Gnuk — A Free Software USB Token Implementation

Niibe Yutaka

<gniibe@fsij.org>

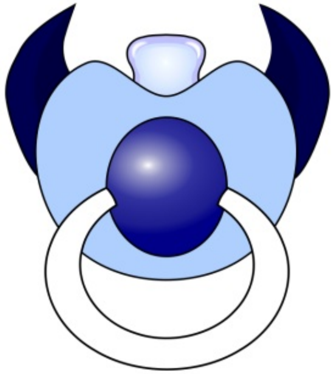
What’s Gnuk?

- Free Software implementation of Cryptographic Token
- For GNU Privacy Guard
- Supports OpenPGP card protocol version 2
- Runs on STM32 processor

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 of **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)

Tool for Privacy 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

Problem to solve

- Where and how we put our **secret keys**?
  - On the disk of our PC
    - Encrypted by passphrase
    - Not Secure Enough
  - OpenPGP card
    - Good (portable, secure)
    - Not easily deployed (reader is not common)

FSIJ USB Token v1 (2008)

- Hardware: Built a PCB
- CPU: Atmel AVR ATmega 328 @20MHz
- Software: RSA computation routine for AVR
  - RSA 1024-bit
    - About 5sec
- Data objects were defined at compile time
- "gpg --card-status", "gpg --clearsign" works

Gnuk (Since 2010)

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

Gnuk Approach

- OpenPGP card protocol, not PKCS#11
  - PKCS#11 can be emulated on top of OpenPGP card protocol
- Simple modern USB communication
  - No physical card
- minimum CCID implementation

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 0.12

- 10 header files in src/
- 17 implementation files in src/
- About 7000 lines of C code

Gnuk Licence

- GNU GPL v3 (and later)

How fast?

- RSA 2048-bit digital signing
  - 1.78sec (version 0.12)
  - 1.54sec (trunk)
- Useful for GnuPG users
- Useful for OpenSSH users

Limitations of Gnuk

- Using normal processor
  - Tamper Resistance?
    - 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 / auth

Current Status of Gnuk (0)

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

Current Status of Gnuk (1)

- Works well:
  - Personalization
  - Passphrase handling
  - Key Import
  - Sign, Decrypt, Auth

Current Status of Gnuk (2)

- Need works of GnuPG:
  - PIN input by keypad
  - Card holder certificate

Current Status of Gnuk (3)

- Not supported:
  - Secure Messaging support
  - Key generation
  - Overriding key import

Known Problems (1)

- Requires newer pcscd, libccid
  - because of modern USB communication
- Requires newer GnuPG
  - for SHA2
- Problems of GnuPG
  - SCDaemon’s permanent connection to pcscd

Known Problems (2)

- Smartcard / Hardware Token is not mature on GNU/Linux
- OpenPGP card is not portable *.gnupg*
    - Just secret keys
    - No pubring
    - No trustdb
- Keypad support of GnuPG

Gnuk Releases

Ver	Date	Ver	Date	Ver	Date
0.13	2011-06-??	0.8	2011-01-19	0.3	2010-10-23
0.12	2011-05-13	0.7	2011-01-15	0.2	2010-09-13
0.11	2011-04-15	0.6	2011-01-14	0.1	2010-09-10
0.10	2011-02-10	0.5	2010-12-13	0.0	2010-09-06
0.9	2011-02-01	0.4	2010-11-09		

Gnuk Development

- Web page:
  - http://www.fsij.org/gnuk/
- Git Repository:
  - http://www.gniibe.org/gitweb

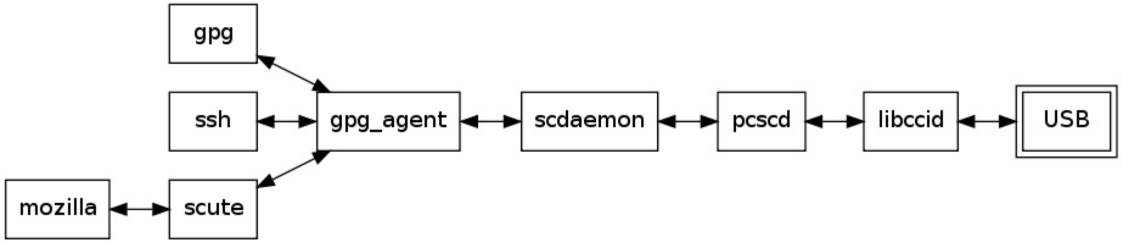
Gnuk Development Requirements

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

Gnuk Host Requirements

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

Processes on host



Steps of building Gnuk Token

- Build gnuk.elf
- Write gnuk.elf to STM32
- Configure Gnuk Token
- Personalize Gnuk Token
- Import keys to Gnuk Token

