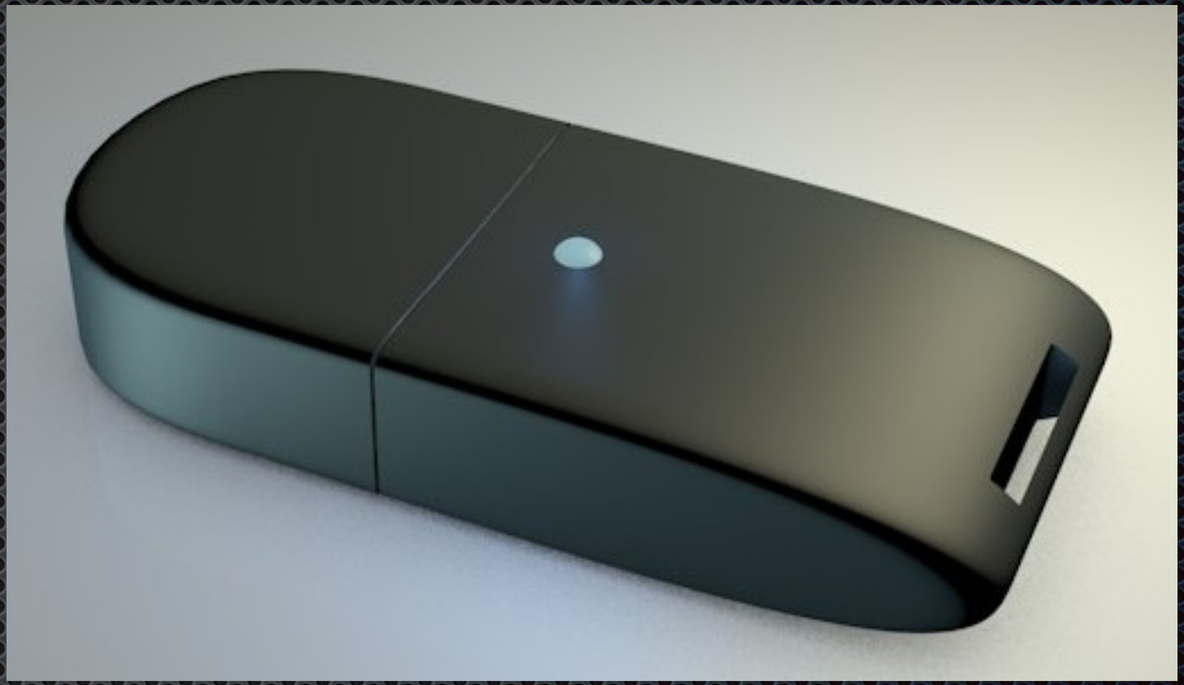
Nitrokey and the Future of End-to-End Encryption

Security Challenges

- Untrusted computers
- Viruses, trojans, security flaws
- Mobile vs. lost or stolen devices
- Security and poor usability
- Passwords don't work!
- Backdoors: Which vendor to trust?

The Nitrokey

- USB device
- Secure key storage
- One Time Passwords (OTP)
- Encrypted mass storage
- Easy to use
- Open Source



Use Cases

- Email encryption: GnuPG, Thunderbird, Evolution, MS Outlook
- SSH, OpenVPN, PC Login, TrueCrypt, Firefox, harddisk encryption ...
- Secure weblogin via OTP: e.g. Google, FB, Dropbox
- Encryted mass storage, hidden volumes

