AYKIT

Verein zur Förderung viel zu großer Logos

FAST TRACK:

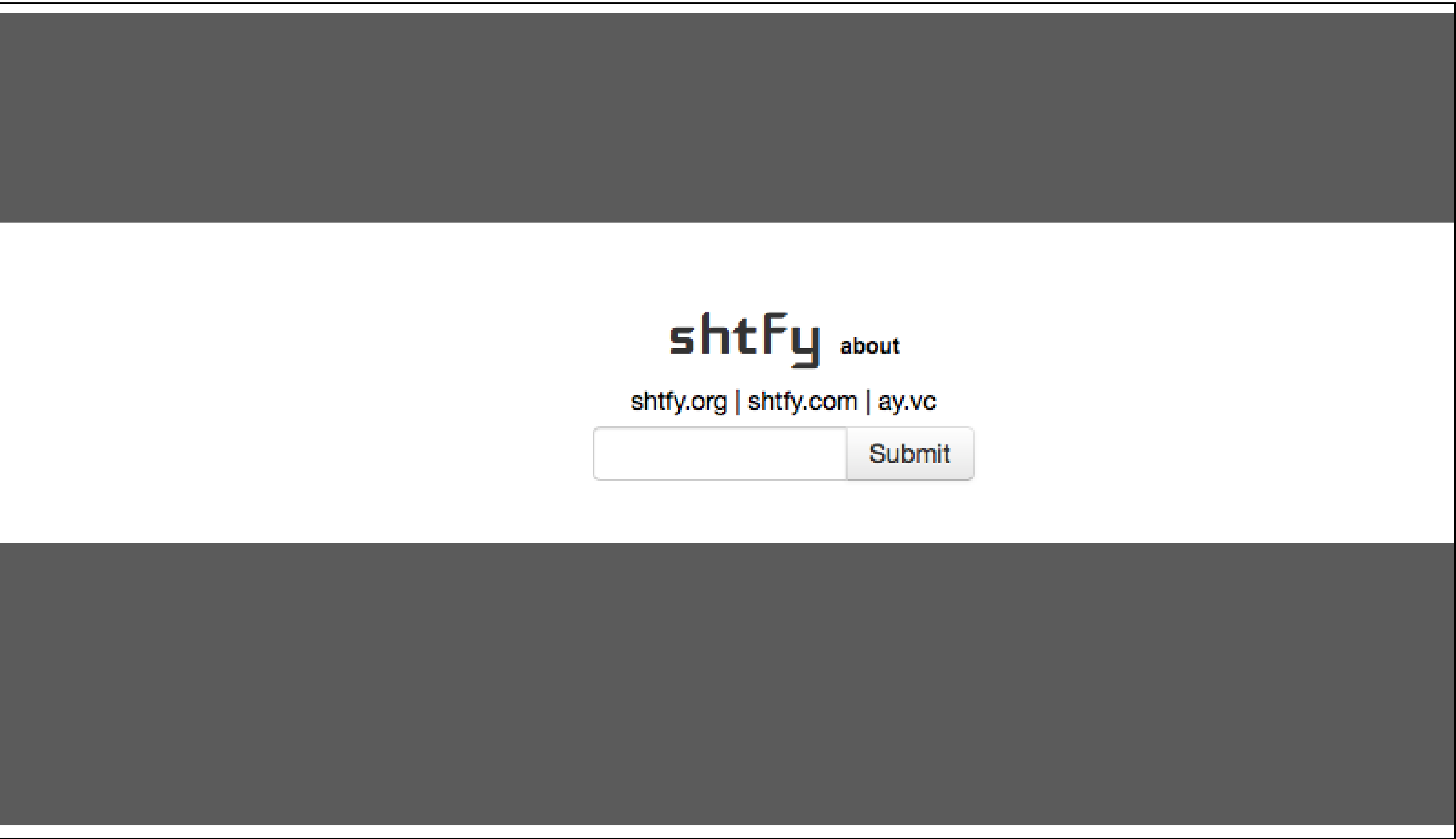
cat

RFC 4226 - HOTP
RFC 6238 - TOTP
RFC 2104 - HMAC

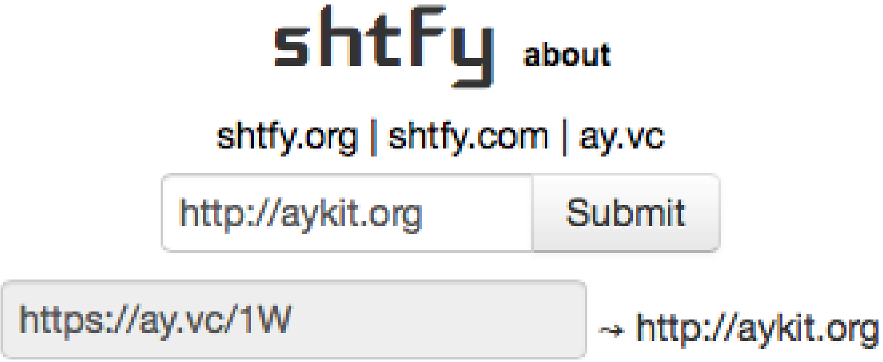
echo

THE END

AYKIT LIKES SHTFY



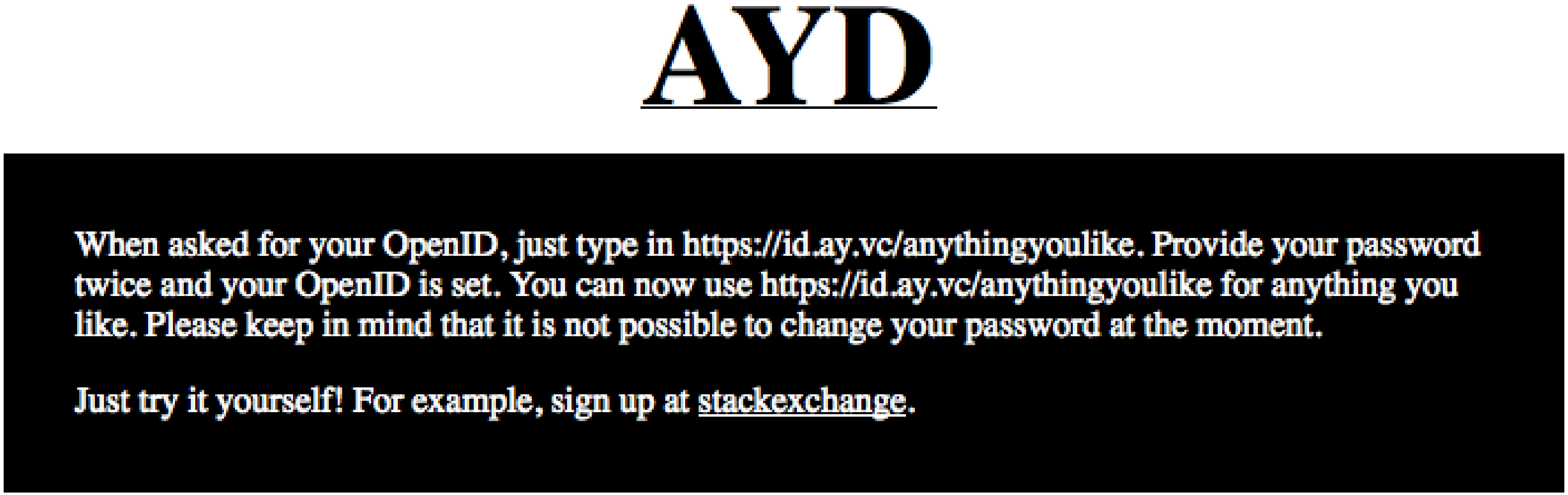
AYKIT LIKES SHTFY



http://aykit.org

https://ay.vc/1W → http://aykit.org

AYKIT LIKES AYD

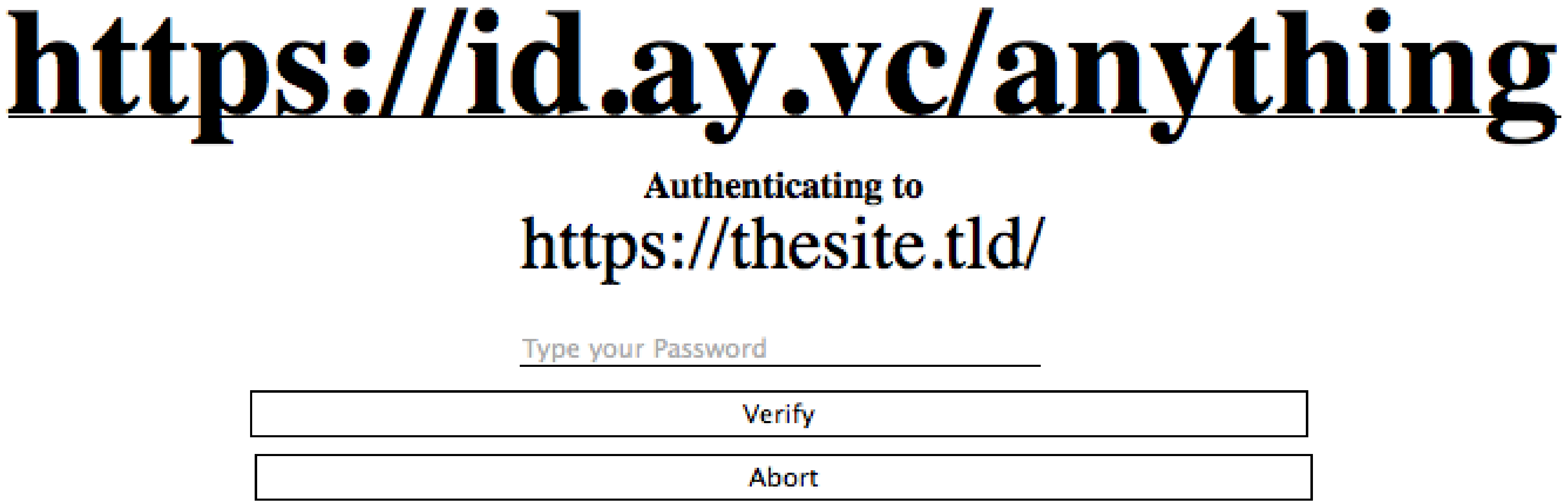


AYD

When asked for your OpenID, just type in https://id.ay.vc/anythingyoulike. Provide your password twice and your OpenID is set. You can now use https://id.ay.vc/anythingyoulike for anything you like. Please keep in mind that it is not possible to change your password at the moment.

Just try it yourself! For example, sign up at stackexchange.

AYKIT LIKES AYD



https://id.ay.vc/anything

Authenticating to

https://thesite.tld/

AYKIT LIKES OWNCLOUD

Manage owncloud notes with “My Own Notes”.

github.com/aykit

(and at the ios/android stores if you want to manage your notes for a good cause)

AYKIT LIKES

THE YESMACHINE

Designing an open hardware cryptographic device

THE YESMACHINE

1. Our goals

2. HOTP or TOTP?

3. What Hardware do we use?

4. What does the software toolchain look like?

5. What’s the status?

AYKIT LIKES GOALS (sometimes)

