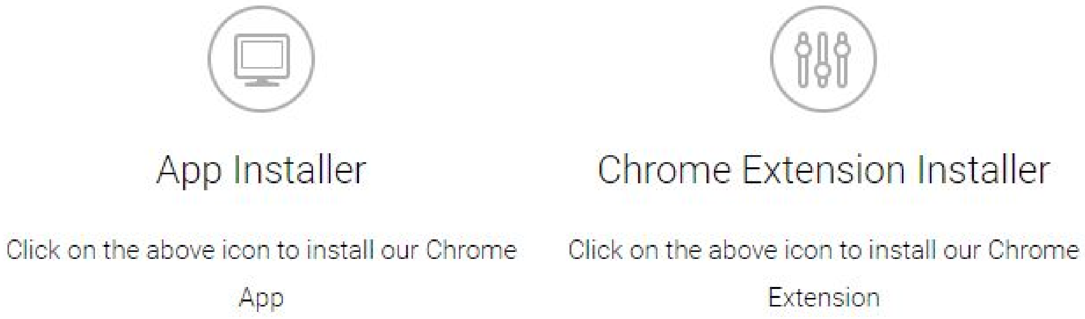
Custom-made programming jig

3.

The Mooltipass Software

Chrome App & Extension

- Cross-platform
- Two-click installation:



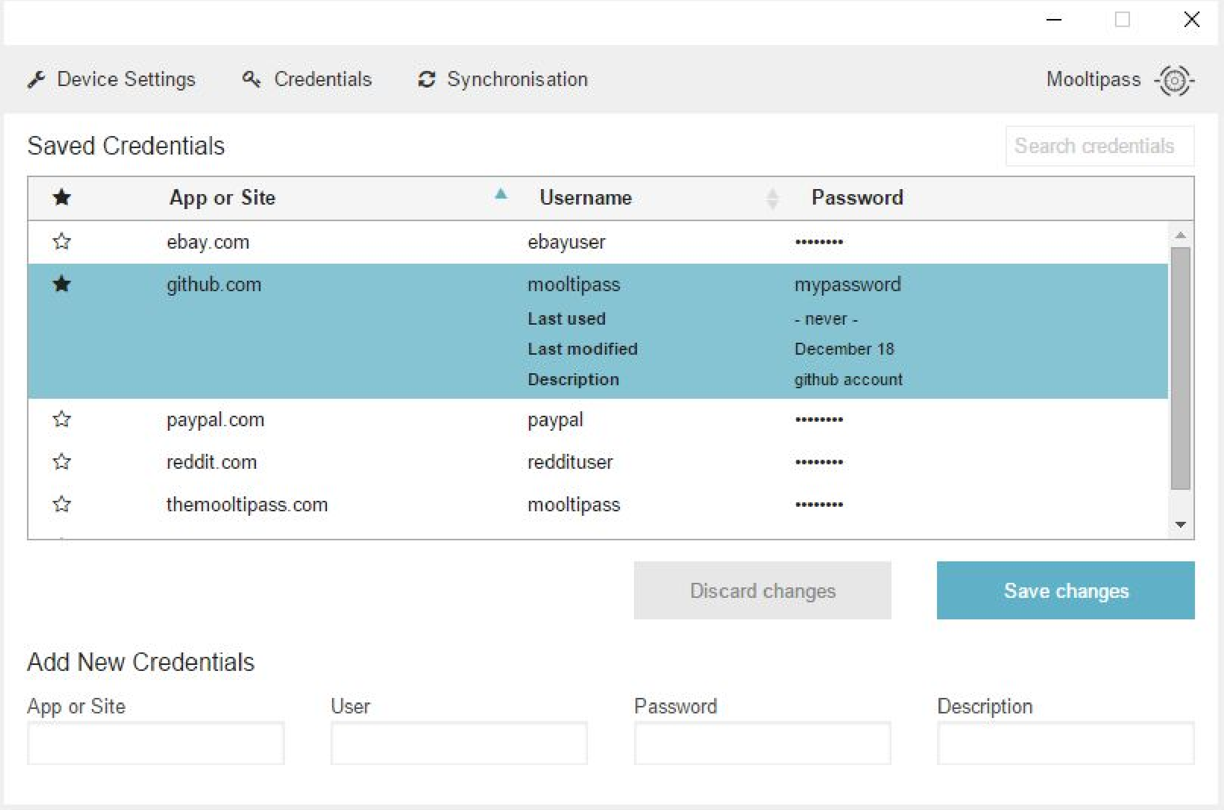
App Installer

Click on the above icon to install our Chrome App

Chrome Extension Installer

Click on the above icon to install our Chrome Extension

Chrome App & Extension



Saved Credentials

★	App or Site	Username	Password
☆	ebay.com	ebayuser	••••••••
★	github.com	mooltipass Last used Last modified Description	mypassword - never - December 18 github account
☆	paypal.com	paypal	••••••••
☆	reddit.com	reddituser	••••••••
☆	themooltipass.com	mooltipass	••••••••