Nitrokey Protects

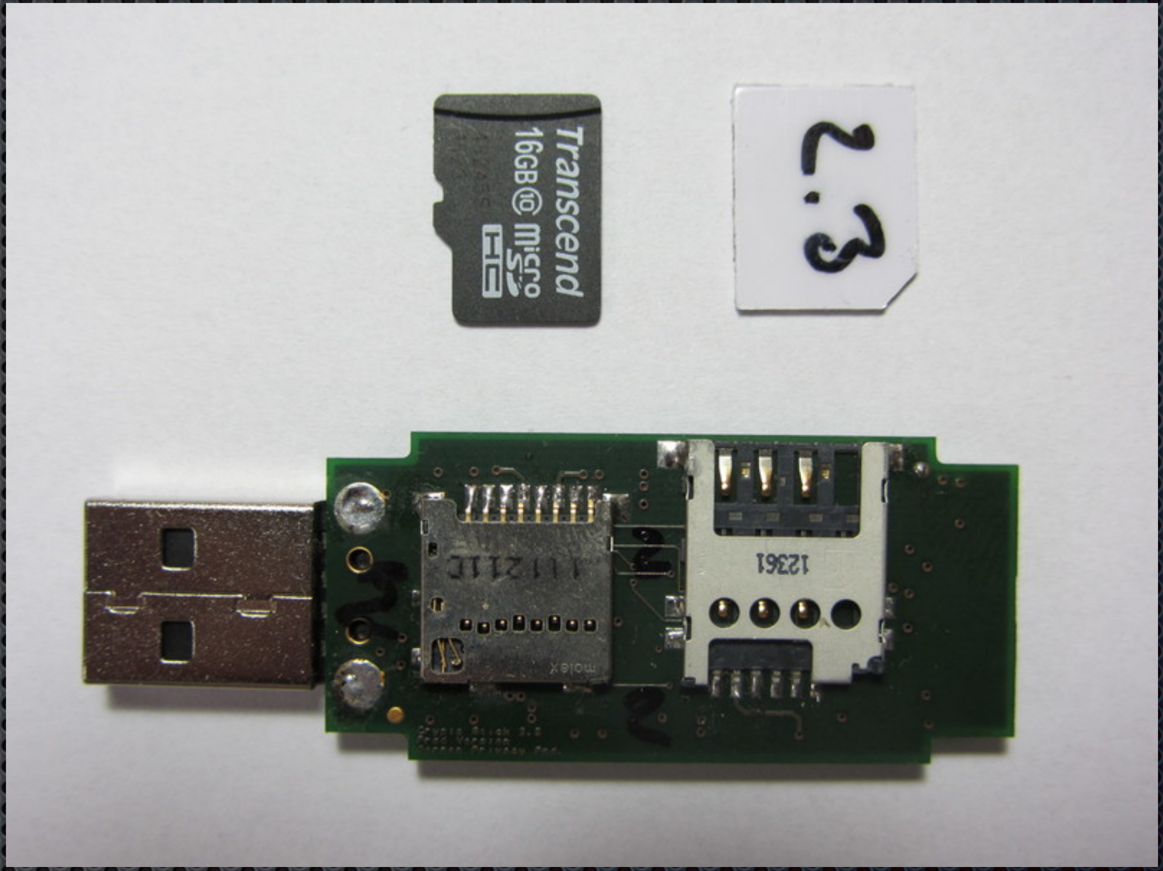
- Key logger, trojan horses, computer viruses
- Thieves, lost
- User mistakes
- "Brute-force" / PIN guessing
- Advanced physical attacks

Secure Key Storage

- Contains the OpenPGP Card
- PIN protection
- Key generation on device or import
- 3 independent keys (authentication, encryption, signature)
- RSA 1024, 2048, 3072, 4096 bit
- Compatible to OpenPGP, S/MIME, PKCS#11

