Secure Mass-Storage

Situation

The aim was to develop a high speed reader device for secure communication with mass storage device/smart-card based on JavaCard technology. This high speed mass storage device was designed for storing huge data with a convenience of smartcard and storage and performance like a hard disk.

With onboard encryption intelligence the reader and storage devices must authenticate an individual before providing access to information stored on the storage media card.

Expected feature set

Secure Storage Device system

Secure Storage Device system including **smart-card** compliant with JavaCard / VISA cards and corresponding **reader device.** The smart-card and reader device should be capable of mutually authenticating each other.

Reader Device

Reader Device a USB composite device, with two different interfaces: **mass storage** and **CCID**

JavaCard Application development

JavaCard Application development on smart-card system for authenticating the user of the card and the reader device which retrieves the data from the smart-card.

Security Engine

Security Engine on Reader Device: It is used to encrypt or decrypt the user-data for storing or retrieving information from the mass storage media card.

Solution

Aftek has designed and developed a complete software solution including firmware design, device driver development, eCos® porting, and embedded application development for the reader.

Aftek also developed a JavaCard application to-transfer data from the card to the host system at high-speeds and in a secure manner. This application was hosted on the JavaCard storage device.

The reader device implemented a very efficient security engine. This engine had the ability to **mutually authenticate** the card, card-owner as well as the reader system with each other. This implementation provided **maximum level of security** for the card based data transfers with the host.

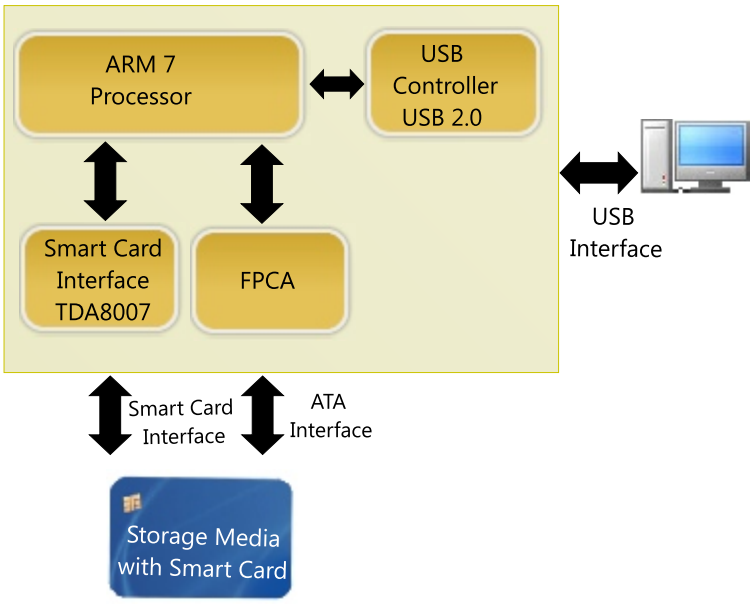
This hard-to-crack security mechanism was implemented on the reader device with ease, optimized execution and with very minimal

Benefits to the client

Aftek leveraged its PKI and Cryptography expertise for providing valuable recommendation and best practices for implementing the desired security. It has helped the client to understand and change the security protocol design devise full-proof security mass storage solution.

Aftek has excellent capabilities in hardware design & development capability. We have provided valuable suggestions and corrections in the reader hardware design provided by the client.

Highly optimized software with very minimal footprint.



Features

- It is a USB composite device, with two different interfaces: mass storage and CCID
- High performance for handling large amounts of data
- Ability to authenticate an individual user (up to 2048 bit PKI)
- 128 / 192 / 256 bits on-board AES encryption of data

JavaCard has been used for authentication. Aftek implemented the following functionalities using java applet technology for securing the card data transfers.

- Card initialization
- User personalization and authorization
- Mutual authentication between the smart card and the reader
- Password change and password recovery
- Encryption, decryption of information using AES algorithms

The data on the recording disk of the card is kept encrypted. The block encryption is done "**on-the-fly**". Decryption of this data occurs on the card only upon validation by the authentication logic. Consequently, if the card is lost the stored information is protected.

Technology

Processor	: Atmel ARM7TDMI processor
USB controller	: Philips ISP1583
Smart card controller	: Philips TDA8007
Programming language	: C and assembly
Operating system	: eCos®
Protocol	: ISO 7816-3 (T=0 and T=1)