



The Making of a Secure Open Source Password Keeper

... from the electronics to the high-level software

Mathieu Stephan

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
- Multiple users
- Cross platform
- 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



Usage Example



Presentation Outline

A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow with a grey outline. The connections form a complex, interconnected web.

Here's how...

... this adventure started

... 20 people collaborated without meeting each other

... we produced two devices from the ground up

... we created the Mooltipass security model

... the Mooltipass hard-, firm- and software was designed

...and what's next!

A decorative network diagram in the bottom left corner, similar to the one in the top right, showing a complex web of interconnected nodes and lines.



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

A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow with a grey outline. The connections form a complex, interconnected web.

- 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
- 
- A decorative network diagram in the bottom left corner, similar to the one in the top right, featuring a cluster of nodes and connecting lines.


Group Communications



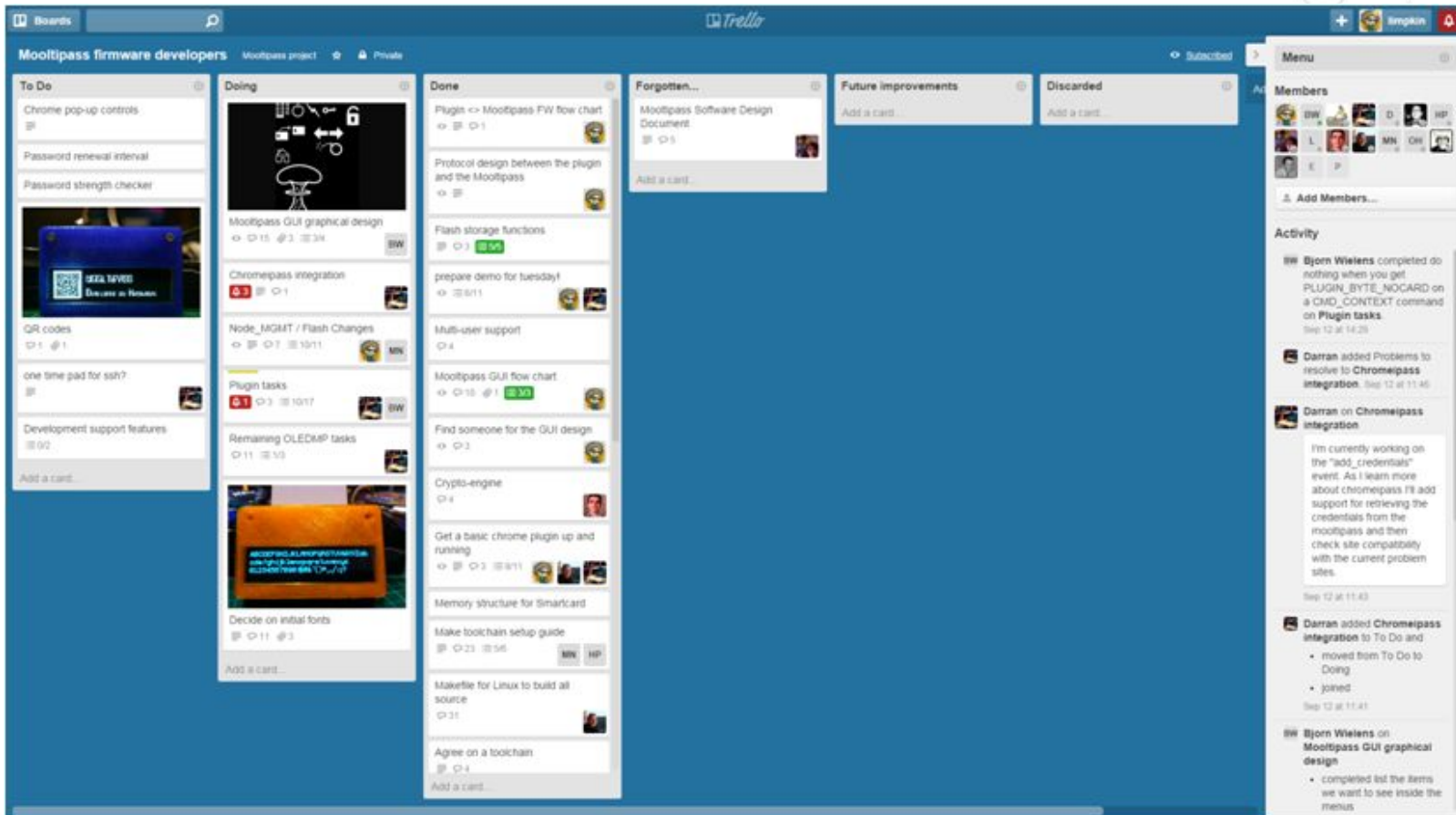
Constraint: people have different availabilities!

- 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
- 

Management Infrastructure



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

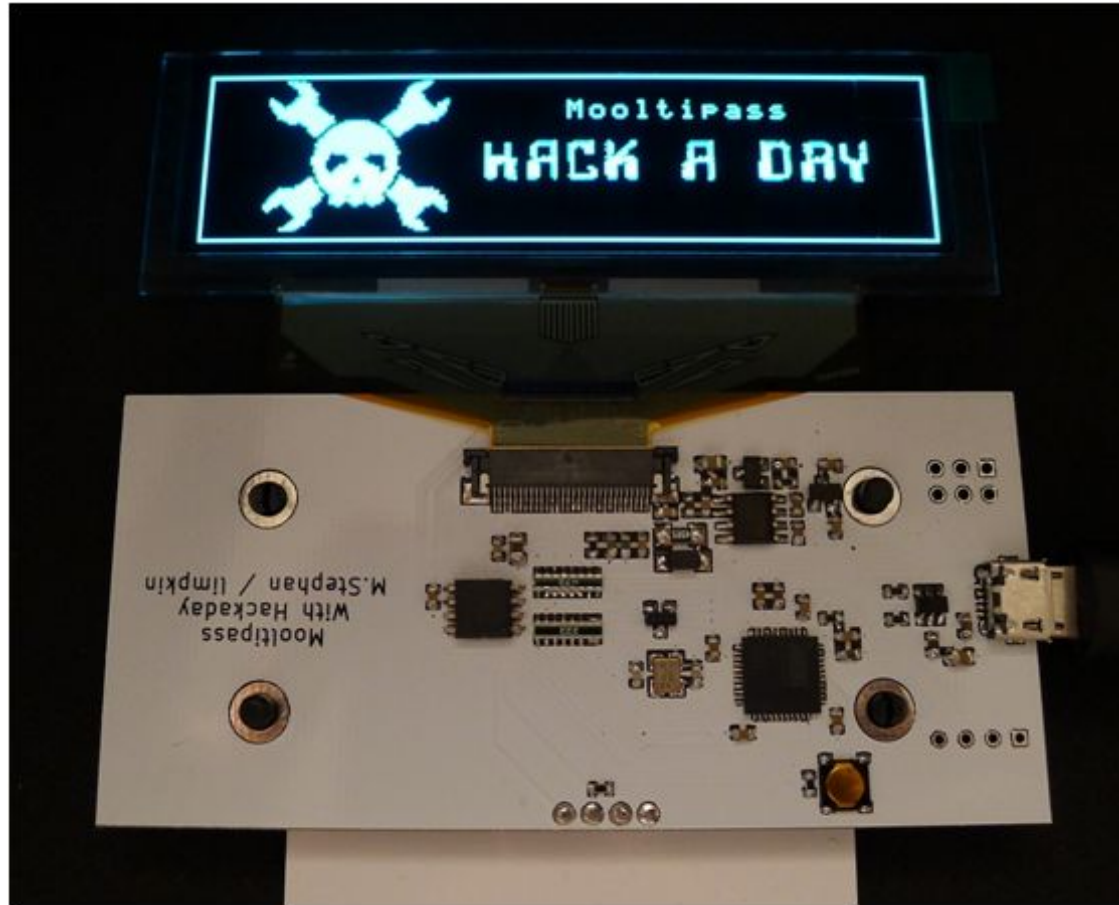


2.