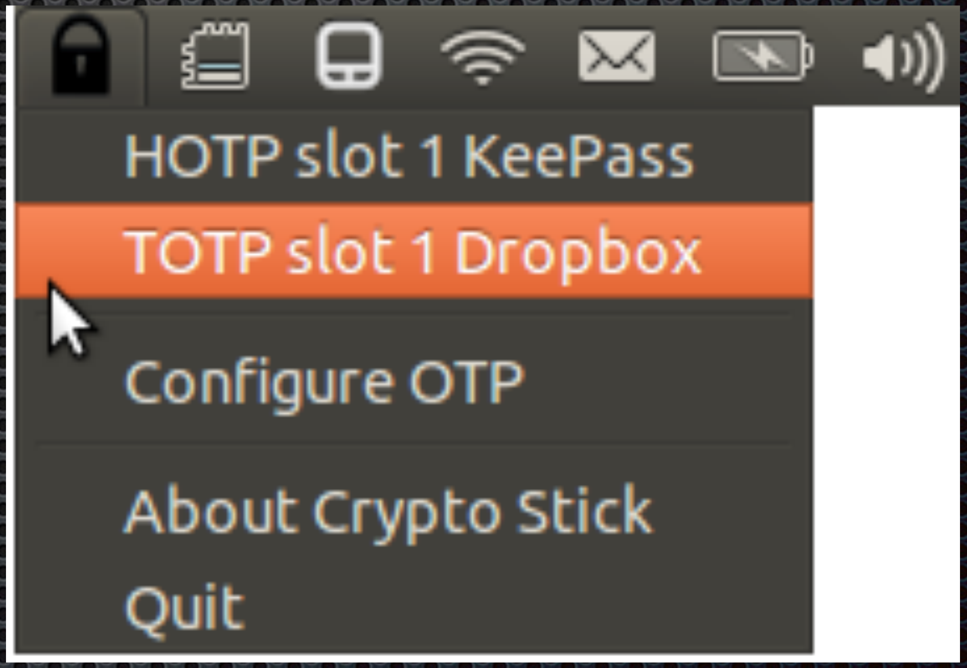
Encrypted Mass Storage

- Hardware encryption
- Max. 64 GB capacity
- Read/write 6 MByte/s
- AES-256
- Write-lock
- Hidden volumes enable plausible deniability



One Time Passwords

- Secure login to websites and local applications
- 2nd factor authentication
- RFC 4226, RFC 6238, Google Authenticator
- Google, FB, Dropbox... See www.dongleauth.info

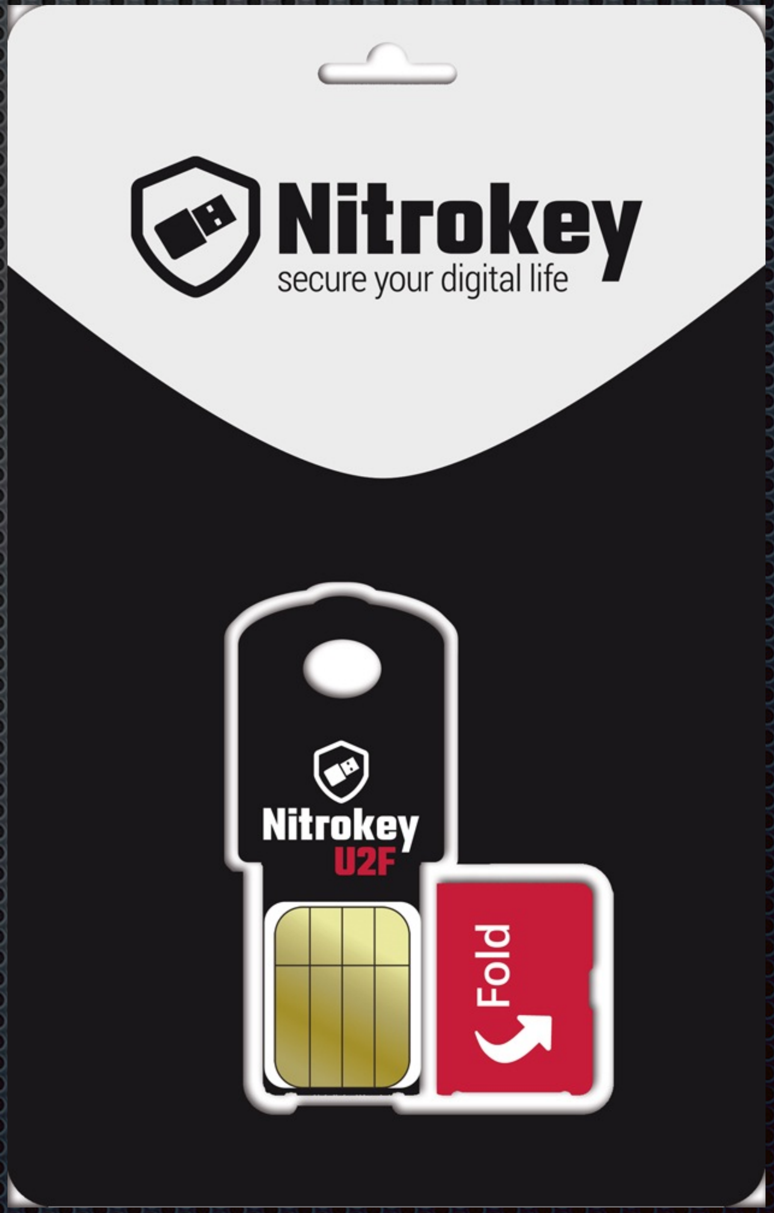


FIDO Universal 2nd Factor (U2F)

