Secured Storage Device

Situation

The objective is to develop a compact electronic reader with onboard encryption intelligence. The device should be able to authenticate an individual before providing access to the information stored on the storage media.

Expected feature set

- USB composite device with two different interfaces: mass storage and CCID
- Support for standard ISO7816-3 compliant smart cards
- Ability to authenticate the user before the data is transferred to or from the massstorage media
- Ability to encrypt or decrypt the data before storing or retrieving from the mass storage media.
- High performance to quickly handle large amounts of data

Solution

Aftek has developed a complete software solution based on eCos® kernel including boot loader, OS porting, drivers' and application development.

An individual user (that is card owner) is authenticated before providing access to the encrypted partition of the storage media. The data received from the host is encrypted before being stored on the storage media. The data is decrypted before transferring to the host.

Encryption algorithm (AES) has been implemented inside FPGA to encrypt or decrypt on the fly before the data is actually written on the storage media.

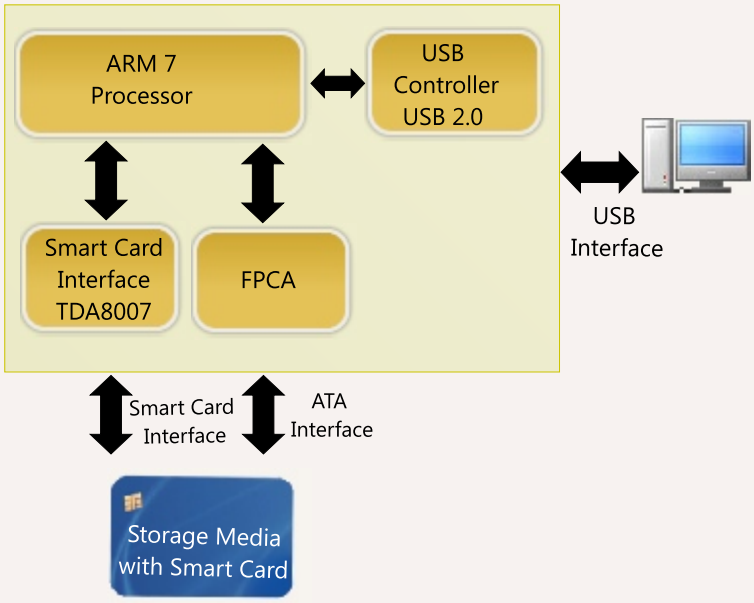
We have also developed an application on a java card using the java applet. The functionalities include:

- card initialization
- card personalization and initialization
- mutual authentication with reader
- password change and recovery

Benefits to the client

- Complete software solution due to expertise in all relevant areas
- Valuable hardware design inputs due to expertise in the similar domain

Architectural overview



Features

- A USB composite device, with two different interfaces: mass storage and CCID Compliant with:
  - Universal serial bus specification, revision 2.0 Device class specification for USB chip/smart card interface devices
  - Device class definition for mass storage devices
  - ISO/IEC 7816-3 (electronic signals and transmission protocols) (T=0 and T=1 protocols)
  - ISO/IEC 7816-4 (inter-industry commands for interchange)
- Ability to authenticate an individual user (up to 2048 bit PKI) 128 / 192 / 256 bits on-board AES encryption of data
- High performance to quickly handle large amounts of data

Technology

Processor	: Atmel ARM7TDMI
USB controller	: Philips ISP1583
Smart card controller	: Philips TDA8007
Programming language	: C and assembly
Operating system	: eCos®
Protocols	: ISO7816-3 (T=0 and T=1)