The Mooltipass Hardware



Functional Prototype



Hand soldered and shipped to contributors

Mooltipass - Case Choice



Designs made by the community

Mooltipass - Final Design



110% funded in Dec. 2014

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



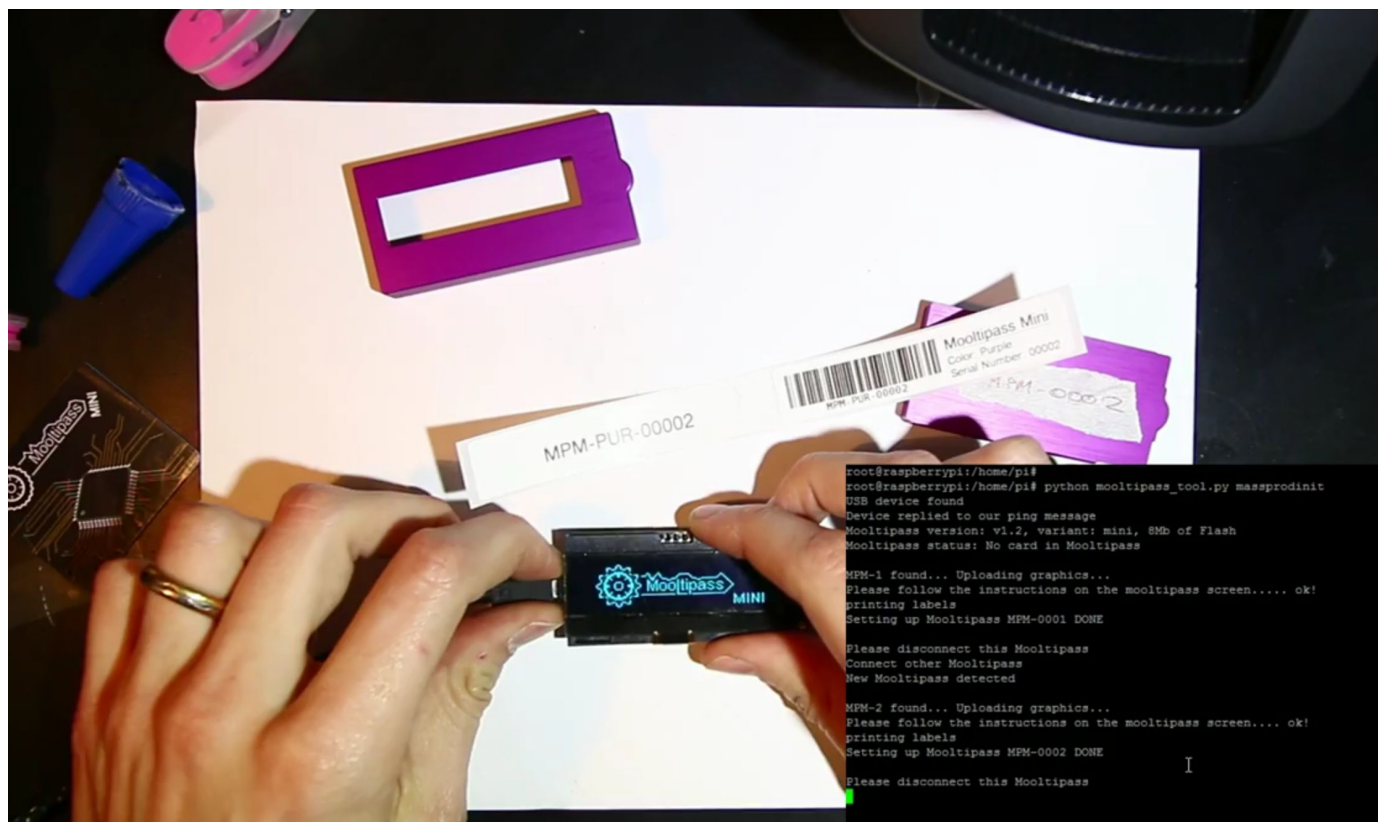
Chinese assembly lines

Mooltipass Mass Production



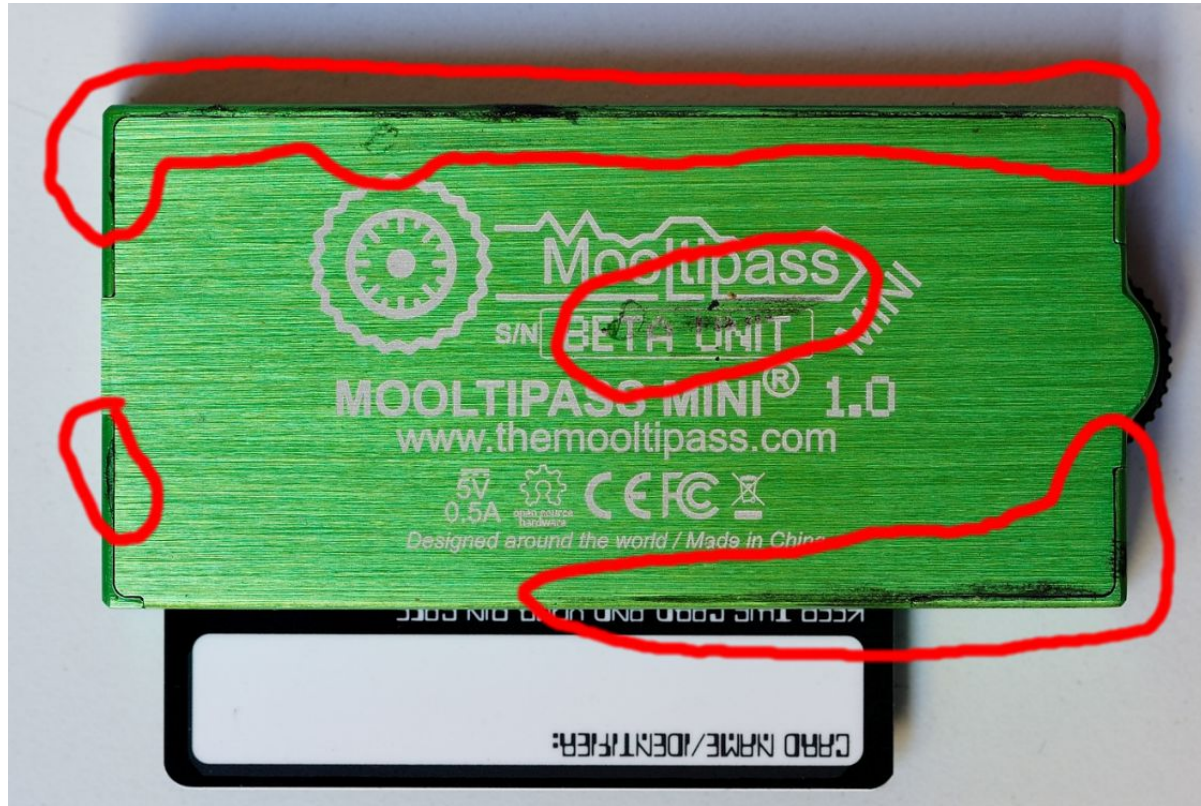
CNC shops

Mooltipass Mass Production



Video instructions for the assembler

