Hardware Crypto Tokens

Slides at: https://www.noteblok.net/2015/06/15/hardware-security-token/

Useful Commands

GnuPG: get card status:

```
gnupg —card-status
```

GnuPG: edit card settings, keys & pins:

```
gnupg —card-edit
```

Yubikey: setup token (there's also a nice GUI):

```
ykpersonalize
```

Yubikey: manage PKI certificates:

```
yubico-piv-tool
```

Links

TOKENS

Name	Price	URL
Yubikey	18 € / 50 €	https://www.yubico.com
NitroKey	not yet available	http://www.nitrokey.com
plug-up Security Key	6 €	http://www.plug-up.com
OpenPGP Smartcard	16,40 €	http://g10code.com/p-card.html
HIDeKey	3-5 €	https://dev.0l.de/wiki/projects/hidekey

SOFTWARE

pass	free — Open Source Software	http://www.passwordstore.org
Keepass		http://keepass.info/help/kb/yubikey.html
OpenKeyChain		http://www.openkeychain.org/
Yubico Authenticator		http://bit.ly/1L1TzVh
Google Authenticator		http://bit.ly/19dDzPR

TOKEN & TFA ENABLED WEBSITES

http://dongleauth.info	 try those!
https://twofactorauth.org	

Terminology

- **OTP:** One-time password
- **TFA, 2FA:** Two / Second-Factor-Authentication
- **SC:** Smart Card (special secure crypto micro processor)
- **TPM:** Trusted Platform Module (enables DRM, Secure Boot)
- **HSM:** Hardware Security Module (used by SSL Certificate Authorities, DNSSEC, Banking)
- **OpenSC:** OSS implementation of PKCS#11 drivers and APIs
- **PSSCLite:** OSS implementation of PS/SC APIs
- **SCdaemon:** GnuPG agent to communicate with an OpenPGP smart card

Standards

- Initiative for Open Authentication (OATH)
  - Time-Based OTP Algorithm (TOTP)
    Standard used for 6-digit TFA codes by Google Authenticator
  - HMAC-Based OTP Algorithm (HOTP)
  - Challenge-Response Algorithm (OCRA)
- Fast Identity Online Alliance (FIDO)
  - Universal Second Factor (U2F)
    Challenge Response Authentication, lobbied by Google / Yubico, supported by the Chrome browser, JavaScript API, Tokens
- OpenPGP Smart card Application 2.1
  Functional specification of the PGP applet on SC's
- Personal Identity Verification (PIV)
- Public Key Cryptography Standards (PKCS)
  - PKCS#11: Cryptographic Token Interface

- Java Card Open Platform (JCOP)
  Operating system for SC's which runs Java applets
- Chip Card Interface Device (CCID)
  USB protocol to communicate with SC's / readers
- Personal Computer/Smart Card (PC/SC)
  APIs for Operating system integration of SC's

- ISO/IEC 7816 *Physical & electrical specs of chip cards, APDU communication, Card dimensions, T=0, T=1 Communication protocols*
- ISO/IEC 14443 *Contactless integrated circuit cards, NFC, RFID*