Using Gnuk Token for SSH authentication

- Don’t run seahorse, but gpg-agent
  - /etc/X11/Xsession.d/60seahorse
- Don’t run ssh-agent, but gpg-agent
- Don’t run gnome-keyring

```
$ gconftool-2 --type bool --set \
  /apps/gnome-keyring/daemon-components/ssh false
```

.gnupg/gpg.conf

```
use-agent
```

.gnupg/gpg-agent.conf

```
enable-ssh-support
```

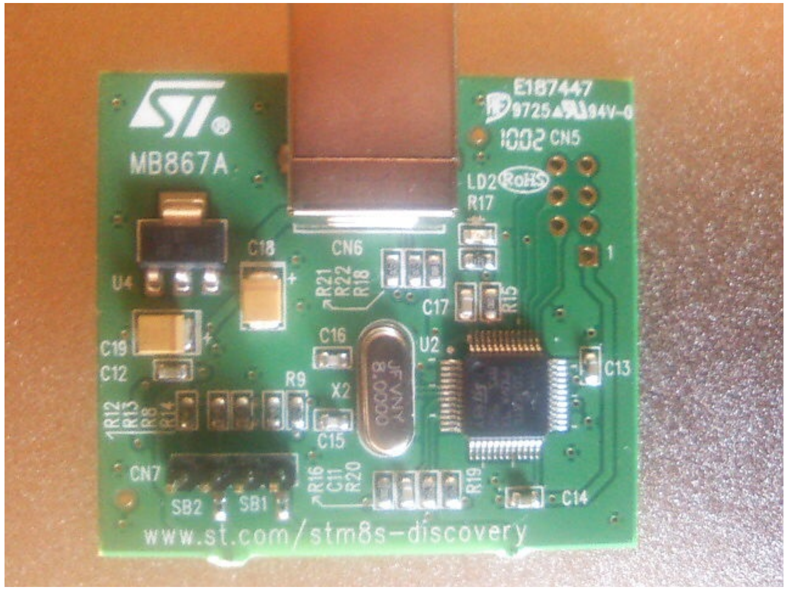
STM8S Discovery Kit (1)

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

STM8S Discovery Kit (2)

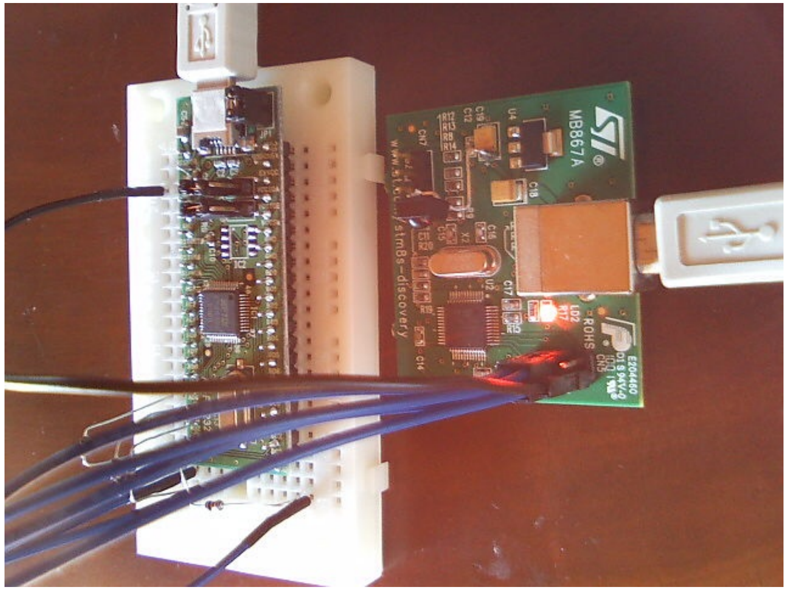
STM8S-Discovery
¥750
STM8S
Everything to discover the STM8S
1. STM8S evaluation board
2. User application area
3. Embedded ST-LINK for STM8S
4. USB interface for debugging and programming
5. Numerous examples available on www.st.com/stm8s-discovery
STM8S-DISCOVERY/ 01-0