Mooltipass Mass Production



... and a lengthy quality control document

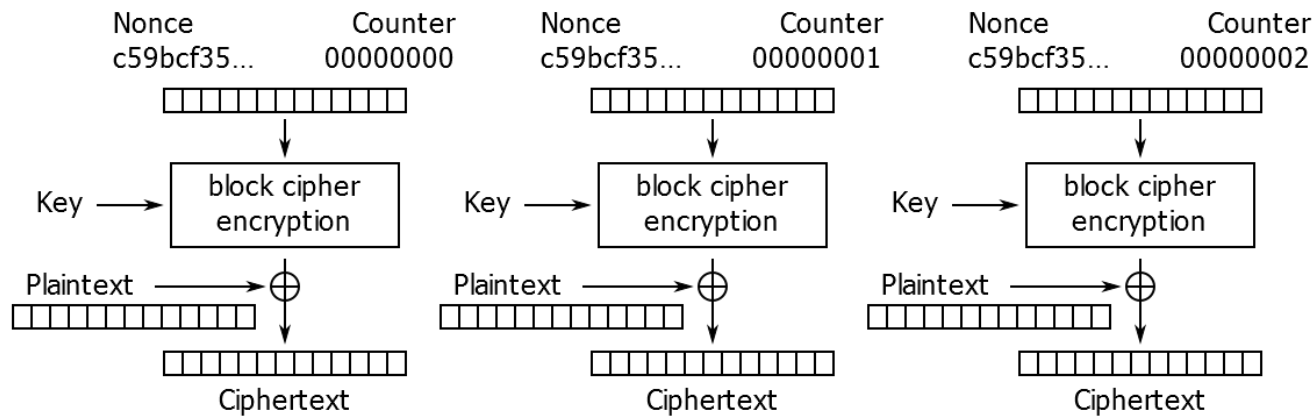


3.

The Mooltipass Firmware

Firmware - AES Encryption

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

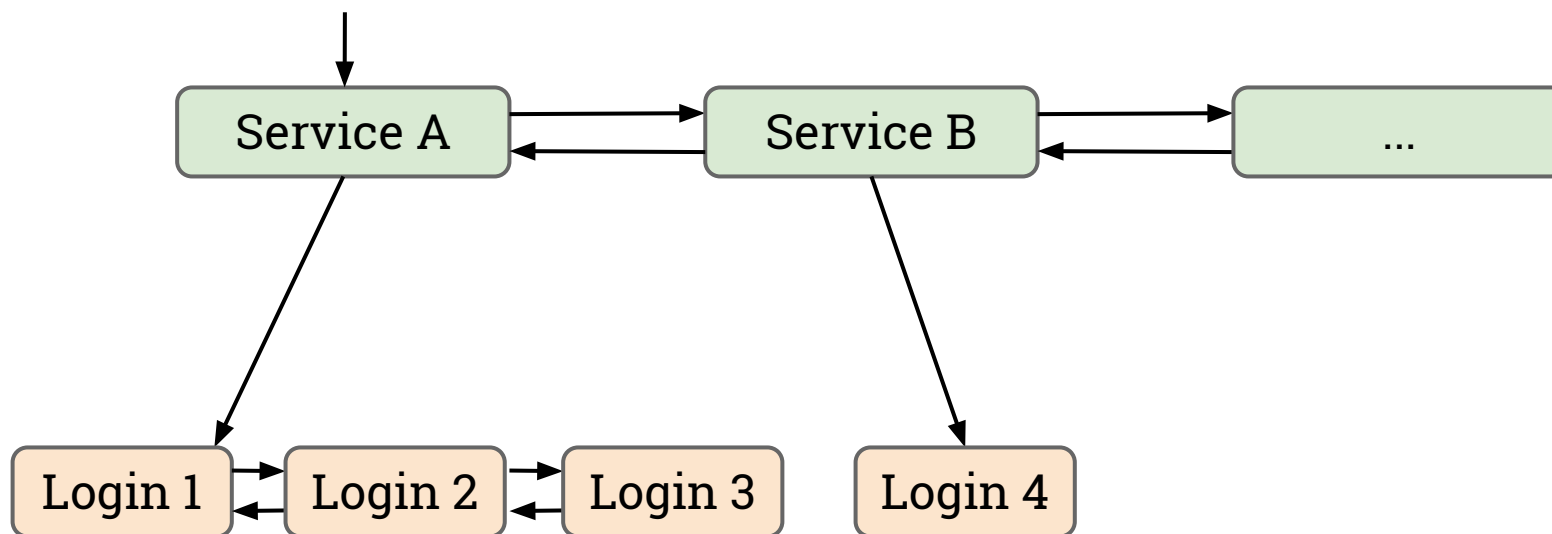


Counter (CTR) mode encryption

Firmware - Encrypted Storage

- Dedicated flash memory used for storage
- 2 types of data
 - Credentials
 - Encrypted blobs
- Sorted linked list data structure

