Gnuk — An OpenPGP USB Token Implementation

Niibe Yutaka
`<gniibe@fsij.org>`

About Me

- Contributor to GNU Project
    - GNU Emacs, Guile, glibc, GCC
    - GPLv3, GNU Privacy Guard
    - Japanese Translation Team
- Contributor to Linux: PLIP, SuperH, M32R
- Debian Developer: Golly
- Chair of FSIJ

Distro and Crypto Token

- Distribution developers care about integrity of distribution
  - GnuPG is our friend
- Where to put my GPG keys?
  - OpenPGP card is great
  - but card reader (possibly big) is not my friend
  - Crypto Stick is great too

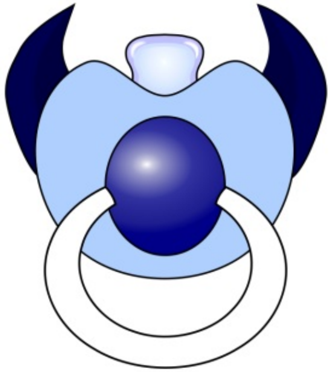
What’s Gnuk?

- Free Software implementation of Cryptographic Token
- Supports OpenPGP card protocol version 2
- Runs on STM32 processor
- Supports RSA 2048-bit

Named after NUK®

- My son used to be with his NUK®, always, everywhere
- I wish Gnuk Token can be a soother for GnuPG user

> NUK® is a registered trademark owend by MAPA GmbH, Germany.



Cryptographic Token?

- Stores your **Secret Keys**
- Performs security operations **on the device**
  - Digital signature
  - Authentication
  - Decryption
- No direct access to **Secret Keys**

How useful?

- Can bring **secret keys** securely
- **On the go**, you can do:
  - Make digital signature
  - Authenticate yourself
  - Read encrypted mail

GNU Privacy Guard (GnuPG)

Privacy Tool by Cryptography

- Conforms to OpenPGP standard
- Usage:
  - Digital Signature
  - Encryption/Decryption
  - Authentication
- Supports "OpenPGP card"

OpenPGP card

- Smartcard to put GnuPG keys
- Follows OpenPGP protocol standard
- Features of v2.0:
  - RSA 1024-bit, 2048-bit, 3072-bit
  - Three keys: Sign, Decrypt, Auth
  - Key generation on the card
  - RSA accelerator

OpenPGP card Applications

- GnuPG
- OpenSSH → gpg-agent
- TLS/SSL Client authentication
  - Scute (Network Security Service)
- PAM
  - Poldi

Gnuk (Since Sep. 2010)

- Focus on software
- CPU choice: STM32 (ARM Cortex-M3)
- Target boards:
  - Olimex STM32-H103
  - STM32 part of STM8S Discovery Kit
  - Original board: FST-01

Gnuk Approach

- OpenPGP card protocol, not PKCS#11
  - PKCS#11 can be emulated on top of OpenPGP card protocol
- Minimum CCID implementation
- Short APDU level exchange

Implementation

- Kernel by ChibiOS/RT
- Crypto by PolarSSL (RSA, AES, SHA1)
- Implements:
  - CCID/ICCD Protocol
  - OpenPGP card protocol / ISO 7816
  - Flash ROM management

As of Gnuk 0.17

- 12 header files in src/
- 20 implementation files in src/
- About 9000 lines of C code

Gnuk Licence

- GNU GPL v3 (and later)

How fast?

- RSA 2048-bit digital signing
  - 1.48sec (version 0.13 or later)
- Useful for GnuPG users
- Useful for OpenSSH users

Limitations of Gnuk

- Using normal processor
  - Tamper Resistance?
    - Flash Read Protection only
  - No RSA accelerator
    - Not that fast
    - Up to 2048-bit

Good points of Gnuk

- Free Software
- Develop/test new things
  - New protocol enhancement
  - New encryption algorithm
  - New PIN input for authentication

Current Status of Gnuk (1)

- GnuPG: works well
- OpenSSH: works well
- Firefox + Scute: Tested on CAcert.org

Current Status of Gnuk (2)

- Not supported:
  - Secure Messaging support
    - USB sniffer can see passphrase
  - Key generation
  - Overriding key import

Known Problems

- OpenPGP card is not portable *.gnupg*
  - Just secret keys
    - No pubring
    - No trustdb

Supported Boards

- Olimex STM32-H103
- Flying Stone Tiny 01 (FST-01)
- STM32 part of STM8S Discovery Kit
- CQ STARM, STBee, STBee Mini