STM32 part

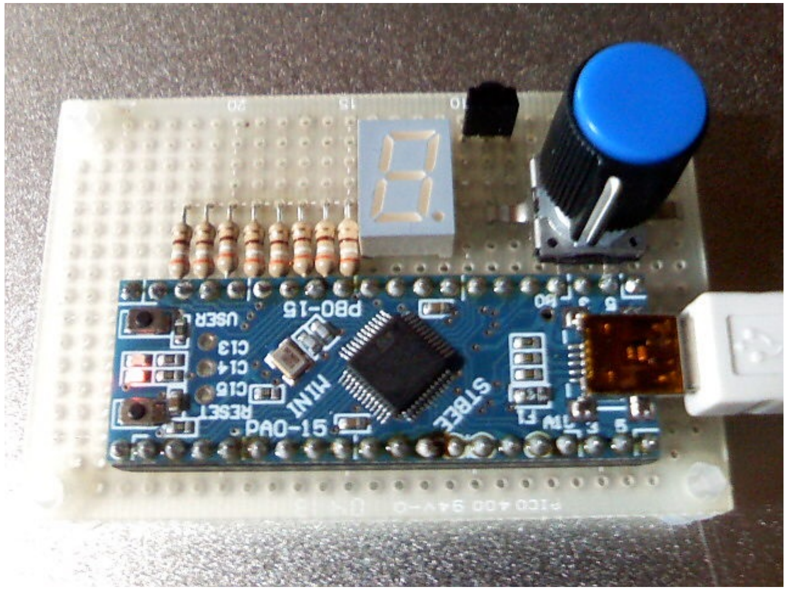

MB867A
E187447
9725 94V-0
1002 CN5
LD2
RoHS
R17
C18
CN6
R21
R22
R18
U4
C17
R15
C19
C16
U2
C12
C13
R9
X2
R12
R13
R8
R14
C15
CN7
R16
C11
R20
R19
C14
SB2
SB1
www.st.com/stm8s-discovery

DIY JTAG Debugger

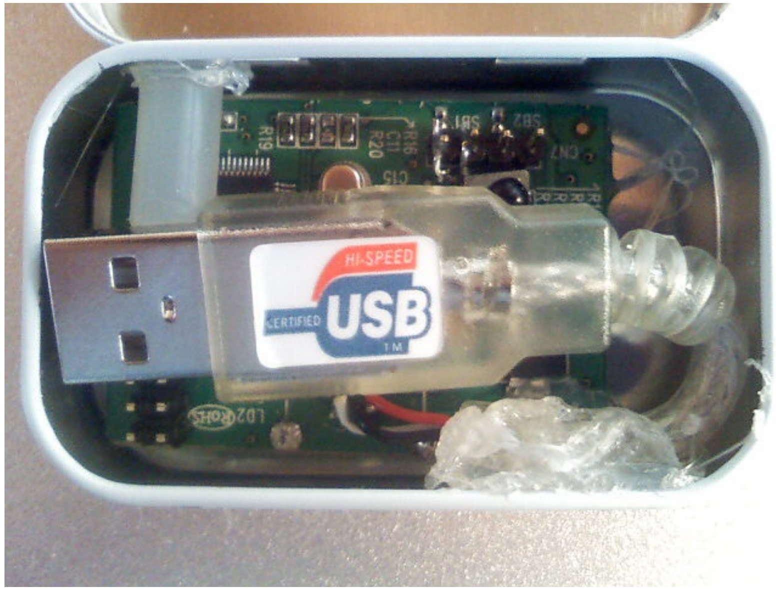
It takes only 2000 JPY, using FTDI 2232 module.



