Art of Technology

DEVELOPED FOR: Armasuisse

Secure USB-Stick

ELECTRONIC DESIGN AND DEVELOPMENT SERVICES

The Secure USB Stick is an intelligent mass storage device for the secure storage of confidential data that can be used with any standard USB connection on Windows and Linux

The secure solution with full user control

Data is symmetrically encrypted by means of a data key used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange a key so that it can be used in the decryption process. A public/private key pair stored on a Smart Card protects the data key that is encrypted with the users public key stored on the Secure USB-Stick. As the entire security relevant software is available in source code, the administrator (customer) has full control over the encryption, decryption and key management and can adapt the encryption and decryption software to his own specific requirements.

Description

The Secure USB-Stick is a storage device with integrated encryption that stores sensitive data on an encrypted partition. No special drivers are necessary, only support for a USB mass storage device is required that is already included as standard in Linux, Windows XP and its successors.

All software necessary for the use of the Secure USB-Stick is stored on a read-only partition and can be run directly from the USB-Stick without installation. The software for the user is currently available for Linux and Windows.

Challenge

- Use standard drivers from PC operating system
- No installation of drivers or applications on PC
- Support for multiple users with individual keys
- Support for Windows and Linux

Solution

The Secure USB-Stick sytem is delvered with:

- any number of Secure USB-Sticks
- firmware for the Secure USB-Stick
- user software for Linux and Windows
- notebook equipped with:
  - administrator tools to issue and manage sticks
  - development and support tools to be used as a design centre to adapt firmware and software

Features

- 1 GByte data volume
- secure USB-Stick is bootable with a Linux live system

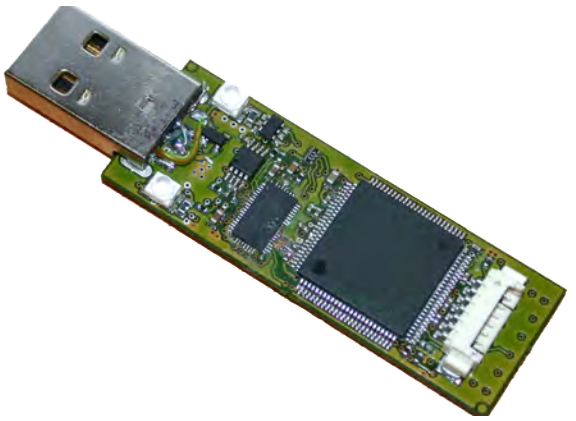
- separate encrypted and unencrypted storage areas
- data on un-encrypted area is read only (for the user)
- senstitive data is encrypted with symmetrical algorithm
  - encryption with Triple-DES or AES
  - key length for data key is 128 or 256 bits

- a unique key is derived for each individual sector of the encrypted drive from the data key to improve security
  - data key for encryption / decryption is asymmetrically encrypted with users' public keys
  - up to 10 different users can be configured per Secure USB-Stick

- user's private key stored on a smart card, or secured with other existing credentials
  - key length of asymmetrical key pair is 1024/2048 bits

Benefits

- safe encryption of data
- data and keys stored separately
- safety-relevant programmes available in source code
- development of software with open source tools
- customer modifiable firmware of Secure USB Stick
- data encryption and decryption is executed directly on the Secure USB Stick
- support for user groups, which can use a USB stick together, while using their "private" smart card



Art of Technology

Art of Technology AG
Technoparkstrasse 1
8005 Zürich
Switzerland

+41 (43) 311 77 00
info@aotag.ch
www.aotag.ch