Gnuk Development

- Web page:
  - http://www.fsij.org/gnuk/
- Git Repository:
  - http://www.gniibe.org/gitweb?p=gnuk.git

Gnuk Development Requirements

- GNU Toolchain for ARM
  - summon-arm-toolchain
- Python (PyUSB, PySCard)
- OpenOCD
- Git

Gnuk Host Requirements

- Tested on Debian, Gentoo
  - GnuPG (>= 1.4.11, >=2.0.14)
  - pcscd (>= 1.5.5)
  - libccid (>= 1.3.11)
- Tested a bit on Windows

Steps of building Gnuk Token

- Build gnuk.elf
- Write gnuk.elf to STM32
- Serial number setup (optional)
- Personalize Gnuk Token
- Import keys to Gnuk Token

Using Gnuk Token for SSH authentication

- Don’t run seahorse, but gpg-agent
- Don’t run ssh-agent, but gpg-agent
- Don’t run gnome-keyring

.gnupg/gpg.conf

```
use-agent
```

.gnupg/gpg-agent.conf

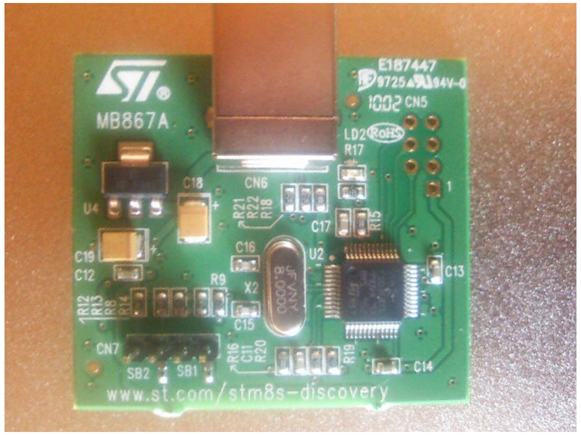
```
enable-ssh-support
```

STM8S Discovery Kit (1)

- Development Kit for STM8S
- Use STM32F103 for USB dongle
- 750 JPY
- Can be: DIY Gnuk Token

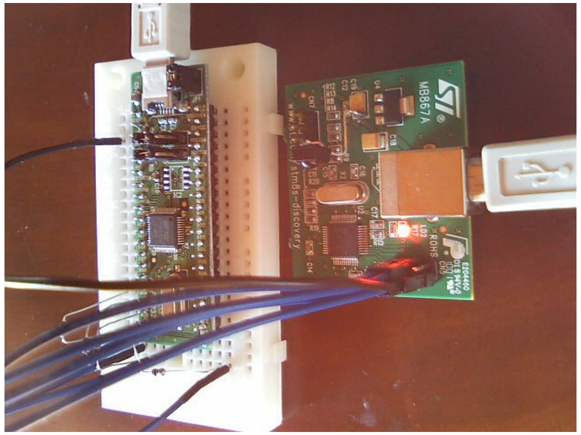
STM8S Discovery Kit (2)

STM32 part

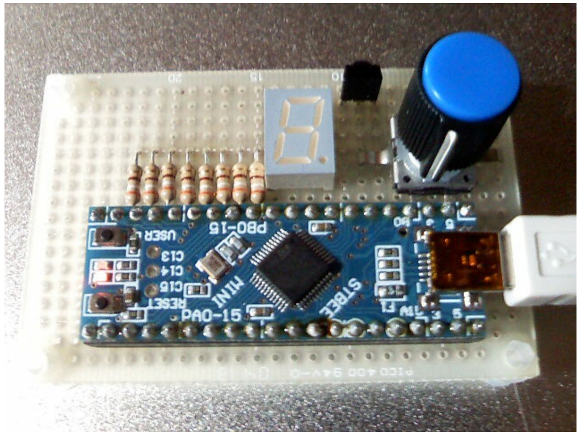


DIY JTAG Debugger

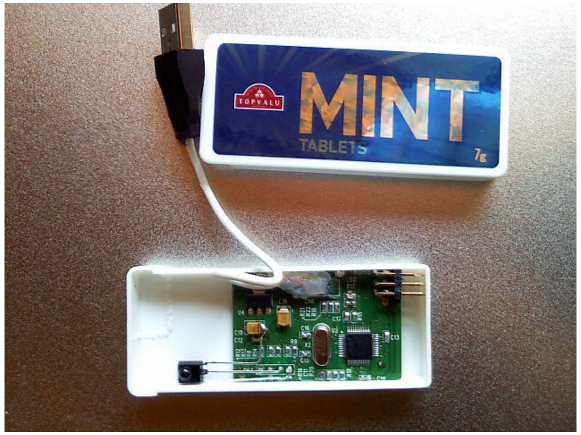
It takes only 2000 JPY, using FTDI 2232 module.