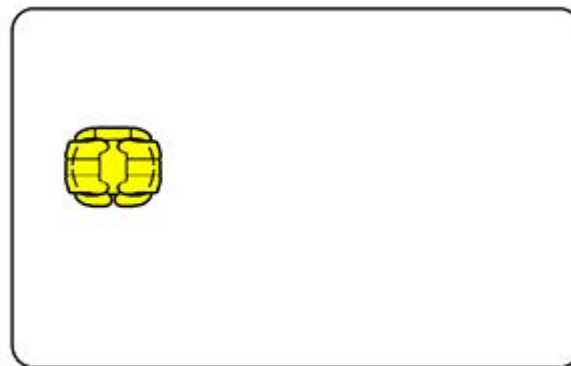
Firmware - Data Structure



Encryption key stored inside the smart card

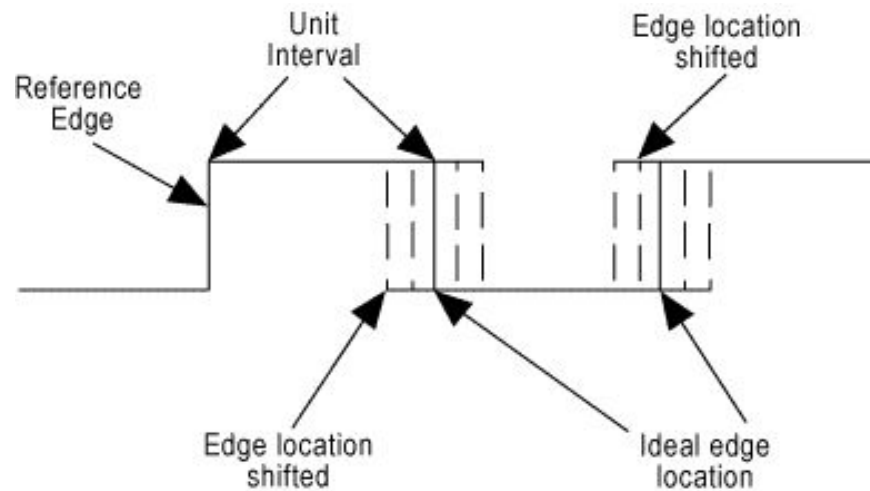
Firmware - Smartcard Use

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



Firmware - RNG

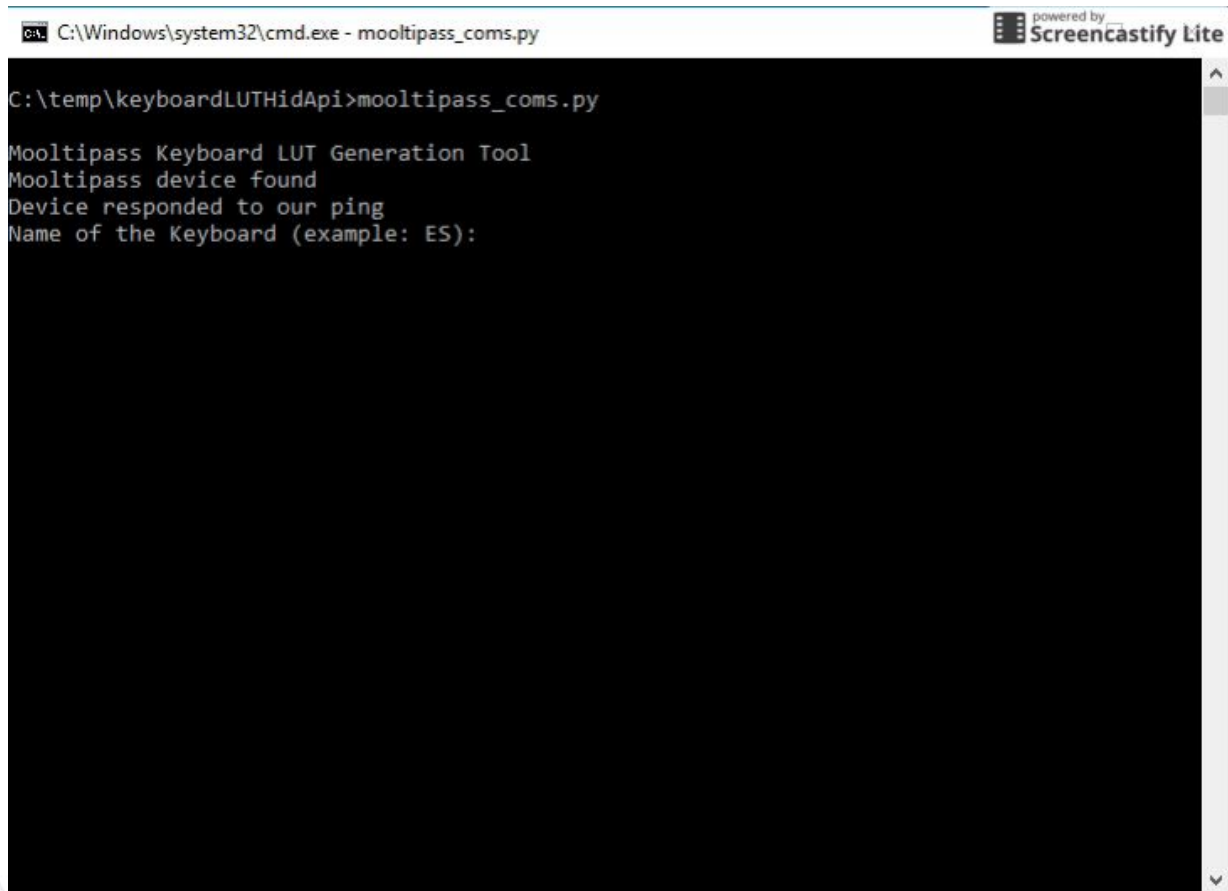
- Uses watchdog timer's natural jitter
- Generate 8 bytes per second (!)



Firmware - USB

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

Firmware - LUT Generation Tool



```
C:\Windows\system32\cmd.exe - mooltipass_comms.py
powered by
Screencastify Lite

C:\temp\keyboardLUTHidApi>mooltipass_comms.py

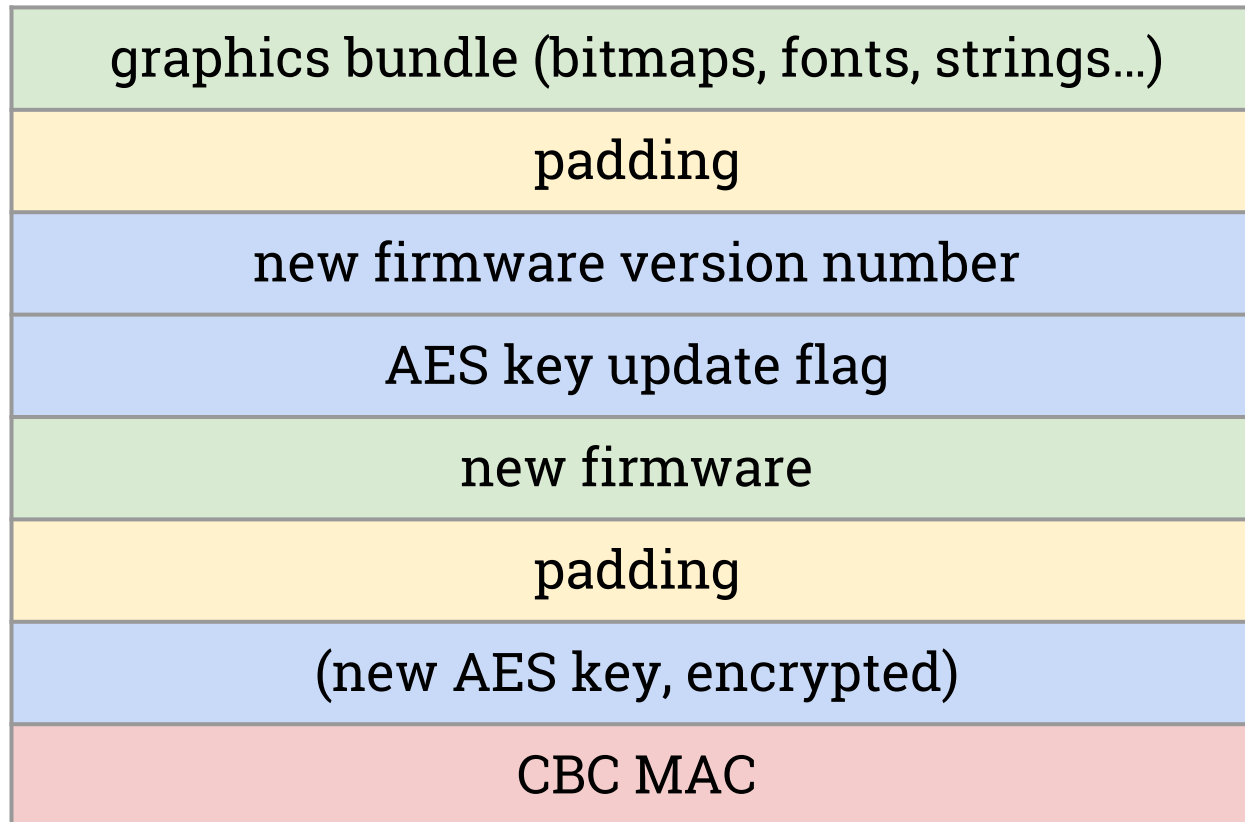
Mooltipass Keyboard LUT Generation Tool
Mooltipass device found
Device responded to our ping
Name of the Keyboard (example: ES):
```

... basically bruteforcing a given layout

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 securely updated

Firmware - Update File Format



Fixed size to mitigate CBC MAC weakness

Firmware - Bootloader

- Checks 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 non-tamper check


Firmware - Security Model

A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow with a grey outline. The connections form a complex, interconnected web.

