OpenPGP-Smartcard-Vergleich

Niklaus ’vimja’ Hofer niklaus@mykolab.ch

June 15, 2019

/me

- Founding member of the Chaostreff Bern
- Studiert an der BFH
  - IT / Infosec

Inhalt

OpenPGP card

requirements

Cards

Comparisons

smartcard

- Does smartcard stuff
- `https://media.ccc.de`

usage

- Protect your keys
- physical security
- PC can use the key but not access it
- Typical crypto stuff with symmetrical encryption
- Still potential for abuse

UIF

- User Interaction Flag
- Requires user interaction for each cryptographic operation
- Good protection from malware

keys

- Generate on card
- Do you trust the card’s RNG?
- Not all cards can generate all keys
- Generate on computer, transfer to card
- Easier backup

Inhalt

OpenPGP card

requirements

Cards

Comparisons

What is important to you?

- Physical security
- Which algorithms do you need?
- Do you need UIF?
- How fast do you need it to be?
- How robust must it be?
- How open must it be?
- Any additional features?
- Key generation limitations

Algorithms

I will focus on 4k RSA and ed25519

I also like my devices to have U2F

Inhalt

OpenPGP card

requirements

Cards

Comparisons

Yubikey

- supports 4K RSA
- fast
- considered secure
- Many additional features
- Available in FIPS certified versions
- Mostly closed these days
- no ed25519

You buy this one because it is robust!

fst-01

- Flying Stone Tiny 01
- Gnuk firmware
- completely open
- hard to retrieve
- extremely poor performance for 4k RSA
- casing may be an option
- various reworks exist but are not manufactured

Nitrokey

- Nitrokey start
  - Based on the fst-01
  - Gnuk firmware as well
  - RSA limited to 2k
  - Open hardware
- Nitrokey Pro (2)
  - Smartcard adapter
  - version 2 supports various curves but not ed25519
  - Handles 4k RSA

Ledger

- Crypto wallet with an OpenPGP card app
- Can hold multiple keypairs and switch between those
- Device has been cracked
- but there is a new one coming soon

Trezor

- Crypto wallet with an app
- Not even a real OpenPGP card
- Requires a separate daemon (!)
- I have not tested that
- Device has been cracked

Inhalt

OpenPGP card

requirements

Cards

Comparisons

Feature matrix

	UIF	4k RSA	ed25519	Open Source	Open Hardware	U2F
Yubikey Neo	No	Yes	No	Yes	No	Yes
Yubikey 4 / 5	Yes	Yes	No	No	No	Yes
Nitrokey Pro (2)	No	Yes	No	Yes	??	No
Nitrokey Start	No	No	Yes	Yes	Yes	No
fst-01	No (*)	Yes (*)	Yes	Yes	Yes	No
Trezor	??	Yes	Yes	Yes	Yes	Yes
Ledger	Yes	Yes	Yes	Yes	??	Yes

Feature matrix

CPU (i7-5930K) 0.2s

Yubikey FIPS (version 2.1) 0.9s

Nitrokey Pro 2 (version 3.3) 3.1s

Nitrokey Pro (version 2.1) 3.2s

Ledger Nano S (Firmware 3.3.1, OpenPGP XL 1.3.1) 4.1s

Flying Stone Tiny 01 (FST-01) 8.2s