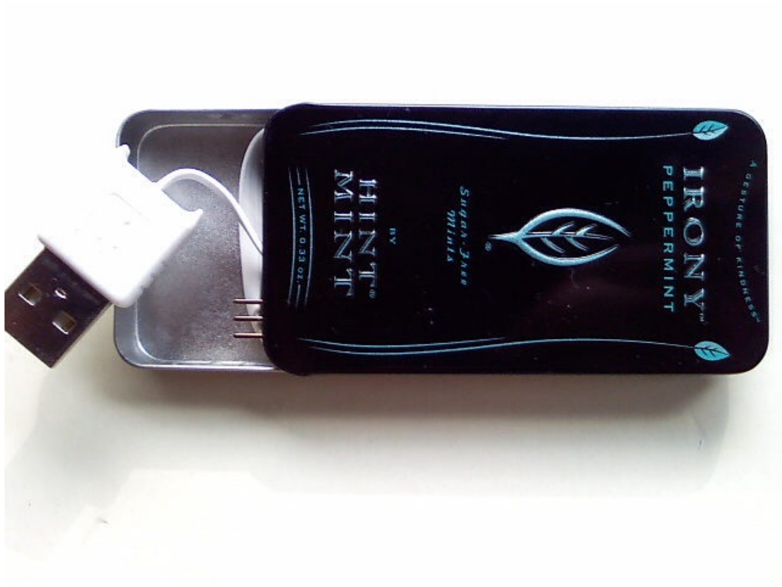
STBee Mini with pinpad



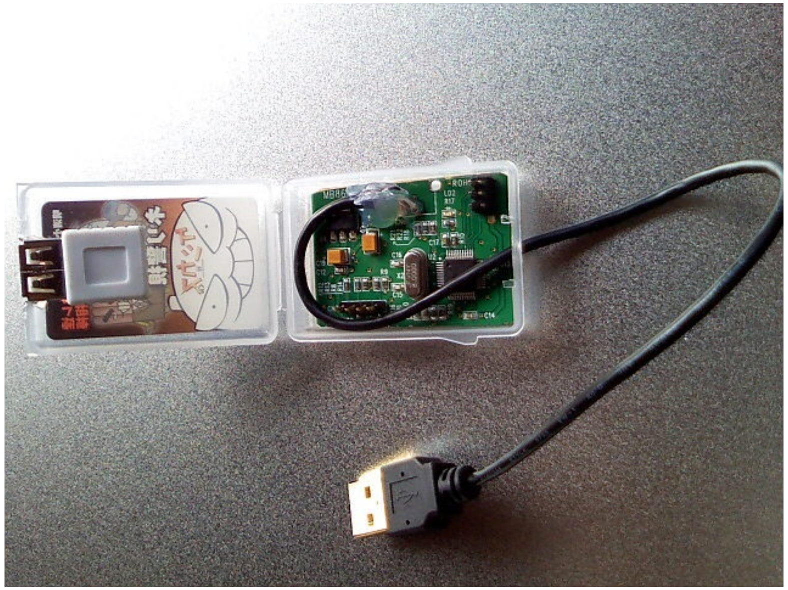
Altoids Tiny Tin



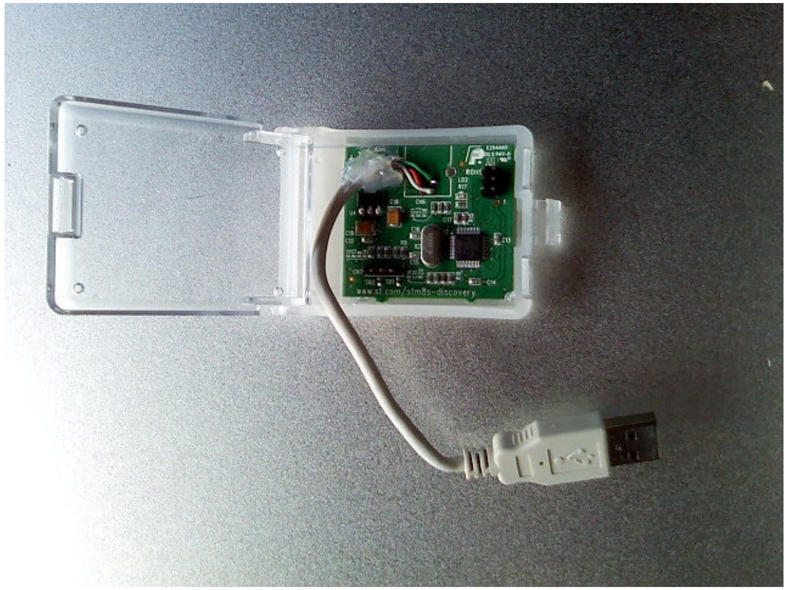
Irony Peppermint Tin



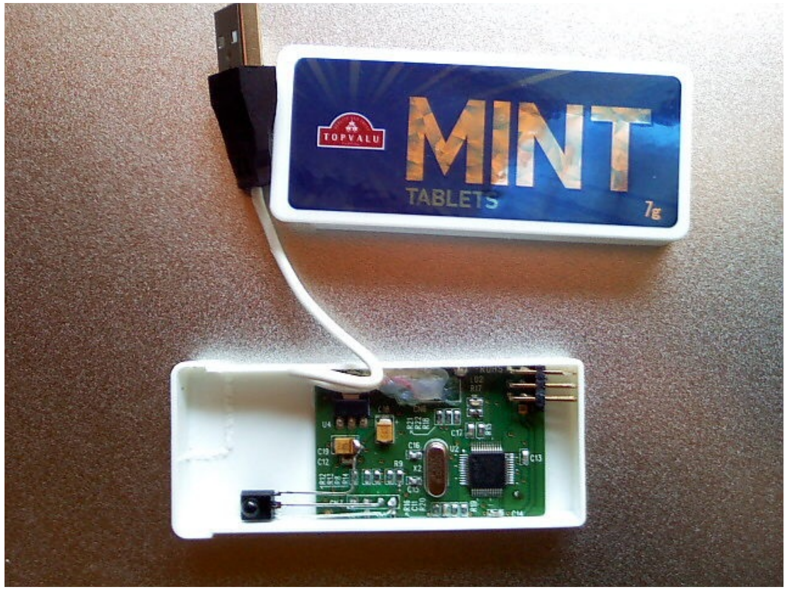
Eraser box



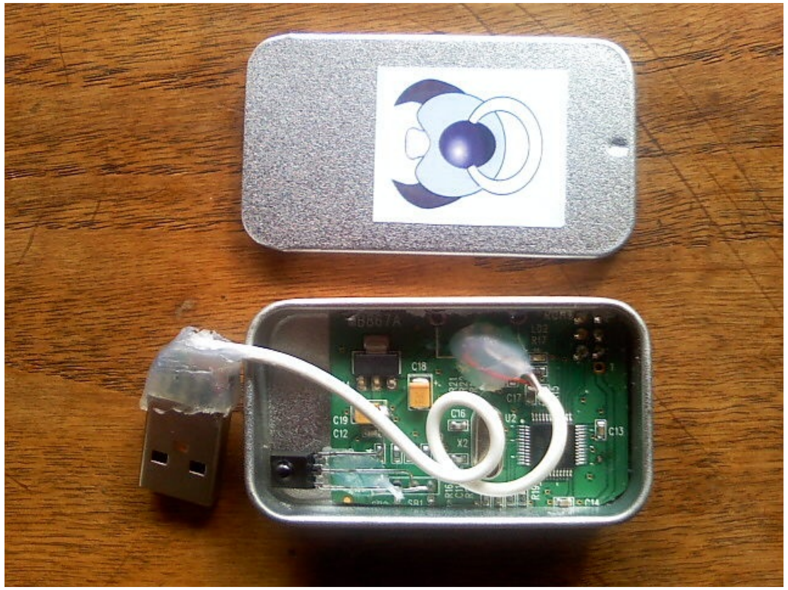
Paper Clip box



Topvalu Mint tablet case



Hair pin case



Comparison of potable secret keys

	Gnuk Token	USB memory	GPF Crypto Stick	OpenPGP card + reader	OpenPGP card App on Smartphone (hypothetical)
Availability	DIY	Good	Good	Good	Application
Maximum Key size	2048	4096	3072	3072	3072 or more
Tamper Resistance	Somehow	No	Good	Good	No
Deployment	Difficult (Need newer software)	Easy	Not-easy	Not-easy	Not-easy
Enhancement/Study	Yes	-	No	No	Yes
Brute force attack	Only few	Unlimited	Only	Only few	Unlimited after

	times		few times	times	break
Hardware Price	Cheap	Cheapest	49 Euro	16.4 + 21 Euro	Expensive
Risk of theft (for other usages)	Low	Middle	Low	Partly	High

Acknowledgments (1)

- Werner Koch for GnuPG
- Giovanni Di Sirio for ChibiOS/RT
- Contributors of Gnuk, including:
  - Hironobu SUZUKI
  - Jan Suhr
  - Kaz Kojima

Acknowledgments (2)

- Contributors of Gnuk, continued:
  - MATSUU Takuto
  - NAGAMI Takeshi
  - Shane Coughlan
  - Werner Koch

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