Relies on the fact that :

- Physical tampering with the device leaves traces
- Microcontroller programming first requires chip erase

Firmware integrity is therefore checked by:

- Reading the read-protected UID at device reception
 - Reading user card-dependent hashes
- 
- A decorative network diagram in the bottom left corner, similar to the one in the top right, featuring a cluster of nodes and connecting lines.

Firmware - Static Analyses

- Performed by security groups, researchers...

Polyspace bugfinder / codeprover results									
Automatically generated report		commit id: 30e85b210ca33d937682a8234d57139cc620e49							
Severity, status and comment are manually assigned by the reviewer		raw results: https://try.blueline.fr/mpm/sca/							
Colored by severity (manual review with code / context knowledge)									
False positives were manually triaged beforehand									
ID	Defect (generated by polyspace)	File	Line	Function	Impact (generated)	Severity (reviewer)	Status (reviewer)	Comment (reviewer)	Detail (generated by polyspace)
33	Dead code	src/CARD_smartcard.c	471	securityValidationSMC()	Low	Low	Investigate	MAT - Not dead code, i is at 0 before the while() so it could still be at 0	If-condition always evaluates to false. Dead branch from line 472 to line 474.
32	Dead code	src/CARD_smartcard.c	471	securityValidationSMC()	Low	Low	Investigate	MAT - See above	If-condition always evaluates to true. Dead branch at line 475.
84	Dead code	src/CARD_smartcard.c	689	firstDetectFunctionSMC()	Low	Low	Investigate	MAT - I agree, will be optimized away though	Default clause of switch at line 682 is dead.
62	Unsigned integer conversion overflow	src/FLASH_flash_mem.c	62	fillPageReadWriteEraseOpcodeFromAd	Low	Low	Investigate	MAT - It's the purpose of the operation: truncating	Conversion from unsigned int16 to unsigned int8 overflows. Valid range: [0 .. 255]
63	Unsigned integer conversion overflow	src/FLASH_flash_mem.c	63	fillPageReadWriteEraseOpcodeFromAd	Low	Low	Investigate	MAT - See above	Conversion from unsigned int16 to unsigned int8 may overflow. Valid range: [0 .. 255]
65	Possible misuse of sizeof	src/FLASH_flash_mem.c	86	sendDataToFlashWithFourBytesOpcode	High	Not a defect	-	MAT - I don't see any sizeof...	Loop boundary is always 1 based on sizeof(array cell)/sizeof(cell type)
61	Non-initialized variable	src/FLASH_flash_mem.c	135	checkFlashID()	High	Not a defect	-	MAT - Not initialized because filled by spi routine	Element of local array is read before being initialized.
60	Non-initialized variable	src/FLASH_flash_mem.c	135	checkFlashID()	High	Not a defect	-	MAT - See above	Element of local array is read before being initialized.
64	Unsigned integer conversion overflow	src/FLASH_flash_mem.c	203	sectorErase()	Low	Low	Investigate	MAT - It's the purpose of the operation: truncating	Conversion from unsigned int16 to unsigned int8 overflows. Valid range: [0 .. 255]
59	Unsigned integer conversion overflow	src/FLASH_flash_mem.c	244	blockErase()	Low	Low	Investigate	MAT - It's the purpose of the operation: truncating	Conversion from unsigned int16 to unsigned int8 overflows. Valid range: [0 .. 255]
5	Vulnerable pseudo-random number generator	src/FLASH_flash_test.c	76	initBuffer()	Medium	Not a defect	-	MAT - I don't see an initBuffer();	rand() is a cryptographically weak PRNG. To make your program more secure, use 'CryptGenRandom' (V)
13	Write without a further read	src/GUI_mini_gui_basic_functions.c	210	miniTextEntry()	Low	Low	Investigate	GUI_mini_gui_basic_functions.c L210	Variable 'filled_tes' is never read after this point.
71	Sign change integer conversion overflow	src/GUI_mini_gui_basic_functions.c	423	miniTextEntry()	Medium	Not a defect	Justified	intended behavior GUI_mini_gui_basic_functions.c L423	Conversion from int16 to unsigned int16 may overflow. Valid range: [0 .. 65535]
72	Dead code	src/GUI_mini_gui_credentials_functions.c	274	guiAskForLoginSelect()	Low	Not a defect	-	MAT - No it is not: https://github.com/lampkin/mooltipass/blob/master/source_code/src/USB/usd_cmd_parser.c#L173	If-condition always evaluates to false. Dead branch from line 275 to line 277.
14	Array access out of bounds	src/GUI_mini_gui_credentials_functions.c	376	favoriteSelectionScreen()	High	Not a defect	Justified	MAT - Yes, exactly why I added that #pragma... the data behind it supports it	Attempt to access to array element -1. Valid index range: [0 .. 62].
16	Write without a further read	src/GUI_mini_gui_pin_functions.c	193	guiGetPinFromUser()	Low	Not a defect	Justified	MAT - yup, we want to erase the pin buffer	Variable 'current_pin' is never read after this point.
15	Write without a further read	src/GUI_mini_gui_pin_functions.c	229	guiCardUnlockingProcess()	Low	Not a defect	Justified	MAT - See above	Variable 'temp_pin' is never read after this point.
19	Write without a further read	src/GUI_mini_gui_pin_functions.c	276	guiScreenLoop()	Low	Not a defect	Justified	MAT - See above	Variable 'pin_code' is never read after this point.
18	Write without a further read	src/GUI_mini_gui_pin_functions.c	308	guiScreenLoop()	Low	Not a defect	Justified	MAT - See above	Variable 'pin_code' is never read after this point.
73	Array access out of bounds	src/GUI_mini_gui_screen_functions.c	574	guiAskForConfirmation()	High	Low	Improve	MAT - We could indeed cap nb_args to 3, but given this arg is never provided from the outside world I doubt it's useful and is easily detected	Attempt to access to array element in range. Valid index range: [0 .. 3].
74	Array access out of bounds	src/GUI_mini_gui_screen_functions.c	574	guiAskForConfirmation()	High	Low	Improve	MAT - See above	Attempt to access to array element in range. Valid index range: [0 .. 2].
66	Use of dangerous standard function	src/LOGIC_logic_aes_and_comms.c	595	getLoginForContext()	Low	High	Justified	MAT - intended behaviour, see comment "Read selected child node, guaranteed to be null terminated by readchildnode function"	Using 'strcpy' can cause the destination buffer to overflow. The output length depends on unknown val
67	Dead code	src/LOGIC_logic_aes_and_comms.c	862	setPasswordForContext()	Low	Low	Improve	MAT - VALID, can be removed	If-condition always evaluates to false. Dead branch from line 863 to line 865.
6	Useless if	src/LOGIC_logic_aes_and_comms.c	1366	loginSelectLogic()	Medium	Low	Investigate	MAT - VALID, else if (state_machine == 2) can be changed to else	Unnecessary code, if-condition is always true.
		src/LOGIC_logic_aes_and_comms.c	197	searchForServiceName()	-	-	Investigate	compare_result (int8) is assigned strcpy, an int16 value / MAT - truncating isn't a problem when only -1 / 0 / 1 are returned	
68	Non-initialized variable	src/LOGIC_logic_eeprom.c	-	setMockI2cPassParameterInEeprom()	High	Not a defect	-	MAT - I'm not sure what's that's all about	Parameter 'val' may be read before being initialized.
2	Pointer or reference to stack variable leaving scope	src/LOGIC_logic_smartcard.c	49	unlockFeatureCheck()	High	Not a defect	Justified	MAT - by design	Address of local memory logicStrng escapes from its scope through conf_text[line]
7	Write without a further read	src/LOGIC_logic_smartcard.c	140	handleSmartcardInserted()	Low	Not a defect	Justified	MAT - yup, we want to erase the pin buffer	Variable 'pin_code' is never read after this point.
70	Sign change integer conversion overflow	src/LOGIC_logic_smartcard.c	153	handleSmartcardInserted()	Medium	Low	Fix	MAT - VALID, BUT checks are only for the positive values: RETURN_VCARD_OK = 0, RETURN_VCARD_UNKNOWN = 1	Conversion from int8 to unsigned int8 may overflow. Valid range: [0 .. 255]
78	Pointer access out of bounds	src/NODEMGMT_node_mgmt.c	911	populateServiceList()	High	Low	Justified	MAT - pNode is 9 bytes buffer and pNode_ptr-service[0] is at address 8 : https://github.com/lampkin/mooltipass/blob/30e85b210ca33d937682a8234d57139cc620e49	Attempt to dereference pointer outside its bounds.
79	Dead code	src/NODEMGMT_node_mgmt.c	1193	updateChildNode()	Low	Low	Improve	MAT - VALID, can be removed - but this code was removed in latest commits	If-condition always evaluates to false. Dead branch from line 1194 to line 1196.

