Crypto Stick

Secure Data Protection through Open Source USB Key

Executive Summary

The Crypto Stick is an USB key with integrated (proprietary) smart card to enable highly secure encryption of e-mails and data, for authentication in networks and for access control. Other than ordinary software solutions, the secret keys are always stored securely inside the Crypto Stick. Their extraction is impossible which makes the Crypto Stick immune to computer viruses and Trojan horses. The user-chosen PIN and the tamper-proof design protect in case of loss and theft. The hardware and software are both available as Open Source to allow verifying the security and integrating with own applications.

Use cases:

- E-mail encryption based on X.509/SMIME and OpenPGP (e.g. Outlook, Thunderbird, Evolution)
- Encryption of data stored on separate storage (e.g. TrueCrypt).
- User authentication on local computers (e.g. Windows, Linux).
- User authentication for network services (e.g. Firefox, OpenSSH, OpenVPN, IPSec, OpenID).

Advantages to ordinary software solutions:

- Secret keys are always stored securely inside the Crypto Stick. Their extraction is impossible. All sensitive cryptographic operations are computed in the Crypto Stick.
- User-chosen PIN protects in case of loss and theft against brute force attacks.
- Immune to computer viruses, Trojan horses, phishing attacks and other malicious software.
- Tamper-proof design prevents sophisticated physical attacks with laboratory equipment.
- Secret keys are generated securely on the Crypto Stick to prevent their extraction by attackers.

Advantages to proprietary security devices:

- Secure implementation can be verified by client and independent third parties to ensure the absence of back doors and security flaws.
- Compatible to a large variety of

software applications such as Outlook, GnuPG, Enigmail, Mozilla Thunderbird, OpenSSH for instance.

- Own custom applications can be integrated easily due to open interfaces and open drivers
- Lack of vendor lock-in increases security of your investment
- Security does not depend on secrets stored centrally at the vendor
- Growing acceptance and user base supports continuously improvement and ensures high security due to peer reviews.
- Transparent and open development process as an open source project

Further advantages:

- Windows, Linux, and MacOS X are supported.
- Additional administrator PIN enables hierarchical use cases.
- Three independent RSA keys, max. length 4096 bit each.
- Import of existing keys and backup of keys possible.
- High security due to embedded smart card which is based on Common Criteria 5-high certification.

Many popular security and encryption devices were broken:

- In 2011 RSA Inc was hacked and secret information about **RSA's securID token** was stolen which allows to crack them.[1]
- In 2010 it was revealed that AES-256 encrypted and **FIPS 140-2 Level 2 certified** USB storage devices of the following vendors could be easily accessed by using a default password:[2] **Kingston, SanDisk, Verbatim, MXI, PICO**

Serious security flaws were also found in the following products:

- **Aladding eToken Pro** (2010)[3]
- **Corsair's Padlock 2** (2010)[4]
- **Raidon's Staray-S-Serie** (2009)[5]
- All USB storage devices from **9Pay, A-Data** and **Transcend** which use fingerprint readers based on the **USBest UT176 and UT169 from Afa Technology** (2008)[6]
- **Excelstor's GStor Plus** (2005)[7]
- **Lexar JumpDrive** (2004)[8]

[1] http://www.wired.com/threatlevel/2011/03/rsa-hacked/
[2] http://www.zdnet.com/blog/hardware/encryption-busted-on-nist-certified-kingston-sandisk-and-verbatim-usb-flash-drives/6655
[3] http://www.youtube.com/watch?v=Yc95myrnQ0E&NR=1
[4] http://www.schneier.com/blog/archives/2010/03/crypto_implemen.html
[5] http://h-online.com/-746225
[6] http://heise.de/-270060
[7] http://heise.de/-270702
[8] http://secunia.com/advisories/12522/

www.crypto-stick.com

About the German Privacy Foundation

The Crypto Stick is sponsored by the non-profit German Privacy Foundation e.V. (GPF). The GPF provides free user support and ensures the ongoing development of the Crypto Stick. Furthermore it offers related training and consulting services.

Contact:

German Privacy Foundation, Berliner Str. 69, 13189 Berlin, Germany, www.privacyfoundation.de