ART OF TECHNOLOGY

electronic system design

Secure USB Stick

THE SECURE SOLUTION WITH FULL CONTROL

The Secure USB Stick is an intelligent mass storage device for the secure storage of confidential data. Data is symmetrical encrypted by means of a data key. A public/ private key pair stored on a Smart Card protects a data key, which is stored on the Secure USB Stick. As the entire security relevant software is available in source code, the user (initiating company) can adapt the en- and decryption software to their requirements and has full control over the en-/decryption as well as the key management.

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 to use the Secure USB Stick. Only support for a mass storage device (e.g USB stick, hard drives etc.) is required. This is included in Windows XP, its successors and Linux.

All programs necessary for the use of the Secure USB Stick are stored on the Secure USB Stick itself and can be run directly without installation. The operating program for the user is currently available in a Windows and a Linux version.

Challenge

- Operation with standard drivers from PC operating system.
- No installation of drivers or applications on PC.
- Support for WINDOWS and LINUX.
- Support for multiple users for a single Secure USB Stick with individual keys.

Solution

The Secure USB Stick solution consists of the USB Sticks containing:

- Firmware for the Secure USB Stick
- User software for WIN and LINUX and a notebook equipped with:
- Administrator tools for issuing and administrating Secure USB Sticks
- Development and support tools, to be used as a design centre to adapt the firmware and software.

Advantages

- Safe encryption of data.
- Data and keys stored separately.
- All safety-relevant program sections are available in source code.
- Development of the software with Open Source Tools.
- Customer modifiable firmware of the Secure USB Stick.
- Data en-/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.

Features

- Data on the flash memory is encrypted with a symmetrical algorithm.
- Encryption with Triple-DES or AES.
- Key length for data key is 128 or 256 bits.
- For each individual sector of the drive a unique key is derived from the data key to improve security.
- The data key for the encryption is asymmetrically encrypted with the users' public keys.
- Currently up to 10 different users are supported per Secure USB Stick.
- The private key is stored on a Smart Card or can be secured with other existing credentials.
- The key length of the asymmetrical key pair is 1024/2048 bits.
- The Secure USB Stick has separate encrypted and unencrypted storage areas.
- All data within the unencrypted area is for the user read only.
- The Secure USB Stick is bootable with a Linux live system.

Art of Technology AG | Zurich | Switzerland | T: +41 (43) 311 7700 | info@aotag.ch | www.aotag.ch