- We had access to some of them...

Flashing the Firmware



Custom-made programming jig



4.

The Mooltipass Software



Python Tool - MooltiPy

Created by one contributor:

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

Chrome App & Extension

- Cross-platform
- Unfortunately Chrome-only
- Two-click installation:



App Installer

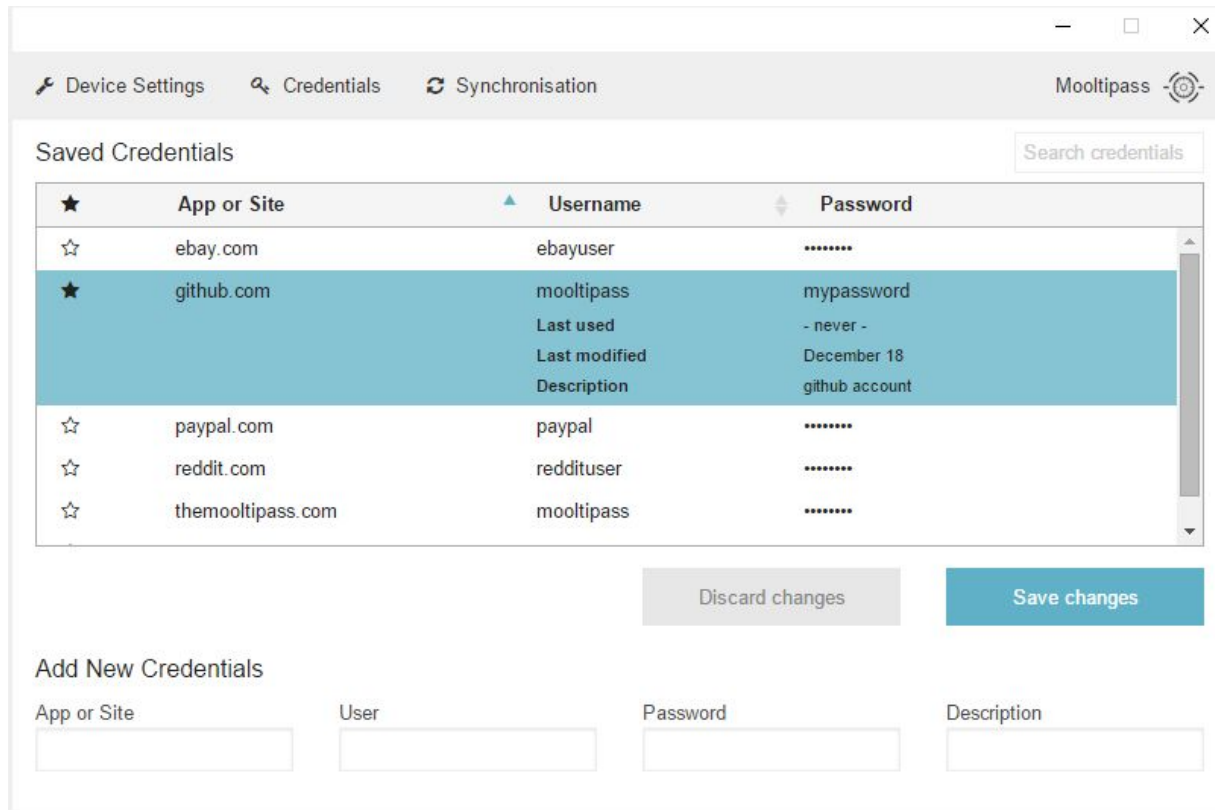
Click on the above icon to install our Chrome
App