- Open Hardware/Software security token

- Support HOTP, or even better, TOTP

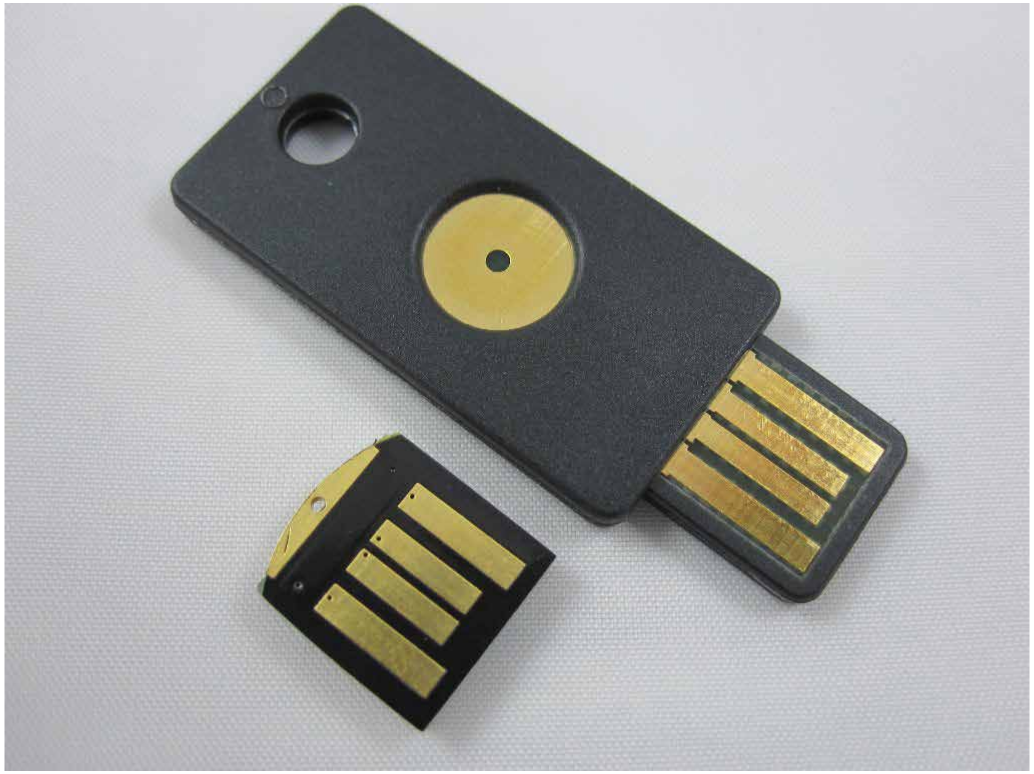
- Most of all: generating and sharing knowledge

AYKIT LIKES GOALS (sometimes)

- Popular architecture: ARM Cortex-M
- Fast enough to do RSA 4096 bit signatures
- Size of stick: as small as possible
- Size of board: self-solderable, 48 pins max.
- Security: Restrict access to keys, MPU

AYKIT LIKES GOALS (sometimes)

And getting rid of those:



AYKIT LIKES HOTP

HOTP:
An HMAC-Based One-Time Password Algorithm

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

AYKIT LIKES HOTP: MAC

Message Authentication Code

Simultaneously verify both the data integrity and the authentication of a message.

MAC = f(message, secret key)

AYKIT LIKES HOTP: HMAC

Specific algorithm for MAC generation

HMAC = hash(key+hash(key+message))