Add New Credentials

App or Site

User

Password

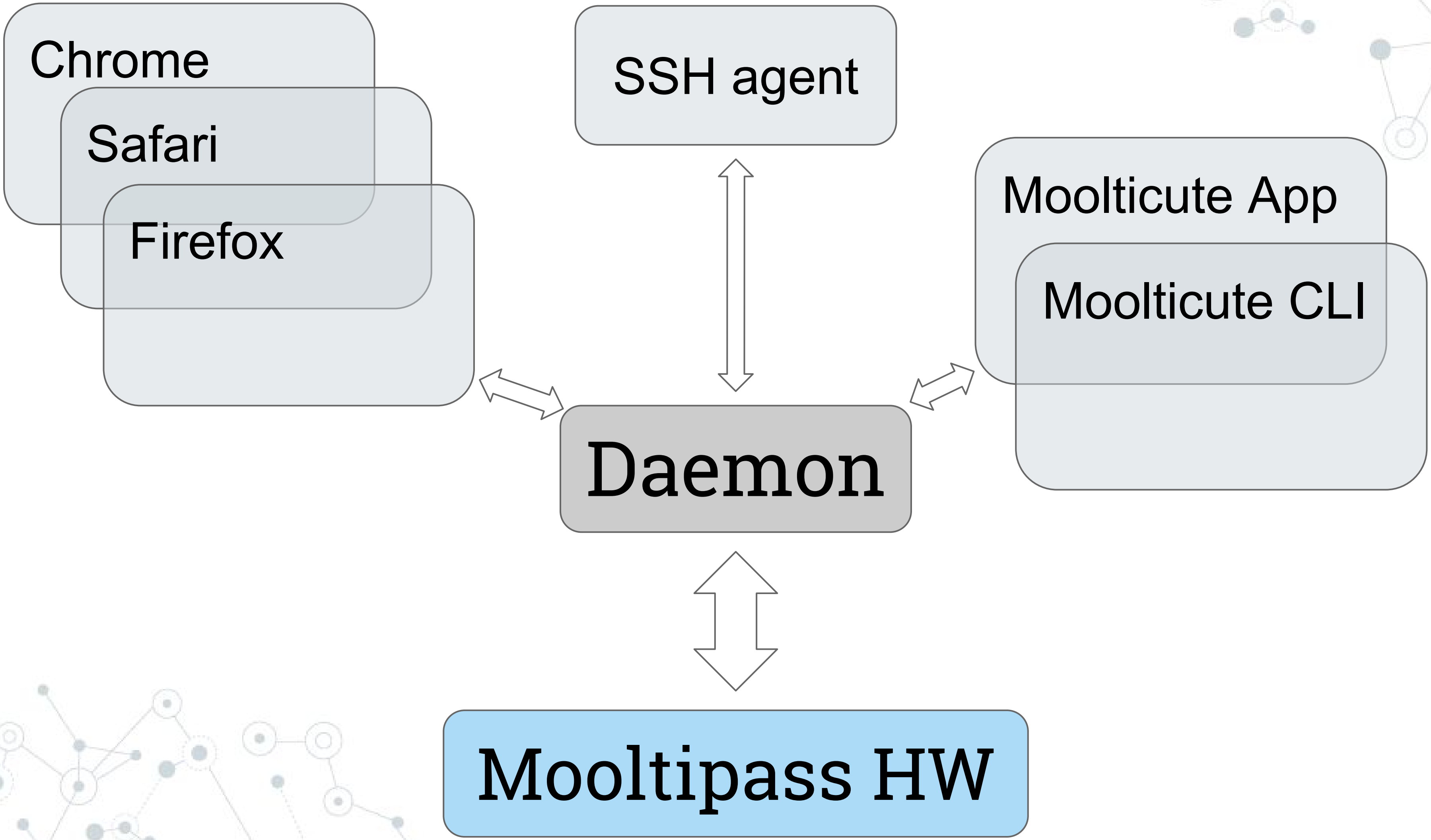
Description

Mooltipass Chrome app

Python Tool - MooltiPy

- Can use all Mooltipass features
- Pure CLI
- Can be called from other apps
- Store / recall small files

Cross Platform Tool - Moolticute



The future of Mooltipass: You!

- Implement native support for applications
- Implement small file storage on Moolticute
- Improve Moolticute Qt GUI
- Create 2FA-only firmware
- Spread the word!

Thanks!

Questions?

You can find me at:
limpkin on freenode.net
mathieu@themooltipass.com