Chrome Extension Installer

Click on the above icon to install our Chrome
Extension

Chrome App - MooltiApp



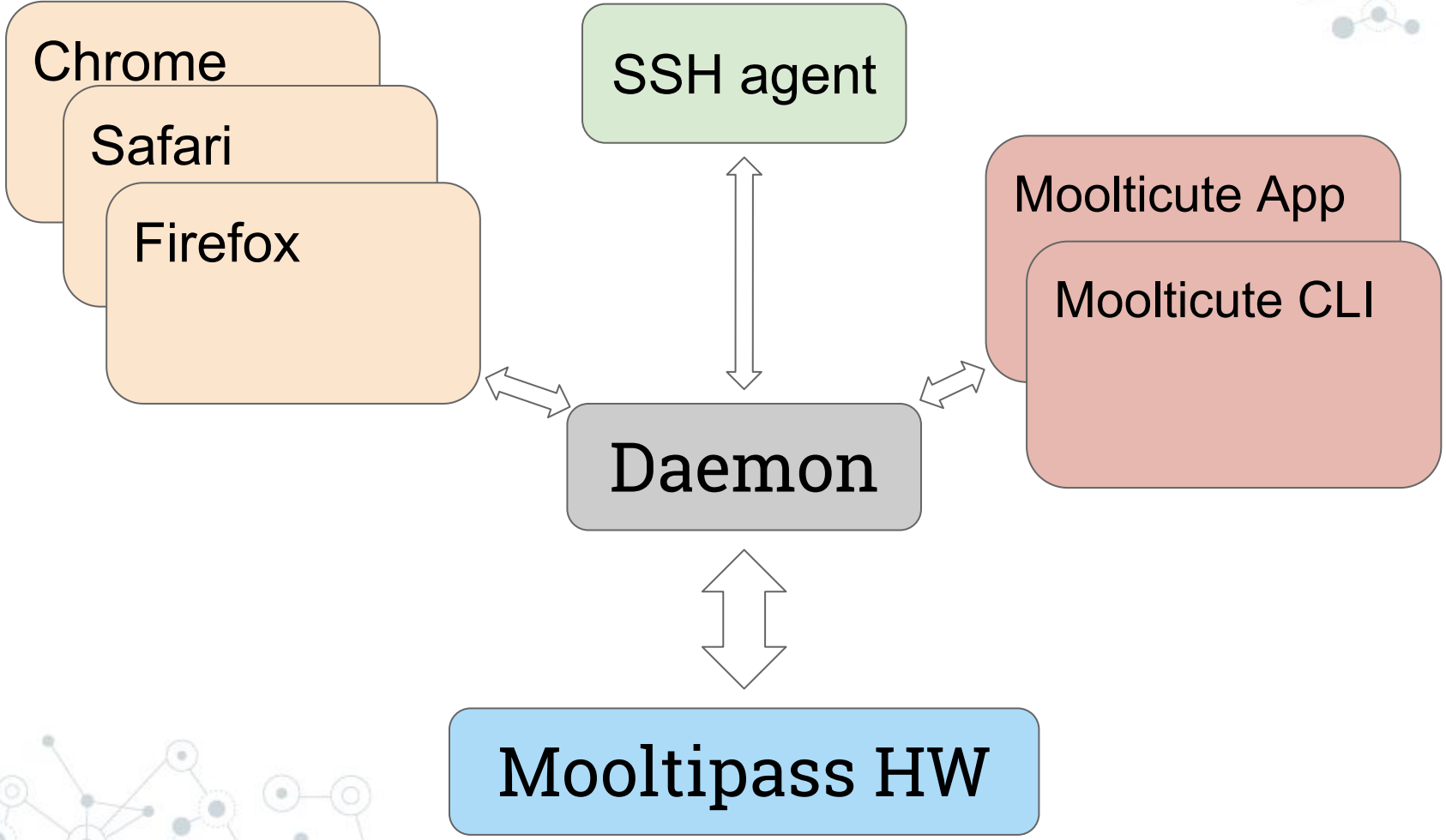
The screenshot displays the Mooltipass Chrome App interface. At the top, there are navigation options: Device Settings, Credentials, and Synchronisation. The main content area is titled "Saved Credentials" and features a search bar labeled "Search credentials". Below this is a table of saved credentials:

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

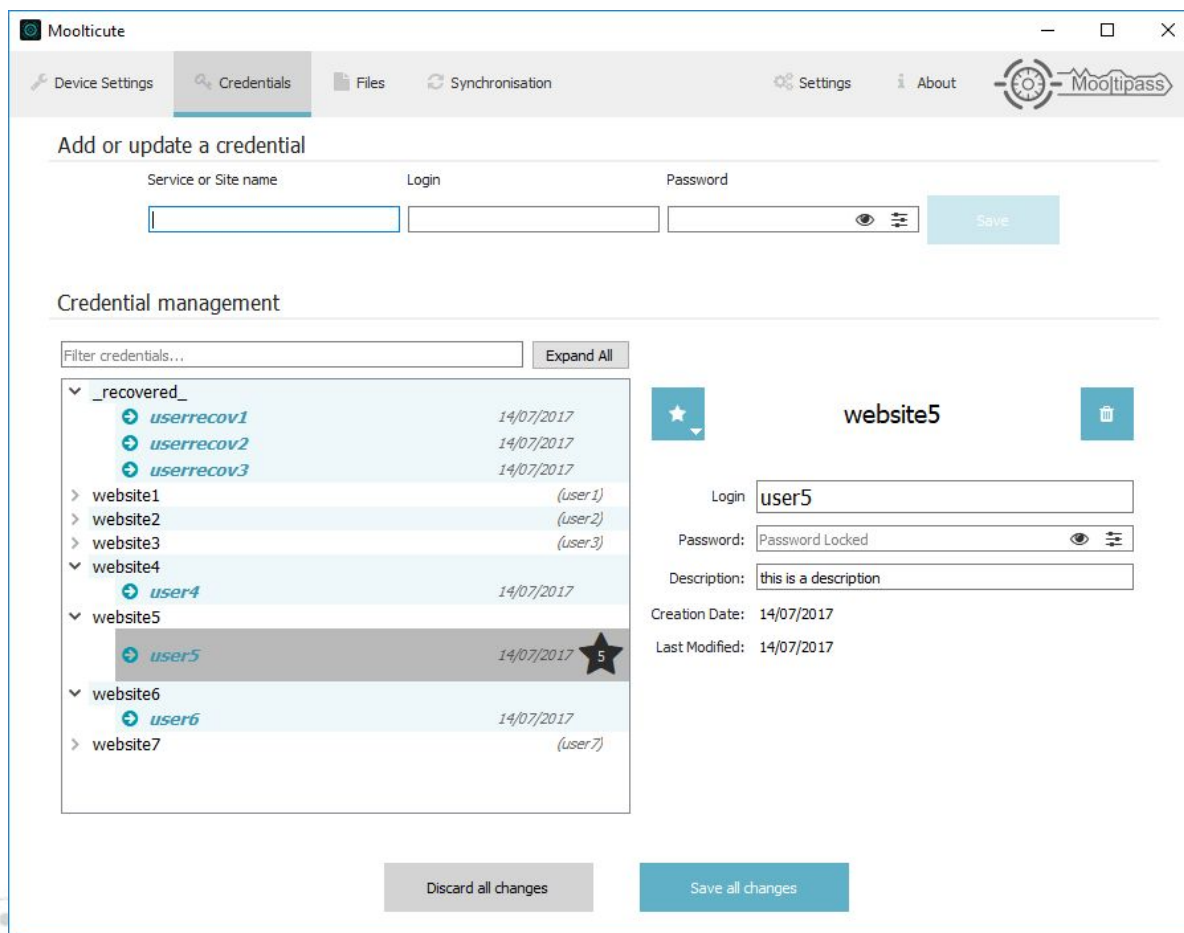
Below the table, there are two buttons: "Discard changes" and "Save changes". At the bottom, there is a section for "Add New Credentials" with four input fields: "App or Site", "User", "Password", and "Description".