PImp: ay.vc/4X

AYKIT LIKES HOTP

HOTP:
An HMAC-Based One-Time Password Algorithm

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

AYKIT LOVES TOTP

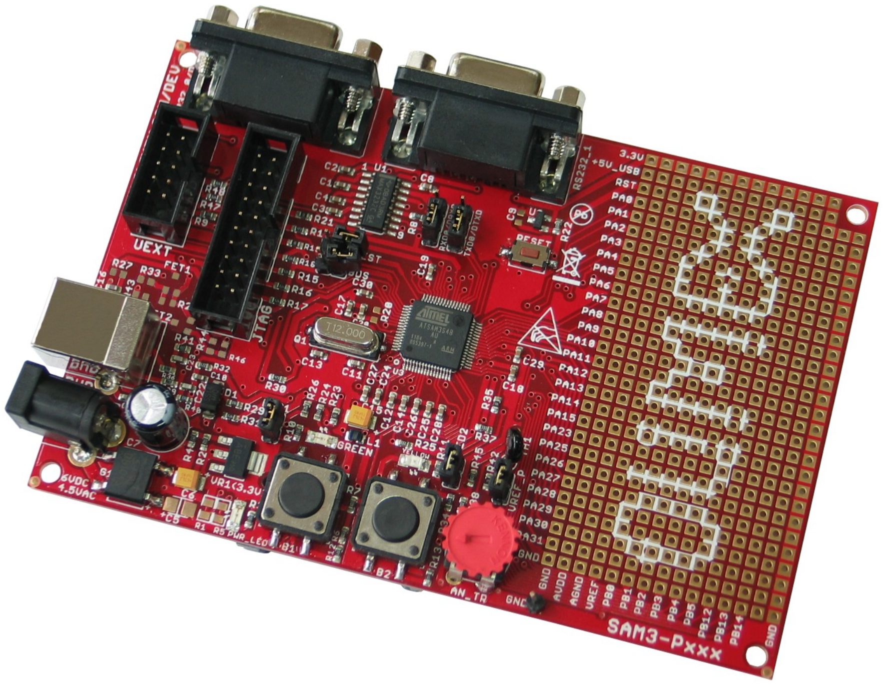
TOTP:
Time-Based One-Time Password Algorithm

HOTP(K,T) = Truncate(HMAC-SHA-1(K,T))