STBee Mini with pinpad



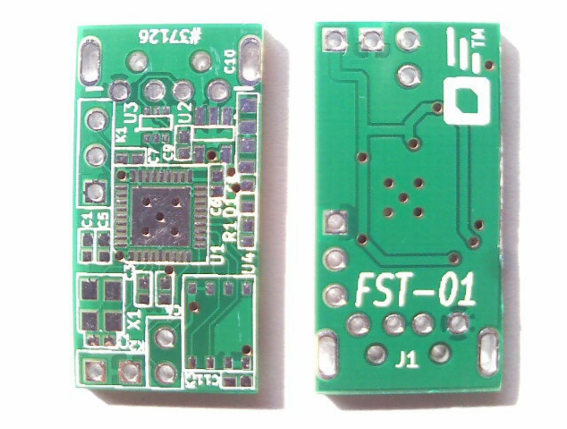
Topvalu Mint tablet case



Hair pin case

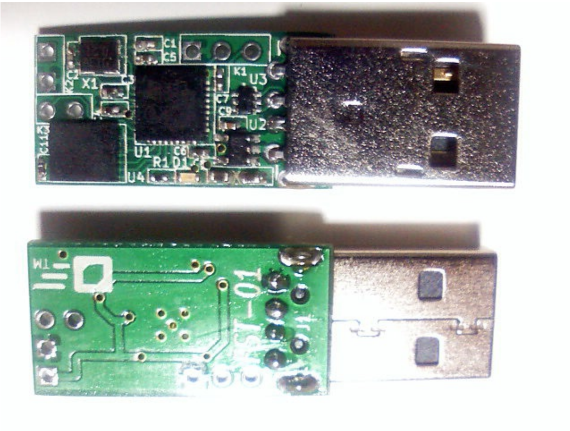
FST-01 PCB

- PCB design by KiCAD
- Distributed under CC BY-SA 3.0



FST-01 Engineering Prototype

- STM32F103TB, SPI Flash memory
- USB Terminator, LDO Regulator
- 12MHz XTAL, LED



Future Work

- ECC P256 support (quite fast)
- configure time USB vendor ID, product ID setup
- Support data other than secret keys
  - Towards portable .gnupg environment

Acknowledgments

- Werner Koch for GnuPG
- Achim Pietig for OpenPGP card specification
- Giovanni Di Sirio for ChibiOS/RT
- Contributors of Gnuk, including:
  - Hironobu SUZUKI
  - Kaz Kojima
  - MATSUU Takuto
  - NAGAMI Takeshi

References (1)

- [GNUPG] GNU Privacy Guard, http://www.gnupg.org/
- [CHIBI] ChibiOS/RT, http://chibios.sourceforge.net/
- [POLAR] PolarSSL, http://polarssl.org/
- [CARD20] Achim Pietig, "Functional Specification of the OpenPGP application on ISO Smart Card Operating Systems (Version 2.0.1)", 2009-04-22.

References (2)

- [CCID] USB Implementers Forum, "Specification for Integrated Circuit(s) Cards Interface Devices", Revision 1.1, 2005-04-22.
- [ICCD] USB Implementers Forum, "Specification for USB Integrated Circuit(s) Card Devices", Revision 1.0, 2005-04-22.
- [ISO7816] ISO/IEC 7816-4:2005, "Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange", 2005.
- [RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer, "OpenPGP Message Format", November 2007.

References (3)

- [FSIJ2009] Niibe Yutaka, "FSIJ USB Token for GnuPG", Japan Linux Symposium, Tokyo, 2009-10-21.
- [PKCS11] RSA Laboratories, "PKCS #11 v2.20: Cryptographic Token Interface Standard", 2004-06-28.
- [PKCS15] RSA Laboratories, "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard", 2000-06-06.
- [FIPS201] Federal Information Processing Standard 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors", March 2006.
- [SP800-78] NIST Special Publication 800-78-3, "Cryptographic Algorithms and Key Sizes for PIV", December 2010.

Gnuk Stickers

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token

FSIJ
GNUK
GnuPG USB Token