...converted into a standalone App using Electron

Cross Platform Tool - Moolticute

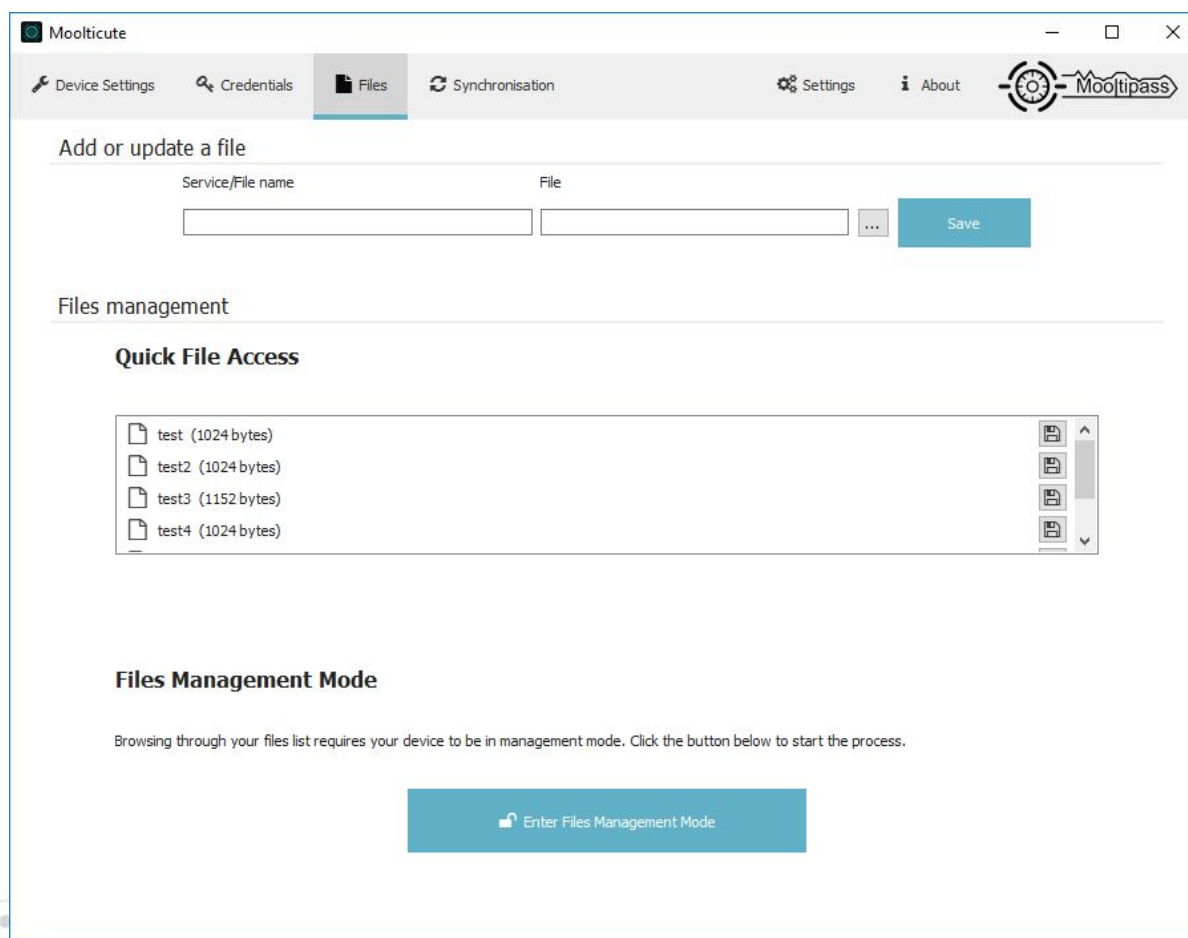


Cross Platform Tool - Moolticute



Qt & C++ - Created by a contributor

Cross Platform Tool - Moolticute



... and now being developed by the Mooltipass team

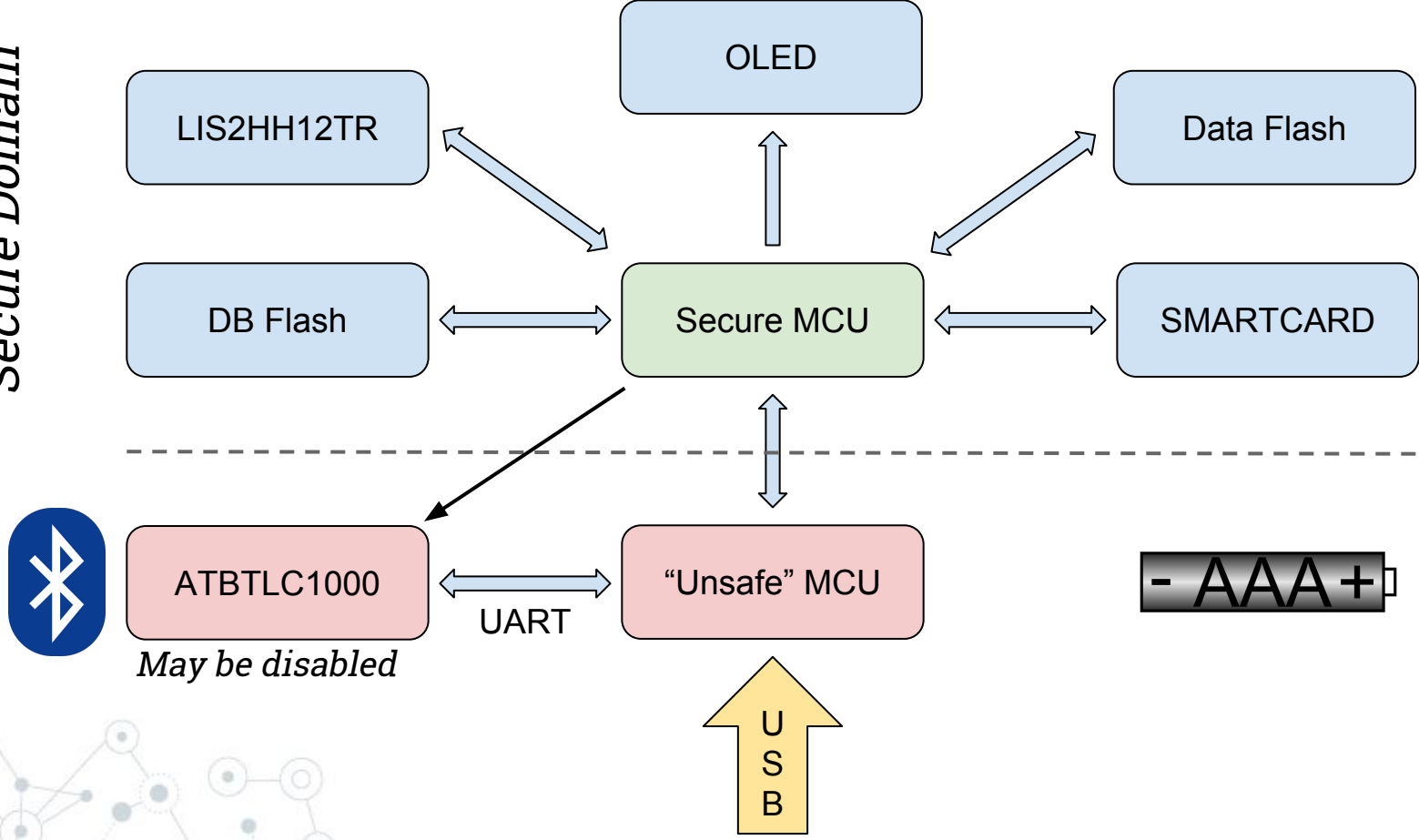


4.

The Next Mooltipass Device!

Next Generation Mini

Secure Domain



Contributors Wanted!

Firmware:

- New database model implementation
- Unicode support implementation
- Bootloader implementation
- User interface design
- U2F implementation
- < your idea[s] here >



Contributors Wanted!

- C++ & QT: frontend for the new firmware features
- Web: implement a user space on mooltipass.com
- Python: security implementation checks
- GIMP: create Mooltipass graphics
- Android & iOS: App development





Thanks!

Questions?

You can find me at:

limpkin on freenode.net

mathieu@themooltipass.com