ows SHA-512 ! Allows SHA-512 ! Allows SHA-512! Allows SH

AYKIT LIKES HARDWARE

OLIMEX

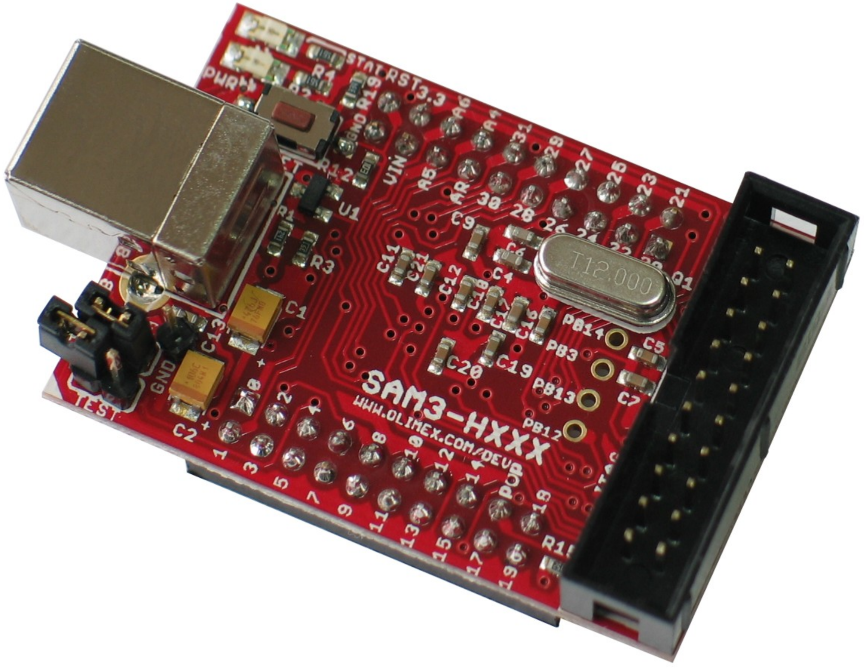


SAM3-P256 development board

SAM3-P256, https://ay.vc/4v

AYKIT LIKES **HARDWARE**

OLIMEX



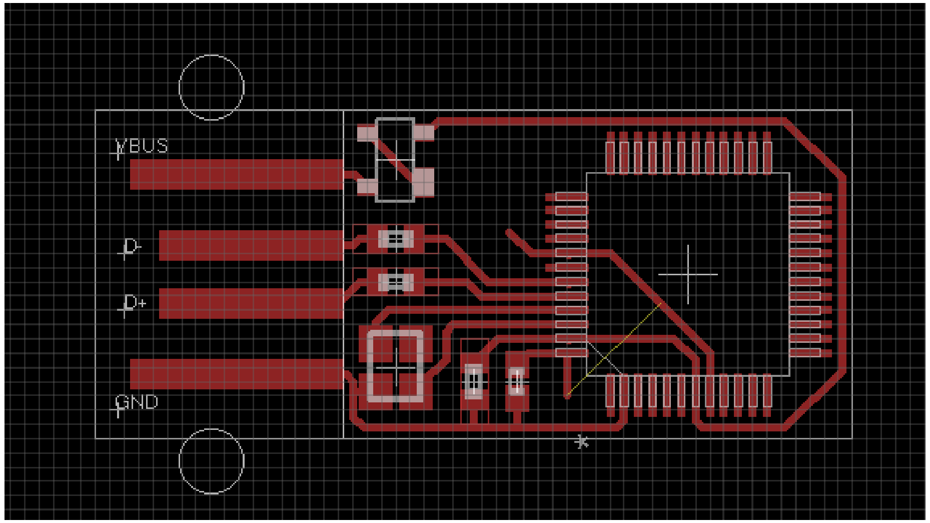
SAM3-H256 development board

SAM3 - H256, https://ay.vc/4Y

AYKIT LIKES HARDWARE

FTDI C232HM-EDHSL-0, https://ay.vc/4Z

AYKIT LIKES HARDWARE



Early board schematic for HOTP (current state)

AYKIT LIKES HARDWARE

max
min
通过ISO9001国际质量管理体系认证
12V 105AH
CHANGJIU
ZHEJIANG ZHENGTONG POWER SUPPIY CO., LTD.

Early board schematic for TOTP (current state)

AYKIT LIKES SOFTWARE

GNU Tools for ARM Embedded Processors

GNU Toolchain for ARM Cortex-M / -R
Dev: ARM
link: https://ay.vc/50

AYKIT LIKES SOFTWARE

Atmel Software Framework

MCU software library for SAM3

Dev: Atmel
Link: https://ay.vc/51

AYKIT LIKES SOFTWARE

Cortex Microcontroller Software Interface Standard

Hardware Abstraction Layer

Dev: ARM
Link: https://ay.vc/52

AYKIT LIKES SOFTWARE

BOSSA

Flashing SAM3 devices

Dev: Shumatech
Link: https://ay.vc/53

AYKIT LIKES SOFTWARE

SCONS

Software Construction Tool, substitutes make

Dev: The SCons Foundation
Link: http://scons.org

AYKIT LIKES SOFTWARE

OpenOCD

On-Chip Debugging (in conjunction with GDB)

Dev: Dominic Rath
Link: https://ay.vc/54

AYKIT LIKES SOFTWARE

GDB

The GNU Project Debugger

Dev: Free Software Foundation
Link: https://ay.vc/55

AYKIT LIKES SOFTWARE

Eclipse

The most used and slowest starting IDE available

Dev: The Eclipse Foundation
Link: http://eclipse.org
Checkout: https://ay.vc/56 for Eclipse with gdb

AYKIT HATES CAVEATS

JTAG via FTDI C232HM-EDHSL-0

See repository for OpenOCD config

AYKIT HATES CAVEATS

Carefully read your specifications and avoid having a bad time:

e.g. what interface to flash device?

AYKIT LIKES FUTURE

Say yes to:

- HOTP
- TOTP
- Passwords
- Private SSH Key
- PKCS#11
- OpenPGP
- OCRA (OATH Challenge-Response Algorithm)

AYKIT LIKES VISITORS

github.com/aykit

github.com/aykit/theyesmachine

aykit.org

mailto:those@aykit.org

AYKIT

Verein zur Förderung von tollen Sachen