- New authentication standard for USB keys
- Secure: Asymmetric crypto (ECC), challenge response
- Easy to use: No driver, no additional software
- Privacy friendly: No identifying certificates
- Native browser support (currently: Chrome only)

U2F with Nitrokey

- Dedicated U2F device
- U2F-support for main Nitrokey device: work in progress



Vision: Universal Encryption

- "U2F for encryption"
- Encryption in JavaScript
- User-keys are stored on Nitrokey
- Use cases: web word processor, invoice creation, calendar, contacts, your own application

Workflow:

1) User data is encrypted in the browser

2) Encrypted data is stored on a server

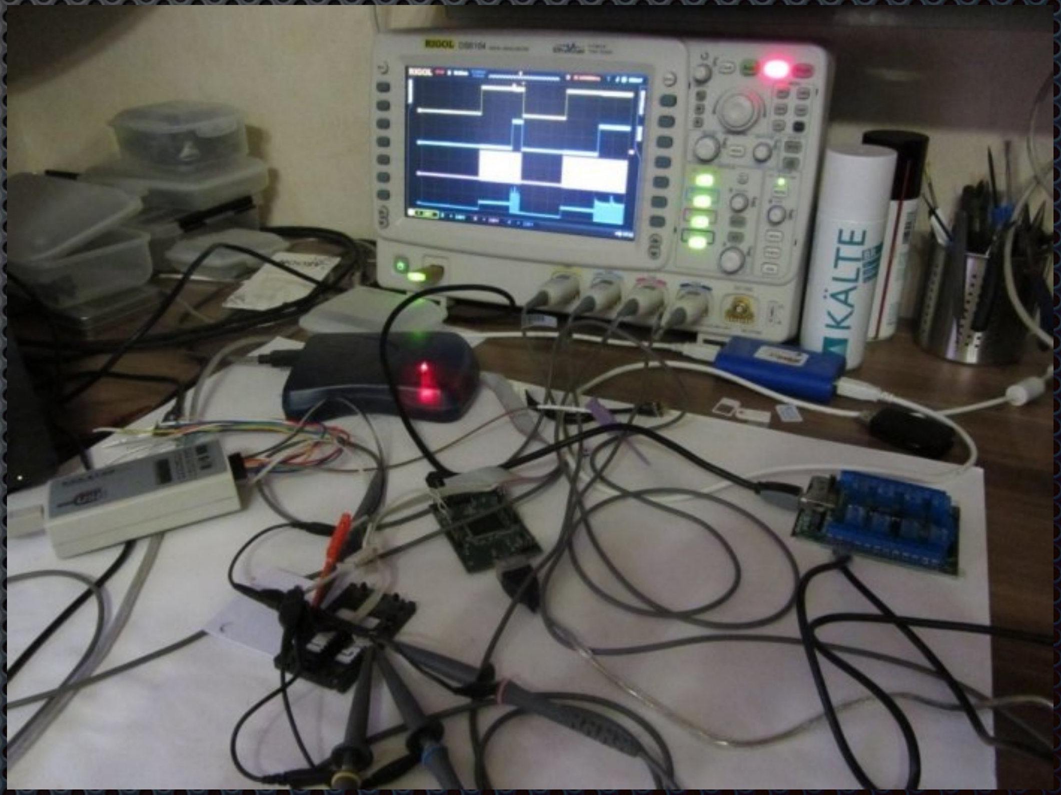
3) After retrieval, user data is decrypted in the browser

Nitrokey

secure your digital life

Hacking

- Open Source: software, hardware, interface!
- Extensible firmware, written in C
- Free development tools
- GUI is based on QT
- Can be soldered at home
- Friendly community



The Nitrokey Project

- Founded in 2008 as Crypto Stick
- Non-profit, small community
- Supported by: German Privacy Foundation, Google Summer of Code, NLnet Foundation
- Version 1.0: 2009
- Version 1.2: 2010
- Version 1.4 beta and Storage beta: 2014